



APX 8000TM/MAX TNT[®]

Reference

Copyright© 2000, 2001 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 techpubs@ascend.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.

Safety, Compliance, and Warranty Information

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

4ESS, 5ESS, A Network of Expertise, AnyMedia, APX 8000, AqueView, AUDIX, B-STDx 8000, B-STDx 9000, ...Beyond Compare, CaseView, Cajun, CajunDocs, CAJUNVIEW, Callmaster, CallVisor, CBX 500, CellPipe, ChoiceNet, ClearReach, ComOS, cvMAX, DACScan, Dacsmate, Datakit, DEFINITY, Definity One, DSLMAX, DSL Terminator, DSLPipe, DSLTNT, Elemedia, Elemedia Enhanced, EMMI, End to End Solutions, EPAC, eSight, ESS, EVEREST, Gigabit-scaled campus networking, Globalview, GRF, GX 250, GX 550, HyperPATH, Inferno, InfernoSpaces, Intragy, IntragyAccess, IntragyCentral, Intuity, IP Navigator, IPWorX, LineReach, LinkReach, MAX, MAXENT, MAX TNT, Multiband, Multiband PLUS, Multiband RPM, MultiDSL, MultiVoice, MultiVPN, Navis, NavisAccess, NavisConnect, NavisCore, NavisRadius, NavisXtend, NetCare, NetLight, NetPartner, OneVision, Open Systems Innovations, OpenTrunk, P550, PacketStar, PathStar, Pinnacle, Pipeline, PMVision, PortMaster, SecureConnect, Selectools, Series56, SmoothConnect, Stinger, SYSTIMAX, True Access, WaveLAN, WaveMANAGER, WaveMODEM, WebXtend, and Where Network Solutions Never End are trademarks of Lucent Technologies Inc. Advantage Pak, Advantage Services, AnyMedia, ...Beyond Compare, End to End Solutions, Inter.NetWorking, MAXENT, and NetWork Knowledge Solutions are service marks of Lucent Technologies Inc. Other trademarks, service marks, and trade names mentioned in this publication belong to their respective owners.

Copyrights for Third-Party Software Included in Lucent Access Networks Software Products

C++ Standard Template Library software copyright© 1994 Hewlett-Packard Company and copyright© 1997 Silicon Graphics. Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Neither Hewlett-Packard nor Silicon Graphics makes any representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Berkeley Software Distribution (BSD) UNIX software copyright© 1982, 1986, 1988, 1993 The Regents of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley, and its contributors. 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Ordering Information

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

Feedback

Lucent Technologies appreciates your comments, either positive or negative, about this manual. Please send them to techpubs@ascend.com.

Lucent Technologies

Customer Service

To obtain product and service information, software upgrades, and technical assistance, visit the eSight™ Service Center at <http://www.esight.com>. The center is open 24 hours a day, seven days a week.

Finding information and software

The eSight Service Center at <http://www.esight.com> provides technical information, product information, and descriptions of available services. Log in and select a service. The eSight Service Center also provides software upgrades, release notes, and addenda. Or you can visit the FTP site at <ftp://ftp.ascend.com> for this information.

Obtaining technical assistance

The eSight™ Service Center at <http://www.esight.com> provides access to technical support. You can obtain technical assistance through email or the Internet, or by telephone.

If you need to contact Lucent Technologies for assistance, make sure that you have the following information available:

- Active contract number, 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 eSight Live chat. Select one of these sites when you log in to <http://www.esight.com>.

Calling the technical assistance center (TAC)

If you cannot find an answer through the tools and information on eSight or if you have a very urgent need, contact TAC. Access the eSight Service Center at <http://www.esight.com> and click **Contact Us** below the Lucent Technologies logo for a list of telephone numbers inside and outside the United States.

You can alternatively call (800) 272-3634 for a menu of Lucent services, or call (510) 769-6001 for an operator. If you do not have an active services agreement or contract, you will be charged for time and materials.

Contents

	Customer Service	iii
	About This Guide	ix
	What is in this guide.....	ix
	What you should know	ix
	Documentation conventions.....	ix
	Documentation set.....	x
Chapter 1	Command Reference	1-1
	Introduction to the command line	1-1
	Using the grep feature	1-1
	Commands that support the grep feature	1-2
	Searching for a pattern	1-2
	Examples of command output	1-3
	Alphabetic list of commands.....	1-4
Chapter 2	Profile and Parameter Reference	2-1
	Numeric.....	2-2
	A.....	2-4
	B.....	2-66
	C.....	2-75
	D.....	2-119
	E.....	2-151
	F.....	2-167
	G.....	2-189
	H.....	2-196
	I.....	2-209
	K.....	2-243
	L.....	2-245
	M.....	2-270
	N.....	2-299
	O.....	2-313
	P.....	2-329
	Q.....	2-365
	R.....	2-367
	S.....	2-394
	T.....	2-455
	U.....	2-499
	V.....	2-509
	W.....	2-521
	X.....	2-523
	Y.....	2-525

Index..... Index-1

Tables

Table 1-1	Slot-card images in first tar file	1-58
Table 1-2	Slot-card images in second tar file.....	1-59

About This Guide

What is in this guide

This guide provides an alphabetic reference to all the profiles, parameters, and commands for APX 8000™ and MAX TNT® units.

Note: This manual describes the full set of features for APX 8000 and MAX TNT units running True Access™ Operating System (TAOS) software version 9.0 or later. Some features might not be available with earlier versions or specialty loads of the software.

This guide hereafter refers to your product as a *TAOS unit*.



Warning: Before installing your TAOS unit, be sure to read the safety instructions in the *Access Networks Safety and Compliance Guide*. For information specific to your unit, see the “Safety-Related Electrical, Physical, and Environmental Information” appendix in your unit’s hardware installation guide.




What you should know

This guide is intended for the person who will configure and maintain the TAOS unit. To use it effectively, you must have a basic understanding of TAOS security and configuration, and be familiar with authentication servers and networking concepts.

Documentation conventions

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

Convention	Meaning
Monospace text	Represents text that appears on your computer’s screen, or that could appear on your computer’s screen.
Boldface monospace text	Represents characters that you enter exactly as shown (unless the characters are also in <i>italics</i> —see <i>Italics</i> , below). If you could 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
[]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination key-stroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 Caution:	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 Warning:	Warns that a failure to take appropriate safety precautions could result in physical injury.
 Warning:	Warns of danger of electric shock.

Documentation set

The APX 8000/MAX TNT documentation set consists of the following manuals:

- **Read me first:**
 - *Edge Access Safety and Compliance Guide*
Contains important safety instructions and country-specific compliance information that you must read before installing a TAOS unit.
 - *TAOS Command-Line Interface Guide*
Introduces the TAOS command-line environment and shows how to use the command-line interface effectively. This manual describes keyboard shortcuts and introduces commands, security levels, profile structure, and parameter types.

- **Installation and basic configuration:**
 - *APX 8000 Hardware Installation Guide*
Shows how to install APX 8000 hardware and includes APX 8000 technical specifications.
 - *MAX TNT Hardware Installation Guide*
Shows how to install MAX TNT hardware and includes technical specifications for MAX TNT units.
 - *APX 8000/MAX TNT Physical Interface Configuration Guide*
Shows how to configure the cards installed in a TAOS unit and their line attributes for such functions as framing, signaling, and channel usage. It also describes how calls are routed through the system and includes information about configuring the unit in a Signaling System 7 (SS7) environment. This guide explains shelf controller redundancy for an APX 8000 unit.
- **Configuration:**
 - *APX 8000/MAX TNT ATM Configuration Guide*
Describes how to configure Asynchronous Transfer Mode (ATM) operations on a TAOS unit. This guide explains how to configure physical layer attributes and how to create permanent virtual circuit (PVC) and switched virtual circuit (SVC) ATM interfaces. It includes information about ATM direct and ATM-Frame Relay circuits.
 - *APX 8000/MAX TNT Frame Relay Configuration Guide*
Describes how to configure Frame Relay operations on a TAOS unit. This guide explains physical layer configuration and restrictions and how to create permanent virtual circuit (PVC) and switched virtual circuit (SVC) interfaces. It includes information about Multilink Frame Relay (MFR) and link management, as well as Frame Relay and Frame Relay direct circuits.
 - *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*
Shows how to configure LAN and WAN routing for analog and digital dial-in connections on a TAOS unit. This guide includes information about IP routing, Open Shortest Path First (OSPF) routing, Internet Group Management Protocol (IGMP) routing, multiprotocol routers, Virtual Routers (VRouters), and tunneling protocols.
 - *MultiVoice™ for APX 8000/MAX TNT Configuration Guide*
Shows how to configure the MultiVoice application to run on a unit in both Signaling System 7 (SS7) and H.323 Voice over IP (VoIP) configurations.
- **RADIUS: TAOS RADIUS Guide and Reference**
Describes how to set up a TAOS unit to use the Remote Authentication Dial-In User Service (RADIUS) server and contains a complete reference to RADIUS attributes.
- **Administration and troubleshooting: APX 8000/MAX TNT Administration Guide**
Describes how to administer a TAOS unit, including how to monitor the system and cards, troubleshoot the unit, and configure the unit to use the Simple Network Management Protocol (SNMP).

- **Reference:**
 - *APX 8000/MAX TNT Reference*
An alphabetic reference to all commands, profiles, and parameters supported on TAOS units.
 - *TAOS Glossary*
Defines terms used in documentation for TAOS units.

Command Reference

Introduction to the command line	1-1
Using the grep feature	1-1
Alphabetic list of commands	1-4

The information in this chapter is designed for quick reference and does not include tutorials.

Note: All references to redundant shelf controllers apply to APX 8000 units only.

Introduction to the command line

You can display a usage summary for any command by entering a question mark and the name of the command:

```
admin> ? command-name
```

For an alphabetic list of commands, just enter a question mark:

```
admin> ?
```

The command line accepts a maximum of 255 characters, including the prompt. If the list of commands displayed as output does not include all of the commands described in this chapter, you might need to authenticate a User profile that has more extensive permissions. For details, see “Auth” on page 1-9.

Using the grep feature

You can filter the output of certain commands to display only the information matching a specified pattern. This functionality operates in a similar way to piping the output of the command to `grep` in UNIX.

Commands that support the grep feature

The number of commands that support the grep-like capability changes on a regular basis as the functionality is integrated into the system. Any command that can produce a large amount of output is a candidate for supporting this functionality. Following is a representative list of commands that currently support it:

ARPTable
ATMlines
Callroute
Dir
Filterdisp
HDLCL
Help
If-admin
Ifmgr
IPcache
List
Modem
Netstat
OSPF
SWANlines
T1channels
UDS3lines
Userstat

Searching for a pattern

To search for a particular pattern in command output, use the following syntax:

command | **grep** [-i] [-v] [-c] ***expression***

Option	Description
<i>command</i>	Command that supports the grep feature.
grep	Display only information that matches the <i>expression</i> pattern.
-i	Use pattern matching that is not case sensitive.
-v	Display only information that does <i>not</i> match the <i>expression</i> pattern.
-c	Count lines containing the <i>expression</i> pattern, but don't print them.
<i>expression</i>	Expression to use for pattern matching.

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

Character(s)	Description
\	Turns off any special meaning of the following character.
.	Matches any single character in the input string.
*	Matches zero or more occurrences of the previous character.
Single or double quotation marks	Enclose a pattern that contains spaces or other quotation marks.
^	Specifies the beginning of a line.
\$	Specifies the end of line.
	Specifies a logical OR.
[...]	Specifies any one of the characters in a range.
(...)	Groups 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. In addition, the number of lines found matching the pattern are displayed at the end of the command. Note that the column headers and footers might be omitted from the display if they do not match the pattern. However, error messages are exempt from pattern matching.

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

Examples of command output

Suppose the Userstat command displays the following lines without filtering:

```
291933498  1.01.06/14 1:16:05/029 64000/64000 MPP 38.13.173.193 LIsbits217
291933429  1.08.05/19 1:16:03/011 64000/64000 PPP 38.13.167.201 LIsbits26
291905815  1.01.02/13 1:11:03/000 34000/26400 PPP 38.13.104.19    ra5
```

The following command displays only the output lines that match the case-insensitive string `lisbits26`:

```
admin> userstat | grep -i lisbits26
291933429  1.08.05/19 1:16:03/011 64000/64000 MPP 38.13.167.201 LIsbits26
<grep> Found 1 line(s) matching search criteria
```

The following command displays only the output lines that *do not* match the expression `LIsbits26`:

```
admin> userstat | grep -v LIsbits26
291933498  1.01.06/14 1:16:05/029 64000/64000 MPP 38.13.173.193 LIsbits217
291905815  1.01.02/13 1:11:03/000 34000/26400 PPP 38.13.104.19    ra5
<grep> Found 2 line(s) matching search criteria
```

The following command displays only output lines that contain the number 64 plus any number of other characters followed by the string PPP:

```
admin> userstat | grep 64.*PPP
291933429 1.08.05/19 1:16:03/011 64000/64000 PPP 38.13.167.201 LISbits26
<grep> Found 1 line(s) matching search criteria
```

The following command displays only output lines that contain the string PPP followed by any four characters and the number 13:

```
admin> userstat | grep PPP....13
291933429 1.08.05/19 1:16:03/011 64000/64000 PPP 38.13.167.201 LISbits26
291905815 1.01.02/13 1:11:03/000 34000/26400 PPP 38.13.104.19 ra5
<grep> Found 2 line(s) matching search criteria
```

The following command displays only output lines that contain the string PPP followed by a space character, any character, and the number 13:

```
admin> userstat | grep "PPP 38.13"
291933429 1.08.05/19 1:16:03/011 64000/64000 PPP 38.13.167.201 LISbits26
291905815 1.01.02/13 1:11:03/000 34000/26400 PPP 38.13.104.19 ra5
<grep> Found 2 line(s) matching search criteria
```

The following command displays only output lines that contain the string LISbits217 or LISbits26:

```
admin> userstat | grep LISbits217|LISbits26
291933498 1.01.06/14 1:16:05/029 64000/64000 MPP 38.13.173.193 LISbits217
291933429 1.08.05/19 1:16:03/011 64000/64000 PPP 38.13.167.201 LISbits26
<grep> Found 2 line(s) matching search criteria
```

Alphabetic list of commands

All commands are listed alphabetically. For an overall alphabetic listing, see the general table of contents.

?

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*]

Option	Description
-a	List all commands. (Without this option, the list includes only commands authorized by the current User profile.)
<i>command-name</i>	Display information about the specified command.

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

```
admin> ?
?                ( user )
auth             ( user )
callroute        ( diagnostic )
clear            ( user )
clock-source     ( diagnostic )
clr-history      ( system )
connection       ( system )
date             ( update )
debug            ( diagnostic )
delete           ( update )
device           ( diagnostic )
dir              ( system )
dircode          ( system )
ether-display    ( diagnostic )
fatal-history    ( system )
format           ( code )
fsck             ( code )
get              ( system )
hdlc             ( system )
help             ( user )
if-admin         ( diagnostic )
igmp             ( system )
[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 with the User security level are always displayed. For details, see “Auth” on page 1-9.

See Also: Help, Auth

ARPTable

Description: Displays or modifies the TAOS unit's 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 TAOS unit can use the ARP table to respond with its own MAC address to ARP requests.

Permission level: System

Usage: `arptable [VRoutername] [-a IP_address MAC_address] | [-d IP_address] | [-f]`

Option	Description
VRoutername	The name of the Virtual Router (VRouter). If you do not specify a VRouter name, the system assumes the global VRouter.
-a IP_address MAC_address	Add an ARP table entry for the device with the specified IP address and MAC address.
-d IP_address	Delete the ARP table entry for the device at the specified IP address.
-f	Clear the ARP table.

Example: To display the ARP table:

```
admin> arptable
```

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

The ARP table displays the following information:

Column	Description
IP Address	The address contained in ARP requests.
MAC Address	The MAC address of the host.
Type	How the address was learned, that is, dynamically (DYN) or by specification of a static route (STAT).
IF	The interface on which the TAOS unit received the ARP request.
Retries	The number of retries needed to refresh the entry after it timed out.

Column	Description
Pkts	The number of packets sent out to refresh the entry after it timed out.
RefCnt	The number of times the TAOS unit consulted the entry.
Time Stamp	The number of seconds since the system has come up. The TAOS unit updates this column every time an ARP entry is refreshed.

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

ATMlines

Description: Displays information regarding DS3-ATM, E3-ATM, and OC3-ATM lines.

Permission level: System

Usage: atm`lines` [`ds3` | `oc3` | `e3`] [`-a` | `-d` | `-f` | `-u`]

Option	Description
<code>ds3</code>	Show information about DS3 lines only.
<code>oc3</code>	Show information about OC3 lines only.
<code>e3</code>	Show information about E3 lines only.
<code>-a</code>	Show information about all lines of the type specified by <code>ds3</code> , <code>e3</code> , or <code>oc3</code> (or all ATM lines if no type is specified).
<code>-d</code>	Show disabled lines of the type specified by <code>ds3</code> , <code>e3</code> , or <code>oc3</code> (or all disabled ATM lines if no type is specified).
<code>-f</code>	Show all free lines of the type specified by <code>ds3</code> , <code>e3</code> , or <code>oc3</code> (or all free ATM lines if no type is specified).
<code>-u</code>	Show lines that are in use of the type specified by <code>ds3</code> , <code>e3</code> , or <code>oc3</code> (or all in-use ATM lines if no type is specified).

Example: In the following example, the ATMlines command displays information about all DS3 lines:

```
admin> atmlines ds3 -a
```

All DS3_ATM lines:

		(dvOp	dvUpSt	dvRq	sAdm	nailg)				
Line	{	1	9	1	}	(Up	Idle	UP	UP	00012)

The output displays the following information:

Column	Description
dvOp	The current operational state of the line (also specified by Device-State): <ul style="list-style-type: none">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 channel in normal operations mode: <ul style="list-style-type: none">Idle indicates that no call is on the line.Busy indicates that the line is handling a call.
dvRq	The required state of the line as specified by Req-State: <ul style="list-style-type: none">Down indicates that the line is required to be in a nonoperational state.Up indicates that the line is required to be in normal operations mode.
SAdm	The desired administrative state of the line (also specified by Desired-State): <ul style="list-style-type: none">Down specifies that the line should terminate all operations and enter the down state.Up specifies that the line should come up in normal operations mode.
naillg	The nailed group to which the line has been assigned.

See Also: UDS3lines

ATMSVCroute

Description: Displays the SVC call-routing table. The system creates an SVC call routing entry for each configured ATM-Interface profile. To make an outbound call to a given destination ATM SVC address, the system consults the SVC call routing table for an address prefix. When the system finds a matching address prefix in the routing table, it uses the specified ATM-Interface profile index to route the call.

Permission level: System

Usage: `atmsvcroute [-d] | [-t]`

Option	Description
-d	Display the SVC routing table.
-t	Toggle debug output.

Example: atmshvcroute -d

```
Prefix=39adfc01020304050507080900, lnk={{1, 4, 1}0}
```

The sample output show a single entry in the routing table. The first item in the entry is the address prefix of the destination ATM SVC address. The second item is the index of the ATM-Interface profile used to route the call.

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`

Option	Description
<i>user-name</i>	Authenticate the specified User profile.

Example: To login as Joe:

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

If you supply the proper password for the User profile you have specified, the TAOS unit enables the privileges in that profile and then displays the system prompt again. Note that the User profile might specify its own system prompt, which is a useful way to flag certain permission levels. For example:

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

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

```
Login incorrect
User:
```

Enter the username again to display the Password prompt.

See Also: Whoami

Callroute

Description: Displays the call-routing database (the total set of all Call-Route profiles).

Permission level: Diagnostic

Usage: `callroute -ah | -an | -ad | -d | -t | -?`

Option	Description
-ah	List available host-side call routing entries.
-an	List available network-side call routing entries.
-ad	List available host-side and network-side call routing entries.
-d	List call routing tables by device.
-t	Toggle module debug level.
-?	Display a usage summary.

Example: In the following display, the output shows host-side call routing entries. All the entries are defaults, except for one Call-Route profile that specifies an inbound phone number.

```
admin> callroute -ah
```

device	#	source	type	tg	sa	phone
1:12:02/0	0	0:00:00/0	any-call-type	0	0	4812
1:12:01/0	0	0:00:00/0	voice-call-type	0	0	
1:12:03/0	0	0:00:00/0	voice-call-type	0	0	
...						
1:12:47/0	0	0:00:00/0	voice-call-type	0	0	
1:12:48/0	0	0:00:00/0	voice-call-type	0	0	

A zero or null field always means *any*. The call-routing database displays the following information:

Column	Description
Device	Interface address to which the TAOS unit routes the incoming or outgoing call. Host-side addresses show incoming-call routes, while network-side addresses show outgoing-call routes. When the TAOS unit has an incoming route for a call, it answers the call, and the host-side address points to the device (such as a modem or HDLC processor) that terminates the WAN circuit. When the TAOS unit places an outgoing call, the network-side address points to the line on which the call goes out.
#	Entry number in the call-routing database.
Source	The network-side address at which the incoming call connects to the TAOS unit, or the host-side interface address at which the outgoing call originates.
Type	Call-route type.
TG	Trunk-group number.
SA	Subaddress number.
Phone	Add-on number.

For an asynchronous V.110 call on a MultiDSP card, the Callroute command lists the card's DSP channels as available host-side call routing entries. For example:

```
admin> callroute -ah
device      # source      type            tg sa
1:06:01/0   2 0:00:00/0   v110-call-type  0 0
1:06:03/0   2 0:00:00/0   v110-call-type  0 0
1:06:05/0   2 0:00:00/0   v110-call-type  0 0
1:06:07/0   2 0:00:00/0   v110-call-type  0 0
1:06:09/0   2 0:00:00/0   v110-call-type  0 0
1:06:11/0   2 0:00:00/0   v110-call-type  0 0
1:06:13/0   2 0:00:00/0   v110-call-type  0 0
1:06:15/0   2 0:00:00/0   v110-call-type  0 0
.
.
.
1:06:95/0   2 0:00:00/0   v110-call-type  0 0
```

To display the PHS call routes on the 96-port MultiDSP slot card, use the `-ah` option to display routes by type or with the `-d` option to display routes by device, as in the following examples:

```
admin> callroute -ah
device      # source      type            tg sa phone
1:07:01/0   4 0:00:00/0   v110-call-type  0  0
1:07:02/0   4 0:00:00/0   v110-call-type  0  0
1:07:03/0   4 0:00:00/0   v110-call-type  0  0
1:07:04/0   4 0:00:00/0   v110-call-type  0  0
1:07:96/0   4 0:00:00/0   v110-call-type  0  0
1:07:01/0   3 0:00:00/0   voip-call-type  0  0
1:07:02/0   3 0:00:00/0   voip-call-type  0  0
1:07:01/0   2 0:00:00/0   phs-call-type   0  0
1:07:02/0   2 0:00:00/0   phs-call-type   0  0
1:07:03/0   2 0:00:00/0   phs-call-type   0  0
1:07:04/0   2 0:00:00/0   phs-call-type   0  0
1:07:05/0   2 0:00:00/0   phs-call-type   0  0
1:07:06/0   2 0:00:00/0   phs-call-type   0  0
1:07:95/0   2 0:00:00/0   phs-call-type   0  0
1:07:95/0   1 0:00:00/0   digital-call-type 0  0
1:07:96/0   1 0:00:00/0   digital-call-type 0  0
```

Command Reference

Clear

```
admin> callroute -d
device      #          source          type  tg      sa phone
1:07:01/0  0 0:00:00/0  voice-call-type  0    0
1:07:01/0  1 0:00:00/0  digital-call-type 0    0
1:07:01/0  2 0:00:00/0  phs-call-type    0    0
1:07:01/0  3 0:00:00/0  voip-call-type   0    0
1:07:01/0  4 0:00:00/0  v110-call-type   0    0
1:07:01/0  5 0:00:00/0  any-call-type    0    0
1:07:02/0  0 0:00:00/0  voice-call-type  0    0
1:07:02/0  1 0:00:00/0  digital-call-type 0    0
1:07:02/0  2 0:00:00/0  phs-call-type    0    0
1:07:02/0  3 0:00:00/0  voip-call-type   0    0
1:07:02/0  4 0:00:00/0  v110-call-type   0    0
1:07:02/0  5 0:00:00/0  any-call-type    0    0
1:07:96/0  0 0:00:00/0  voice-call-type  0    0
1:07:96/0  1 0:00:00/0  digital-call-type 0    0
1:07:96/0  2 0:00:00/0  phs-call-type    0    0
1:07:96/0  3 0:00:00/0  voip-call-type   0    0
1:07:96/0  4 0:00:00/0  v110-call-type   0    0
```

See Also: Modem, HDLC, Show, Tlchannels

Clear

Description: Clears the terminal session screen and places the system prompt at the top row of the VT100 window.

Permission level: User

Usage: `clear [-r]`

Option	Description
-r	Reset the terminal session's VT100 attributes.

Example: To clear the screen:

```
admin> clear
```


CLeval

Description: Enables the call-logging evaluation license. You can enable the license once each system reset.

Permission level: System

Usage: `cleval`

Example: To enable the call-logging evaluation license, enter the CLeval command:

```
admin> cleval
Date: 04/12/2000. Time: 06:45:07
The call logging evaluation is hereby granted for a period
of 30 days, the current evaluation license will expire on
Date: 05/12/2000. Time: 06:45:07
```

Dependencies: Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

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 throughout the system. 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.

The Clock-Source command applies to units with T1, E1, T3, or FrameLine™ cards. It 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 can execute this command on the shelf controller or on an individual T1, E1, T3, or FrameLine card. You must first execute the Open command to open a session with the card.

Permission level: Diagnostic

Usage: `clock-source`

Example: The Clock-Source command on the shelf controller shows the master clock's slot card line number:

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

On the slot cards, the Clock-Source command uses one-base indexes for the card's lines. For example, to open a session with a T1 card and display its clock-source settings:

```
admin> open 1 1
t1-1/15> 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
```

See Also: Line, Open, T1channels

Clr-History

Description: Clears the fatal-error log.

Permission level: System

Usage: `clr-history [-f]`

Option	Description
No arguments	Clear the primary controller's fatal-error log.
-f (APX 8000 unit only)	Clear the primary and secondary controller's fatal-error logs. The cleared log on the secondary controller might be overwritten by a transfer of information from the primary controller while the controllers are exchanging information.

Example: To clear the log on a MAX TNT unit:

```
admin> clr-history
```

To clear the log for both controllers on an APX 8000 unit:

```
admin> clr-history -f
```

See Also: Fatal-History

Connection

Description: Specifies that the upper-left portion of the status window must display 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: An administrator opens a window with connection status information displayed:

admin> `connection`

2 Connections	Status
001 tomw PPP 1/7/14 19200	Serial number: 6201732 Version: 1.0F
002 timl MP 1/7/3 56000	
	Rx Pkt: 11185897
	Tx Pkt: 42460
	Col: 129
	09/27/2000 12:20:15 Up: 3 days, 21:47:32
	M: 29 L: info Src: shelf-1/controller
	48 out of 48 modems passed POST
	Issued: 16:48:02, 09/27/2000

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

For each active connection, the displays includes a line that shows the user or station name, type of connection, T1 shelf/line/channel on which the call was placed or received, and the bandwidth or baud rate. (The shelf number is always 1.) You can press the Down-Arrow key to scroll through the list of active connections.

To display a prompt below the status window, press the Escape key. To close the status window, enter the Status command:

admin> `status`

See Also: Line, List, Log, Status, View

Date

Description: Displays TAOS unit's system date and time. The date and time are stored in the Timedate profile.

Permission level: Update

Usage: `date`

Dependencies: If you try to use the Date command to set the system date and time, the system displays the following message:

error: Use TIMEDATE profile to set system time/date

Debug

Description: Enables or disables diagnostic output.

Permission level: Diagnostic

Usage: `debug on | off`

Syntax 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)
```

Delete

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

Permission level: Update

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

Syntax element	Description
<code>-f</code>	Delete without prompting for confirmation.
<code>profile-type</code>	A type of profile, as listed by the Dir command.
<code>profile-index</code>	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
```

Dependencies: Deleting a VRouter profile deletes the Virtual Router (VRouter). If you delete a VRouter with active connections, you must perform a system reset. If a system reset is not possible, you must manually tear down the VRouter's active connections and then modify the local Connection, IP-Interface, and IP-Route profiles that point to the VRouter.

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 bring a device up or down. For a list of devices supported by the TAOS unit, see the description of Device-Address.

Permission level: Diagnostic

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

Option	Description
<code>-d</code>	Bring the specified device down.
<code>-t</code>	Toggle debug output level.
<code>-u</code>	Bring the specified device up.
<code>-?</code>	Display a usage summary.
<code>interface_address</code>	The interface address of the device, specified as shelf, slot, item number, and logical item number. The shelf number is always 1.

Example: To bring down modem #24 in slot #3:

```
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 TAOS 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]]`

Option	Description
<code>profile-type</code>	List all the profiles of the specified type.
<code>profile-index</code>	Display information about the specified profile.

Example: To list all profile types, enter the Dir command with no options:

```
admin> dir
ADMIN-STATE-PERM-IF  SNMP Permanent Interface Admin State
ADMIN-STATE-PHYS-IF  SNMP Physical Interface Admin State
ANSWER-DEFAULTS      Answer profile
ATALK-GLOBAL          Global Appletalk parameters
ATALK-INTERFACE       Appletalk interfaces
ATMP                  ATMP profile
BASE                  System version and enabled features
```

CALL-INFO	Active call information
CALL-LOGGING	Call logging
CALL-ROUTE	Call routing attributes
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
FILTER	Filter Profile
FRAME-RELAY	Frame-Relay link configuration
IP-GLOBAL	Global TCP/IP parameters
IP-INTERFACE	IP interfaces
IP-ROUTE	Static IP routes
IPX-GLOBAL	Global IPX parameters
IPX-INTERFACE	IPX interfaces
IPX-ROUTE	Static IPX routes
IPX-SAP-FILTER	IPX Sap Filters
L2-TUNNEL-GLOBAL	Layer 2 tunnel global profile
LAN-MODEM	LAN Modem Disable State
LOAD-SELECT	Code images to load
LOG	System event logging configuration
SERIAL	Serial interfaces
SLOT-INFO	Slot Info profile
SLOT-STATE	Slot Operational State
SLOT-TYPE	Slot Type profile
SNMP	SNMP configuration
SWAN	Swan line parameters
SWAN-STAT	Swan line status
SYSTEM	System-wide basic parameters
T1	DS1 line parameters
T1-STAT	DS1 line status
T3	DS3 line parameters
T3-STAT	DS3 line status
TERMINAL-SERVER	Terminal server parameters
TIMEDATE	Current system date and time
TRAP	SNMP trap destinations
TUNNEL-SERVER	Tunnel server profiles
USER	Administrative user accounts
VRROUTER	Virtual Router

Example: To list all Connection profiles, as well as all RADIUS profiles for nailed-up connections, specify `conn` as the profile type. For example:

```
admin> dir conn
169  08/31/2000 22:21:07  dallas
195  09/12/2000 10:14:08  chicago
189  09/14/2000 09:34:44  nyc1
177  09/14/2000 11:38:09  nyc2
187  10/22/2000 15:34:53  la
201  10/14/2000 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 (leftmost) field shows the number of bytes 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.

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

```
admin> dir conn dallas
169  08/31/2000 22:21:07  dallas
```

See Also: List, Get

Dircode

Description: Displays the contents of the PCMCIA flash-card code directory. The flash cards contain code for the slot cards, shelf controller, and profiles. The system configuration is stored in the onboard NVRAM.

Permission level: System

Usage: `dircode`

Example: Dircode command output looks like the following:

```
admin> dircode flash-card-2
Card 2, format FTL/FAT, capacity 8MB
/current:
shelf controller  1231877 Tue Sep 19 17:17:22 2000 9.0.0
8t1-card          209191 Tue Sep 19 17:17:42 2000 9.0.0
4ether2-card      180385 Tue Sep 19 17:17:56 2000 9.0.0
hdlc2-card        588610 Tue Sep 19 17:18:38 2000 9.0.0
```

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.

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

Card N is not formatted for use with this system

The flash card is blank, corrupted, or formatted for another environment, such as DOS. To use this card, you must issue a Format command first.

Card N is temporarily unavailable

The flash card is currently coming up or is being formatted.

Card N is unavailable

The flash card experienced an error and is inaccessible. Check that the card is inserted properly.

See Also: Format, Fsock, Load

DNStab

Description: Displays the local Domain Name System (DNS) host table, which supplies host IP addresses when DNS fails to successfully resolve a hostname. This table is not a DNS cache, but a fallback option, listing up to eight host addresses for important or frequently used connections.

Permission level: System

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

Option	Description
-s	Display the local DNS table. This options is supported on all slot cards that support DNS.
entry-number	Display an entry from the local DNS table. You can specify an integer from 1 to 8.

Example: To display the local DNS table:

```
admin> dnstab -s
```

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

```
Local DNS Table
```

Name	IP Address	# Reads	Time of last read
1: "barney"	200.65.212.12 *	2	Feb 10 10:40:44 99
2: "rafael"	200.65.212.23	3	Feb 10 9:30:00 99
3: "donatello"	200.65.212.67	1	Feb 11 11:41:33 99
4: "wheelers"	200.65.212.9	1	Feb 12 8:35:22 99

The output contains the following fields:

Field	Description
Local DNS Table	Specifies whether Enabled=Yes in the DNS-Local-Table subprofile of the IP-Global profile.
AutoUpdate	Specifies whether Auto-Update=Yes in the DNS-Local-Table subprofile of the IP-Global profile.
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 SNTP is not in use, the field contains hyphens.

DS3link

Description: Enables you to carry out a diagnostic session with an unchannelized DS3 card. You must first execute the Open command to open a session with the card.

Permission level: Diagnostic

Usage: `ds3link -a | -c | -d | -l | -i | -s | -t | -?`

Option	Description
<code>-a</code>	Display current DS3 line alarms.
<code>-c</code>	Display and clear line error statistics.
<code>-d 1-7</code>	Display current DS2 line state.
<code>-l on off</code>	Perform an external loopback test.
<code>-i on off</code>	Perform an internal loopback test.
<code>-s</code>	Display line error statistics without clearing.
<code>-t</code>	Toggle debug output.
<code>-?</code>	Display summary.

Opening a session with an unchannelized DS3 card

Before you can use the DS3link command, you must open a session with the card on which you wish to perform diagnostics. For example, to open a session with the card in slot 15:

```
admin> open 1 15
t3-1/15>
```

Displaying alarms on the DS3 line

To display alarms on the line, specify the **-a** option. For example:

```
t3-1/15> ds3link -a
  Loss of Signal:           false
  Out of Frame:            false
  Alarm Indication Signal: false
  Idle Signal:             false
  Yellow Signal:           false
  In Red Alarm:            false
  C-bit parity framing:    false
```

An alarm condition of **true** has the following significance:

Alarm	Description (if the condition is true)
Loss of Signal	The DS3 line is not functioning. A sequence of 175 consecutive zeroes was detected.
Out of Frame	The DS3 line cannot receive or transmit data because the TAOS unit has lost the frame alignment on the received signal.
Alarm Indication Signal (AIS)	A device on the line has sent the AIS signal, rather than regular data, in order to take the line out of service.
Idle Signal	The remote device has no data to send.
Yellow Signal	Also called Remote Alarm Indicator, (RAI). A device on the DS3 line is detecting framing-error conditions in the signal it receives.
In Red Alarm	An out-of-frame condition has lasted for more than 2.23 msec.
C-bit parity	The remote end is using C-bit parity.

Displaying and clearing line error statistics

To display and clear line error statistics, specify the **-c** option. For example:

```
t3-1/15> ds3link -c
  Line Code Violations:    2136611
  Framing Errors:         67279
  Excessive Zeros:        2098353
  P-bit Parity Errors:     217318
  C-bit Parity Errors:     0
  Far End Block Errors:    0
  DS2 1 Framing Errors:    8415
  DS2 2 Framing Errors:    8415
  DS2 3 Framing Errors:    8415
  DS2 4 Framing Errors:    8415
  DS2 5 Framing Errors:    8415
  DS2 6 Framing Errors:    8415
  DS2 7 Framing Errors:    8415
  Statistics cleared.
```

Following are descriptions of the fields in the output:

Field	Description
Line Code Violations (LCV)	The TAOS unit detected a Bipolar Violation, indicating that one of the low-level rules for encoding data was violated in the received signal.
Framing Errors (FERR)	The number of errors in the bits used to frame the DS3 signal. DS2 and DS3 framing requires that certain bit positions in the signal (framing bits) have fixed values. These known points of reference are used to determine where frames begin and end. If enough framing-bit errors occur, the signal is Out Of Frame (OOF).
Excessive Zeros	Three or more zeroes were seen in a row, which violates the density requirements of B2ZS.
P-bit Parity Errors (PERR)	The number of times that the P-bit parity check failed. The P bits in a DS3 frame are used to encode parity for the entire frame. Each PERR indicates that a received frame's content did not match its parity bits, a condition that implies data corruption. The P bits are recalculated by each device that forwards the DS3 signal, and therefore measure errors between sections.
C-bit Parity Errors (CPERR)	The number of times that the C-bit parity check failed. This parity check is offered under C-Bit-Parity framing only.
Far End Block Errors (FEBE)	The number of times the remote end has sent an FEBE signal, indicating it has received DS3 frames with either Framing Errors (FERR) or C-bit Parity Errors (CPERR).
DS2 # Framing Errors (FERR)	The number of errors in the bits used to frame the DS2 signal.

Displaying the line state of a DS2

To display the line state of a DS2, specify the `-d 1-7` option. For example, to display the state of the third DS2:

```
t3-1/15> ds3link -d 3
State of DS2 3:
Out of Frame:           false
Alarm Indication Signal: false
Yellow Signal:          false
In Red Alarm:            false
Reserved Bit:            false
```

An alarm condition of `true` has the following significance:

Alarm	Description (if condition is true)
Out of Frame	The third DS2 stream in the DS3 line cannot receive or transmit data because the unit has lost the frame alignment on the received signal.
Alarm Indication Signal (AIS)	The unit is receiving an AIS on this DS2 stream of the DS3 line. A device on the line has sent the AIS signal, rather than regular data, in order to take the line out of service.
Yellow Signal	Also called Remote Alarm Indicator (RAI). A device on the DS2 stream is detecting framing-error conditions in the signal it receives.
In Red Alarm	An out-of-frame condition has lasted for more than 9.9 msec.
Reserved Bit	The state of the reserved bit does not have any significance in diagnosing the state of the DS2 stream.

Performing an external loopback test

To perform an external loopback test, specify the `-l on` option:

```
t3-1/15> ds3link -l on
DS3 remote loopback activated
```

When the DS3 remote loopback is activated, the unit returns the signal it receives on the DS3 line. After the test, enter the DS3link command with the `-l off` option:

```
t3-1/15> ds3link -l off
DS3 remote loopback deactivated
```

Performing an internal loopback test

The `-i` option connects the DS3 receive path to the DS3 transmit path at the D3MX. The transmitted DS3 signal is still sent to the network as well. The following example shows how to activate and then deactivate a DS3 internal loopback:

```
t3-1/15> ds3link -i on
DS3 internal loopback activated
t3-1/15> ds3link -i off
DS3 internal loopback deactivated
```

E1sig

Description: Displays the state of all E1 channels. You must first execute the Open command to open a session with the E1 card.

Permission level: Diagnostic

Usage: `e1sig`

Example: To diagnose the state of all E1 channels:

```
admin> open 1 10
e1-1/10>
```

```
e1-1/10> elsig
E1: 0, Channel: 1, state: 1
E1: 0, Channel: 2, state: 1
E1: 0, Channel: 3, state: 1
E1: 0, Channel: 4, state: 1
E1: 0, Channel: 5, state: 1
E1: 0, Channel: 6, state: 1
E1: 0, Channel: 7, state: 1
E1: 0, Channel: 8, state: 1
E1: 0, Channel: 9, state: 1
E1: 0, Channel: 10, state: 1
E1: 0, Channel: 11, state: 1
E1: 0, Channel: 12, state: 1
E1: 0, Channel: 13, state: 1
E1: 0, Channel: 14, state: 1
E1: 0, Channel: 15, state: 1
E1: 0, Channel: 17, state: 1
E1: 0, Channel: 18, state: 1
E1: 0, Channel: 19, state: 1
E1: 0, Channel: 20, state: 1
E1: 0, Channel: 21, state: 1
E1: 0, Channel: 22, state: 1
E1: 0, Channel: 23, state: 1
E1: 0, Channel: 24, state: 1
E1: 0, Channel: 25, state: 1
E1: 0, Channel: 26, state: 1
E1: 0, Channel: 27, state: 1
E1: 0, Channel: 28, state: 1
E1: 0, Channel: 29, state: 1
E1: 0, Channel: 30, state: 1
E1: 0, Channel: 31, state: 1
```

E1-Stats

Description: Reports DS1-level line errors on an E1 card. You must first execute the Open command to open a session with the card.

Permission level: Diagnostic

Usage: **e1-stats** [**-c**] *line*

Syntax element	Description
-c	Display statistics for the line, and reset the statistics to 0 (zero).
<i>line</i>	Line on the card.

Example: To open a session with a card in slot 13:

```
admin> open 1 13
e1-1/13>
```

To display and reset the statistics on line 2:

```
e1-1/13> e1-stats -c 2
DS1 Line 2:
CRC Errors:                0
Frame Slips:               9872
Framing Bit Errors:        0
Out of Frame Events:       0
Far End Block Errors:      0
Line Code Violations:      0
    Statistics cleared.
```

The significance of each number in the output is as follows:

Field	Description
CRC errors	Data corruption in the signal.
Frame slips	The TAOS unit received E1 data at a greater or less frequency than that of the internal line clock. In the process of realigning itself to the transmitter, the TAOS unit can skip or repeat a frame.
Framing bit errors	The TAOS unit detected a framing bit that was incorrect. E1 framing requires that certain bit positions (known as framing bits) have a fixed value in the signal.
Out of Frame Events	The TAOS unit no longer detects a framing pattern in the receiving signal, or it detects a pattern at a different relative offset than expected.
Far end block errors	How frequently the remote end reported errors in E1 frames transmitted by the TAOS unit.
Line Code Violations	The TAOS unit detected either a Bipolar Violation or Excessive Zeros, indicating that one of the low-level E1 rules for encoding data was violated in the received signal.
Statistics cleared	The statistics have been reset to 0 (zero), because the command included the <code>-c</code> option.

Ether-Display

Description: Displays the contents of Ethernet packets.

Permission level: Diagnostic

Usage: `ether-display port# n`

Syntax element	Description
port#	The Ethernet port on which the packets are received or transmitted. If you specify 0 (zero) for the port number, the TAOS unit displays all ports.
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 . .... {^.<
```

To stop displaying the Ethernet statistics, enter:

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

Note: You must set Debug On for Ether-Display to have any effect.

Fanstatus

Description: Displays fantray status information, such as the fan's RPM and status, and the unit's ambient temperature.

Permission level: System

Usage: fanstatus

Example: The current fan mode can be displayed as either full-speed or low-noise.

For example, the following output shows the fan mode set to full-speed with an ambient temperature of 33 degrees Celsius:

```
admin> fanstatus
```

```
APX8000 Fantray status
Fantray ambient temperature: 33 C
Current fan mode: Full-speed
```

Fan #	RPM	Status
=====		
1	3367	GOOD
2	3214	GOOD
3	3075	GOOD
4	3075	GOOD
5	3214	GOOD
6	3289	GOOD

The following command output shows the fan mode set to low-noise with an ambient temperature of 27 degrees Celsius:

```
admin> fanstatus
```

```
APX8000 Fantray status
Fantray ambient temperature: 27 C
Current fan mode: Low-noise
```

Fan #	RPM	Status
=====		
1	1992	GOOD
2	2050	GOOD
3	1992	GOOD
4	2020	GOOD
5	2050	GOOD
6	2020	GOOD

See Also: Thermalstatus

Fatal-History

Description: Displays the TAOS unit's fatal-error log. Every time a fatal error occurs on the TAOS unit, it is logged to the fatal-error log. Available flash 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: When you display the fatal-error log on an APX 8000 unit, information similar to the following appears:

```
admin> fatal-history
SYSTEM IS UP:  Index: 100  Revision: 9.0  Slot 1/41 (apxsre)
                Date: 10/07/2000.      Time: 12:07:39
PRIMARY SELECTED:  Index:  98  Revision: 9.0  Slot 1/41 (apxsre)
                Date: 10/07/2000.      Time: 12:07:52

OPERATOR RESET:  Index:  99  Revision: 9.0  Slot 1/41 (apxsre)
                Date: 10/07/2000.      Time: 12:20:02
Reset from 172.31.1.254, user profile admin.

SYSTEM IS UP:  Index: 100  Revision: 9.0  Slot 1/41 (apxsre)
                Date: 10/07/2000.      Time: 12:22:06
PRIMARY SELECTED:  Index:  98  Revision: 9.0  Slot 1/41 (apxsre)
                Date: 10/07/2000.      Time: 12:22:19
```

When you display the fatal-error log on a MAX TNT unit, information similar to the following appears:

```
admin> fatal-history
OPERATOR RESET:  Index:  99  Revision: 1.3Ap6 Shelf 1 (tntsr)
                Date: 09/20/2000.      Time: 16:56:01
Reset from unknown, user profile super.

OPERATOR RESET:  Index:  99  Revision: 1.3Ap6 Shelf 1 (tntsr)
                Date: 09/24/2000.      Time: 11:56:10
Reset from unknown, user profile super.
```

See Also: Clr-History

FE-Loop

Description: Performs a line loopback at the transceiver of a T1, E1, or T3 card. You must first execute the Open command to open a session with the card.

Permission level: Diagnostic

Usage: `fe-loop line in|out on|off`

Syntax element	Description
<i>line</i>	DS1 line.
<i>in</i>	Perform local loopback. This option is useful for performing a check of the line-card hardware. It is not supported by the T3 card.
<i>out</i>	Perform remote loopback. This option is useful when a line is being provisioned or diagnosed.
<i>on</i>	Enable loopback.
<i>off</i>	Disable loopback.

Example: To loop the CSU towards the network for the first DS1 in slot 1:

```
admin> open 1 1
t1-1/1>
t1-1/1> fe-loop 1 out on
```

The receive side of the T1 is not bridged to the TAOS unit. To turn the loopback off:

```
t1-1/1> fe-loop 1 out off
```

See Also: DS3link

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]`

Option	Description
<code>-s [filtername]</code>	If filtername 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]`

Argument	Description
No argument	Display all active sessions and their filter names.
<i>sessNum</i>	Display filter details for the specified session.

Example: admin> `filterdisp`

```

ID      Username      Src Route-Filter Data-Filter Call-Filter TOS-Filter
-----
010    dialin-23      ext
016    dialin-4       ext
017    edleung         ext          < filters present >
018    jwebster        ext          < filters present >
019    pyan            loc          datfilt2      callfilt4  tostestfilt
020    guest           ext
021    pvc2            loc          route-pvc
022    pvc4            loc
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. Externally authenticated sessions, such as RADIUS sessions, have no associated filter names. They appear with a `<filters present>` notation. The columns in the command output provide the following information:

Output field	Specifies
ID	Identification number for the session.
Username	Name of the authenticated profile.
Src	Whether the profile is downloaded through RADIUS (<code>ext</code>) or recognized as a local profile (<code>loc</code>).
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, <code><filters present></code> 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, <code><filters present></code> indicates that a data filter has been applied. If blank, no data filter applies.

Output field	Specifies
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, <filters present> 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, <filters present> indicates that a TOS filter has been applied. If blank, no TOS filter applies.

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
```

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
```

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
```

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
```

See Also: Filtcache

Format

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

Permission level: Code

Usage: `format [-f] device`

Syntax element	Description
-f	Force format without asking for verification.
device	The name of the flash card to be formatted. The following are valid names: <ul style="list-style-type: none">• <code>[flash-card-]1</code>• <code>[flash-card-]2</code> Note that device names can be abbreviated as 1 and 2.

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

error: flash card N is not present

No flash card is detected in the specified slot (1 or 2).

error: flash card N is unavailable

The flash card in the specified slot is already being formatted, is just coming up, or is in an error condition.

error: flash card N is write-protected

The write-protect switch is set on the card in the specified slot (1 or 2).

error: flash card N is currently in use

One or more images on the flash card are currently in use (being read by a slot card in LOAD state or being written as part of a code download).

Example: After inserting a PCMCIA flash card in the second (rightmost) slot on the shelf controller, you would format it as follows:

```
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 card. For each file found, the command displays the type-name, type-number, decimal and hex byte counts, date written to flash, 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*

Argument Significance

- b** Try to ignore bad magic. Each flash card file system contains two directory blocks: an in-use block and an empty block used when deleting information. Both directory blocks contain a *magic* identifier, which indicates that they are indeed directory blocks. A candidate directory block is one that is missing the magic identifier but contains information that can be interpreted as directory-block information. If Fsck finds no valid directory block but does find a candidate directory block, this option causes it to ignore the bad magic and go ahead and use the candidate directory block anyway. This option allows the file system to be used normally until the next reboot, assuming that the Fsck command found no other errors.
- c** Do not check file contents. By default, Fsck 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 Fsck to check only the file-system format.
- v** Display verbose messages, including the number of blocks used, a block list, and (unless the -c option is specified) various information about the files found.
- device** The name of the flash card to be checked. The following are valid names:
 - [flash-card-]1
 - [flash-card-]2

Note that device names can be abbreviated as 1 and 2.

Example: admin> **fsck 1**

```
Card version info 'No version tuple found.'
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: 99
Clusters lost during interrupted writes: 0
Other reserved clusters: 3339
```

See Also: Dircode, Format, Load

FWALLdblog

Note: The FWALLdblog command is not supported by the TAOS unit at this time.

Description: Displays firewall messages.

Permission level: Diagnostic

Usage: **FWALLdblog**

Messages generated by firewalls have the following format:

date time router-name ASCEND: interface message

Following the date and time the message was logged is the name of the router from which the message was sent. The name of the interface (for example, ie0) is also shown. The message itself can contain one or more of the following fields:

protocol local direction remote length frag log tag

Each field has the following significance:

Field	Description
<i>protocol</i>	<p>For non-IP protocols, shows the 4-digit hexadecimal Ether Type or the network protocol name. For IP protocols, shows either the IP protocol number (up to 3 decimal digits) or one of the following names:</p> <ul style="list-style-type: none">• ip-in-ip• tcp• icmp• udp• esp• ah <p>The ICMP value might also include the ICMP Code and Type as: <i>[code]/[type]/icmp</i>. For a list of IP protocols, see the description of the Protocol setting.</p>
<i>local</i>	<p>For non-IP packets, shows the packet's source or destination Ethernet MAC address (depending on whether the packet is inbound or outbound). On a WAN connection, the two MAC addresses are all zeros.</p> <p>For IP packets, indicates the packet's source or destination IP address. In the case of TCP or UDP, also includes the TCP or UDP port number as <i>([IP_address] ; [port])</i>.</p>
<i>direction</i>	<p>An arrow shows the direction in which the packet was traveling (<- for inbound or -> for outbound).</p>

Field	Description
<i>remote</i>	For non-IP packets, specifies the packet's source or destination Ethernet MAC address (depending on whether the packet is inbound or outbound). For IP packets, specifies the packet's source or destination IP address. In the case of TCP or UDP, also includes the TCP or UDP port number as (<i>[IP_address] ; [port]</i>).
<i>length</i>	Specifies the length of the packet in octets (8-bit bytes).
<i>frag</i>	Indicates packet fragmentation. This field is present if the packet has a nonzero IP offset or the IP More-Fragments bit is set in the IP header.
<i>log</i>	Reports packet status or header flags. Packet status messages include: <ul style="list-style-type: none"> • <i>corrupt</i>—The packet is internally inconsistent. • <i>unreach</i>—The packet was generated by an <i>unreach</i> rule in the firewall. • <i>!pass</i>—The packet was blocked by the data firewall. <p>Packet header flags are TCP flag bits, including <i>syn</i>, <i>fin</i>, and <i>rst</i>. The <i>syn</i> flag should only be displayed for the initial packet, which has the <i>syn</i> flag set and the <i>ack</i> flag not set.</p>
<i>tag</i>	Contains user-defined tags.

See Also: FWALLversion

FWALLversion

Note: The FWALLversion command is not supported by the TAOS unit at this time.

Description: Displays the firewall versions supported by the current system software.

Permission level: Diagnostic

Usage: FWALLversion

Example: To display the supported firewall versions:

```
admin> FWALLversion
1 2
```

The output shows all firewall versions supported in the current code. The version numbers are separated by spaces.

See Also: FWALLdblog

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 1-102.

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

Permission level: System

Usage: `get profile-type [profile-index] [sub-profile]`
`[param-name [param-index]]`

Syntax element	Description
profile-type	The 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	The profile index (the name or address that distinguishes a profile from others of the same type). To see profile indexes, use the Dir command.
sub-profile	A subprofile within the specified profile.
param-name	A 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 Interface-Address parameter contains both the physical-address and logical-item indexes.

APX 8000 examples

The following example shows how to use the *param-name* argument for the IP address of an Ethernet interface on an APX 8000 unit:

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

The next example shows how to use a parameter index on the Get command line of an APX 8000 unit:

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

MAX TNT examples

The following example shows how to use the *param-name* argument for the IP address of an Ethernet interface on a MAX TNT unit:

```
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
```

The next example shows how to use a parameter index on the Get command line of a MAX TNT unit:

```
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
```

Generic examples

To display the contents of a Connection profile called Dallas:

```
admin> get connection dallas
[in CONNECTION/dallas]
station* = dallas
active = yes
encapsulation-protocol = mpp
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 "" "" +
ppp-options = { ***** ***** stac 1524 no 600 600 }
mp-options = { 1 1 2 }
mpp-options = { "" quadratic transmit 1 1 15 5 10 70 }
tcp-clear-options = { "" 0 }
answer-options = { }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
```

To display the OSPF subprofile:

```
admin> get connection dallas ip-options ospf
[in CONNECTION/dallas:ip-options:ospf-options]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 30
dead-interval = 120
priority = 5
authen-type = simple
auth-key = unit0
cost = 10
```

Command Reference

Get

```
down-cost = 1000
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
```

The Get command, followed by a space and a period, displays the contents of the current location in the working profile:

```
admin> get .
[in CONNECTION/dallas:ip-options:ospf-options]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 30
dead-interval = 120
priority = 5
authen-type = simple
auth-key = unit0
cost = 10
down-cost = 1000
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
```

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

```
admin> get . ..
[in CONNECTION/dallas:ip-options]
ip-routing-enabled = yes
vj-header-prediction = yes
assign-address = no
remote-address = 10.9.5.6/24
if-remote-address = 0.0.0.0
local-address = 0.0.0.0/0
routing-metric = 7
down-metric = 7
preference = 100
down-preference = 255
private-route = no
multicast-allowed = no
address-pool = 0
auth-pool-address = 0.0.0.0
ip-direct = 0.0.0.0
rip = routing-off
ospf-options = { no 0.0.0.0 normal 10 30 120 5 simple ***** 10 +
multicast-rate-limit = 100
client-dns-primary-addr = 0.0.0.0
client-dns-secondary-addr = 0.0.0.0
client-dns-addr-assign = yes
client-default-gateway = 0.0.0.0/0
```

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

```
admin> get . ip ospf
[in CONNECTION/dallas:ip-options:ospf-options]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 30
dead-interval = 120
priority = 5
authen-type = simple
auth-key = unit0
cost = 10
down-cost = 1000
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
```

See Also: Read, Write, List

HDLC

Description: Displays information about the channels handled by the High-Level Data Link Control (HDLC) controller. The HDLC controller handles all channels except those using Serial Line Internet Protocol (SLIP), Compressed Serial Line Internet Protocol (CSLIP), or asynchronous PPP. A multichannel connection uses multiple HDLC channels.

Permission level: System

Usage: `hdlc -a | -d | -f | -i | -p`

Option	Description
-a	Display all available HDLC channels.
-d	Display disabled HDLC channels.
-f	Display failed/nonexistent HDLC channels.
-i	Display in-use HDLC channels.
-p	Display all possible HDLC channels.

Example: To display information about all available HDLC channels, specify the `-a` option:

```
admin> hdlc -a
HDLC channels available for use:

                                (dvOp  dvUpSt  dvRq  sAdm)
HDLC { { 1 5 1 } 1 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 2 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 3 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 4 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 5 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 6 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 7 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 8 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 9 }          (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 10 }         (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 11 }         (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 12 }         (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 13 }         (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 14 }         (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 15 }         (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 16 }         (Up  Idle  UP  UP )
HDLC { { 1 5 1 } 17 }         (Up  Idle  UP  UP )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

The data displayed includes the physical address and channel number, and the following status information about each channel:

Column	Description
dvOp	<p>The current operational state of the channel (also specified by the Device-State setting):</p> <ul style="list-style-type: none"> Down indicates that the channel is in a nonoperational state. Up indicates that the channel is in normal operations mode.
dvUpSt	<p>The status of the channel in normal operations mode:</p> <ul style="list-style-type: none"> Idle indicates that no call is on the line. Active indicates that the channel is handling a call.
dvRq	<p>The required state of the channel as specified by ReqD-State:</p> <ul style="list-style-type: none"> Down indicates that the channel is required to be in a nonoperational state. Up indicates that the channel is required to be in normal operations mode.
SAdm	<p>The desired administrative state of the channel (also specified by the Desired-State setting):</p> <ul style="list-style-type: none"> Down specifies that the channel should terminate all operations and enter the down state. Up specifies that the channel should come up in normal operations mode.

The actual state of the channel 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 force a channel to the new state. It indicates that the TAOS unit should change the channel state in a graceful manner.

The `hdlc -p` command prints statistics every second, rather than summarizing the statistics in the output report. Using this option provides a more detailed picture of error conditions. In addition, the total number of open channels is displayed. Following is a sample of the command's output:

```
hdlc2-1/4> hdlc -p
send rcvq sndq rcvq d scr bufr crc long overrun inex abort txund nopen
0      0      0    400 1000 1800 0      0      0      0      0      0      0
0      0      0    400 1000 1800 0      0      0      0      0      0      0
0      0      0    400 1000 1800 0      0      0      0      0      0      0
0      0      0    400 1000 1800 0      0      0      0      0      0      0
0      0      0    400 1000 1800 0      0      0      0      0      0      0
```

The output displays the following fields:

Field	Description
send	Total number of packets sent in the previous second.
rcvq	Total number of packets received in the previous second.
sndq	Total number of packets currently queued for transmission.
rcvq	Total number of packets currently queued for reception.
dscr	Total number of buffers for which there is an accounting. This value is useful for detecting a buffer leak. Currently, there is a total of 1800 buffers.
bufr	Total number of buffers for which there is an accounting. This value is useful for detecting a buffer leak. Currently, there is a total of 1800 buffers.
crc	Total number of packets received with CRC errors in the previous second.
long	Total number of packets received in the previous second that were too long. Currently, the maximum packet length is 2048 bytes.
ovrun	Total number of packets received in the previous second that could not be saved because there were not enough buffers.
inex	Total number of packets received in the previous second that were not a multiple of eight bits (after zero extraction).
abort	Total number of packets received in the previous second that were aborted by the reception of at least seven ones.
txund	Total number of packets transmitted in the previous second that were aborted because buffer chains were not ready in time. This status should always be zero since chained buffers are not used.
nopen	Total number of HDLC channels currently open. An HDLC channel corresponds to one or more TDM channels.

See Also: Modem, Show, Slot

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]`

Option	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 )
callroute                       ( diagnostic )
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 )
hdlc                           ( system )
help                            ( user )
if-admin                        ( diagnostic )
line                            ( system )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

To display help text about the Dir command, for example:

```
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 execute a command, the command is not displayed unless you specify the `-a` option. Commands with the User security level are always displayed. For detailed information, see “Auth” on page 1-9.

See Also: ?, Auth

If-Admin

Description: Displays information about or changes the state of an SNMP interface. Each device in the system has a unique SNMP interface number assigned to the device when a card is installed. Interface numbers are stored in NVRAM, which is not affected by system resets, so 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 | -?`

Option	Description
-a	List available SNMP interface numbers.
-d interface	Administratively down a specified SNMP interface
-l	List SNMP interface/device address mappings.
-u interface	Administratively bring up a specified SNMP interface.
-r interface	Reset an SNMP interface.
-?	Display a usage summary.

Example: To display a list of available SNMP interface numbers, specify the `-a` option:

```
admin> if-admin -a
Available SNMP interface numbers
      118 - infinity
```

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 bring up SNMP interface number 111:

```
admin> if-admin -u 111
interface 111 state change forced
```

IGMP

Description: Displays multicast information about Internet Group Membership Protocol (IGMP) groups and clients. The IGMP command applies only if the TAOS unit forwards multicast packets to members of multicast groups. It lists the members of groups to which the TAOS unit forwards multicast packets, and displays information about the groups.

Permission level: System

Usage: `igmp group | client | debug | hbdebug`

Keyword	Description
group	Display active multicast group addresses and interfaces.
client	Display multicast clients.
debug	Display IGMP debug information, such as statistics about queries to clients and replies from clients.
hbdebug	Display heartbeat messages.

Example: To display active multicast group addresses and interfaces for each group, specify the `group` argument:

```
admin> igmp group
IGMP Group address Routing Table Up Time: 0:0:22:17
Hash      Group Address  Members  Expire time  Counts
  N/A      Default route  * (Mbone)  .....      2224862
   10      224.0.2.250
                                2          0:3:24      3211 :: 0 S5
                                1          0:3:21      145  :: 0 S5
                                0 (Mbone)  .....      31901 :: 0 S5
```

The output contains the following fields:

Field	Description
Hash	Index to a hash table (displayed for debugging purposes only). N/A indicates that the Default route is not an entry in the hash table.
Group address	IP multicast address used for the group. An asterisk indicates the IP multicast address being monitored, meaning that members join this address by local application. The Default route is the MBONE interface (the interface on which the multicast router resides). If the TAOS unit finds that there is no member in a group, it forwards multicast traffic for the group to the MBONE interface.

Field	Description
Members	ID of each member of each multicast group. The zero ID represents members on the same Ethernet interface as the TAOS unit. All other IDs go to members of each group as they inform the TAOS unit that they have joined the group. If a client is a member of more than one group to which the TAOS unit forwards multicast packets, it has more than one multicast ID. The interface labeled Mbone is the interface on which the multicast router resides.
Expire time	When this membership expires. The TAOS unit sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the TAOS unit removes the entry from the table. If the field contains periods, this membership never expires. A string of periods means that the default route never times out.
Counts	Number of packets forwarded to the client, the number of packets dropped due to lack of resources, and the state of the membership. The state is displayed for debugging purposes.

To display a list of multicast clients, use the `client` argument:

```
admin> igmp client
IGMP Clients
Client      Version  RecvCount  CLU      ALU
0 (Mbone)   1        0          0        0
2           1        39         68       67
1           1       33310      65       65
```

The 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.
Version	Version of IGMP being used.
RecvCount	Number of IGMP messages received on that interface.
CLU	CLU is Current Line Utilization, and ALU is Average Line Utilization. Both indicate the percentage of bandwidth utilized across this interface. If bandwidth utilization is high, some IGMP packet types are not forwarded.
ALU	

Dependencies: This command is not applicable if IP multicast forwarding is not enabled.

IPcache

Description: Displays information about IP route caches. A route cache enables a slot card to route IP packets to another slot, reducing the route-processing overhead on the shelf controller. The shelf controller is still responsible for managing routing protocols and the route caches themselves, but each slot card is able to check a small IP cache and route packets to a destination slot. When a slot card receives an IP packet for which it has no cache entry, it forwards that packet to the shelf controller. The shelf controller routes it to the proper slot and writes a cache entry. The cache entry is downloaded to the route cache of all slot cards via the control bus.

Permission level: System

Usage: `ipcache [-r VRoutername] cache|debug|disable|enable`

Option	Description
-r VRoutername	The name of the Virtual Router (VRouter). If you do not specify a VRouter name, the system assumes the global VRouter.
cache	Display the cache.
debug	Turn on debugging.
disable	Disable the route cache. (Available only on slot cards.)
enable	Enable the route cache. (Available only on slot cards.)

Example: The following example shows command output on the shelf controller:

```
admin> ipcache cache
Hsh      Address      Gateway      Ifname      Sh/Sl/T      MTU
20       50.0.0.20        10.168.26.74 wan392      1/14/D      1524
40       20.0.0.40        20.0.0.40    ie1-3-1     1/3 /S      1500

Cache Limit 0 Cache Count 2 Cache over limit 0 No.packets 9

Mem Usage: Allocated 1k bytes
Free block count 22
```

The following example shows command output on a slot card:

```
admin> open 1 3
ether2-1/3> ipcache cache
Hsh Address      Gateway      Sh/Sl/T Switched MTU      MPath
0   99.1.1.1      10.168.21.30 1/14/D 0        1524    Y/0.0.0.0/0
20  50.0.0.20     10.168.28.170 1/15/D 85068    1524    Y/0.0.0.0/0
40  20.0.0.40     20.0.0.40    1/3 /S 0        1500    N
```

The shelf number is always 1. The T (Type) column following the shelf and slot numbers can specify D for dynamic cache entries or S for static cache entries. The MPath column indicates whether the cache entry is derived from multipath routes. If it represents a multipath route, the column indicates Y and the destination address. If it is not a multipath route, the column indicates N.

IP-Pools

Description: Displays the status of the IP address pools configured in the IP-Global profile.

Permission level: System

Usage: `ip-pools [VRoutername]`

Syntax element	Description
<code>-r VRoutername</code>	The name of the Virtual Router (VRouter). If you do not specify a VRouter name, the system assumes the global VRouter.

Example: When you enter the IP-Pools command with no arguments, the following type of output is displayed:

```
admin> ip-pools
Pool#           Base           Count      InUse
1                10.154.3.50       50         0
3                10.154.3.150      50         1
Number of remaining allocated addresses: 99
```

The sample output shows two configured pools, with the base address, address count, and number of addresses in use for each pool.

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|delete`

Syntax element	Description
<code>add</code>	Add an IP route to the routing table.
<code>delete</code>	Delete an IP route from the routing table.

Adding a static IP route to the routing table

To add a static IP route to the TAOS unit's routing table, use the IProute Add command.

```
iproute add [-r VRoutername] dest_IPaddr[/subnet_mask]
gateway_IPaddr[/subnet_mask] [pref] [metric]
```

Syntax element	Description
-r VRoutername	The name of the Virtual Router (VRouter). If you do not specify a VRouter name, the system assumes the global VRouter.
dest_IPaddr/subnet_mask	Destination network address and 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 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.

For example, consider the following command:

```
admin> iproute add 10.1.2.0/24 10.0.0.3/24 1
```

It 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).

If you try to add a route to a destination that is already in the routing table, the TAOS unit does not replace the existing route unless it has a higher metric than the route you attempt to add. If you get the message **Warning: a better route appears to exist**, the unit has rejected your attempt to add a route. Note that Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) updates can change the metric for the route.

Note: Any routes you add with the IProute Add command are lost when you reset the TAOS unit.

Deleting a static IP route from the routing table

To remove a static IP route from the TAOS unit's routing table, enter the IProute Delete command.

```
iproute delete [-r VRoutername] dest_IPaddr/subnet_mask
[gateway_IPaddr[/subnet_mask]]
```

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 and OSPF updates can add back any route you remove with IProute Delete. Also, the TAOS unit restores all routes listed in the IP-Route profile after a system reset.

Line

Description: Specifies that the upper-right or lower-right portion of the status window (or both) must display T1, E1, DS3, or Asynchronous Transfer Mode (ATM) 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]] | [-p]`

Option	Description
all	Display status information about all T1 lines.
enabled	Display status information only about enabled T1 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).
-p	Print line-status information at the command line.

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

```
admin> line top
```

```

2 Connections
001 tomw PPP 1/7/14 19200 SanFran+ 1/13/8 RA I.....
002 timl MP 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
48 out of 48 modems passed POST

Issued: 16:48:02, 09/27/2000
[Next/Last Conn <dn/up arw>, Next?Last Page: <pg dn/up>, Exit: <esc>]
```

To display a prompt below the status window, press the Escape key. To scroll through the list of lines, press the Up-Arrow or Down-Arrow key, or to page up or down through the lines, press the Page Up or Page Dn key. Line status information includes the following identifiers and codes:

- A line identifier in shelf/slot/line format. The shelf number is always 1.
- A two-character code indicating the line's link status.
- A single-character code indicating channel status. For an SS7 data trunk, this character code is always 7.
- A single-character code indicating channel type.

Following are the link-status codes:

Code	Description
LA (T1 lines) TE (E1 lines)	Link Active. The line is active and physically connected.
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, it is improperly configured, it has a very high error rate, or it is supplying inadequate synchronization.
YA	Yellow Alarm. The TAOS unit is receiving a Yellow Alarm pattern, which indicates that the other end of the line cannot recognize the signals the TAOS 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 TAOS unit to indicate that the line is currently inoperative.
DS	Disabled. The line might be physically connected, but the T1 or E1 profile specifies that it is inactive.

Following are the channel-status codes:

Code	Description
.	The channel is not available for one of the following reasons: <ul style="list-style-type: none"> • 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 (first E1 channel only).
*	The channel is connected in a current call.
-	The channel is currently idle (but in service).
@	The channel is disabled.
b	The channel is a backup NFAS D channel (T1 PRI only).
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 (inband signaling on T1 only).
d	The TAOS 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 nailed.
o	The channel is out of service (ISDN and SS7 only).
s	The channel is an active D channel (ISDN only).

Code	Description
h	The channel is on hold. ²
N	A Net2Net call is being dialed.
R	A Net2Net call is ringing.
	A Net2Netcall is connected.
D	A DTPT call is being dialed.
%	A DTPT call is connected.

Following are the channel-type codes:

Code	Description
T	T1 inband signaling
I	T1 PRI signaling
P	Non-Facility Associated Signaling (NFAS) Primary
S	NFAS Secondary
N	All other NFAS types

Following are the status indications for DS3-ATM lines:

Status indicator	Meaning
(blank)	DS3-ATM profile does not exist.
DS	DS3-ATM profile disabled.
LA	Link Active.
LS	Loss Of Signal.
LF	Loss Of Frame.
YA	Yellow Alarm Receive.
1S	Alarm Indicator Signal (AIS) Receive.

Following are the status indications for OC3-ATM lines:

Status indicator	Meaning
(blank)	OC3-ATM profile does not exist.
DS	OC3-ATM profile disabled.
LA	Link Active.
LS	Loss Of Signal.
LF	Loss Of Frame.
YA	Yellow Alarm Receive.
1S	Alarm Indicator Signal (AIS) Receive.

With the **-p** option, the Line command displays line status information directly to screen. For example, the following is sample output for T1 lines:

```
admin> line -p
Address Line State CARR LOOP DS0 Channel Status      Signaling Type
1/01/01 ACTIVE      --  LOOP ..... inband
1/01/02 RED ALARM  LOC  -- ..... r1-inband
1/01/03 ACTIVE      --  --  ----- inband
1/01/04 RED ALARM  --  --  ..... isdn-nfas
1/01/05 RED ALARM  LOC  --  ..... inband
1/01/06 DISABLED   --  --  @@@@@@@@ @@@@@@@@ @@@@@@@@ inband
1/01/07 DISABLED   --  --  @@@@@@@@ @@@@@@@@ @@@@@@@@ inband
1/01/08 DISABLED   --  --  @@@@@@@@ @@@@@@@@ @@@@@@@@ inband
```

Following is sample output for E1 lines:

```
admin> line -p
Address Line State CARR LOOP DS0 Channel Status      Signaling Type
1/14/01 ACTIVE      --  --  .----- s----- el-indian-signa
1/14/02 RED ALARM  LOC  --  ..... el-dpnss-signal
1/14/03 ACTIVE      --  --  .----- s----- el-indian-signa
1/14/04 DISABLED   --  --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
1/14/05 DISABLED   --  --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
1/14/06 DISABLED   --  --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
1/14/07 DISABLED   --  --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
1/14/08 DISABLED   --  --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
```

The command displays the following line status information:

Output field	Description
Address	Shelf/Slot/Line number of the line. The shelf number is always 1.
Line State	Status of the line. The LB line-state indicator specifies that an E1 line is looped back via the <code>fe-loop</code> command.
CARR	Carrier. If the system detects a loss of carrier on a line, LOC is displayed. If the line sees carrier, it displays dashes (--).
LOOP	Loopback status. If the line is locally looped, LOOP is displayed. Otherwise, the column contains dashes (--).
DS0 Channel Status	State of the individual DS0 lines.
Signaling Type	The type of signaling in use on the line.

See Also: Connection, Log, Status, T1channels, 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 (“closing” the subprofile). The List command works only on the working profile.

Permission level: System

Usage: **list** [...] [**param-name** [**param-index**] [**sub-profile**]]

Option	Description
.. (two periods)	Close the current subprofile and return to the previous higher context.
param-name	A parameter in the current context. If the parameter is in a subprofile, you must specify the subprofile name first.
param-index	Complex parameters have an index. For example, the Interface-Address parameter contains both the physical-address and logical-item indexes.
sub-profile	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 = mpp
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 "" "" +
ppp-options = { ***** ***** stac 1524 no 600 600 }
mp-options = { 1 1 2 }
mpp-options = { "" quadratic transmit 1 1 15 5 10 70 }
tcp-clear-options = { "" 0 }
answer-options = { }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
```

To list the PPP-Options subprofile:

```
admin> list ppp
[in CONNECTION/dallas:ppp-options]
send-password = *****
recv-password = *****
enabled = yes
link-compression = stac
mru = 1524
lqm = no
disconnect-on-auth-timeout = yes
lqm-minimum-period = 600
lqm-maximum-period = 600
```

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

```
admin> list ..
```

To use the List command to display the Answer-Options subprofile:

```
admin> list .. answer
[in CONNECTION/dallas:answer-options]
profile-required = no
ans-default = no
profile-source = no
clid-auth-mode = ignore
```

Dependencies: 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 might be located on the disk of the PC you are using for the terminal session with the TAOS unit or on a network host that supports TFTP.

Permission level: Update

Usage: `load [-v][-l | -t][-e password] load-type [-subtype] source [device]`

Syntax element	Description
-v	Display verbose output for configuration loads.
-l (APX 8000 units only)	Load the code on the local controller without synchronizing the code image with the peer controller. If you do not use the -l option, the system automatically attempts to synchronize code with the peer controller after loading code onto its own flash memory or PCMCIA. This behavior is common on both the primary and secondary controllers.
-t (APX 8000 units only)	Transfer the image from this controller to the peer controller after the download is complete.
-e <i>password</i>	Use encryption. The <i>password</i> argument specifies the password used to generate the key for encryption and decryption. The -e option supports only a network target. The system restores the configuration by applying the same encryption it used to save it (either DES or MD5).

Syntax element	Description
<i>load-type</i>	<ul style="list-style-type: none"> <code>amdm</code>—code for an Analog Modem card <code>boot-sr</code>— shelf-router boot load <code>config</code>— configuration file <code>csmx</code>—code for a Series56™ II card <code>csmv</code>—code for a Series56 III card <code>ds3-atm</code>—code for a DS3-ATM card <code>ds3-atm2</code>—code for a DS3-ATM2 card <code>e1-8</code>— code for an E1 card <code>enet2</code>—code for an Ethernet-2 card <code>enet3</code>—code for an Ethernet-3 card <code>hdlc2</code>—code for a Hybrid Access™ II card <code>hdlc2ec</code>—code for a Hybrid Access III card <code>madd</code>—code for a 48-port MultiDSP card <code>sr</code>— shelf-router runtime load (resides in onboard flash memory) <code>stm0</code>—code for an STM-0 card <code>swan</code>— code for a Serial WAN (SWAN) card <code>t1-8</code>— code for a T1 card <code>t3</code>—code for a T3 card <code>tar</code>—a tar file containing all slot card code images <code>uds3</code>—code for an unchannelized DS3 card <code>ue1</code>—code for an E1 FrameLine card <code>unchan-t1</code>—code for a T1 FrameLine card
<i>-subtype</i>	<p>The subtype of the image:</p> <ul style="list-style-type: none"> <code>-normal</code> (for regular image, the default) <code>-debug</code> (for debugging image) <code>-diagnostic</code> (for diagnostic image) <p>The Load command supports subtype alignment, which enables you to change the subtype of the image. For example, if you load an image whose header specifies that it is a normal image, but you specify the <code>-debug</code> subtype, the image saved in flash memory has a subtype of Debug instead of Normal.</p>
<i>source</i>	<p>The location from which the file will be loaded:</p> <ul style="list-style-type: none"> <code>network host filename</code>—After typing the word <code>network</code>, you can specify a hostname or IP address and the name of the file on a TFTP host. The maximum size of the file you can load is 16 Mb. <code>console</code>—The PC connected to the TAOS unit by means of the serial port.

Syntax element Description

device The name of the flash card to load. The valid device names are:

- [flash-card-]1
- [flash-card-]2

The [flash-card-]1 value is the default. Note that device names can be abbreviated as 1 and 2.

The syntax of the `load tar` command enables you to specify multiple filenames:

```
load tar network host file1.tar [file2.tar] [...] [flash-card-id]
```

TAOS slot-card images are provided in two tar files. The first tar file contains the most commonly used slot-card images (Table 1-1).

Table 1-1. Slot-card images in first tar file

Filename	Contents	
	Description	Slot-card images
tntrel.tar	Shelf controller	tntsr
	Ethernet	tntenet2 tntenet3 tntenet3nd
	HDLC	tnthdlc2 tnthdlc2ec
	T1-specific images	tnt8t1 tntt3 tntut1 tntpctfit
	MAX TNT modem images	tntcsmx tntcs3v tnt-madd tntmdm56k
tntrele.tar	Shelf controller	tntsre
	Ethernet	tntenet2 tntenet3 tntenet3nd
	HDLC	tnthdlc2 tnthdlc2ec
	E1-specific images	tnt8e1 tntue1 tnt-pct-fie
	MAX TNT modem images	tntcsmx tntcs3v tnt-madd tntmdm56k

Table 1-1. Slot-card images in first tar file (continued)

Filename	Contents	
	Description	Slot-card images
apxrel.tar	Shelf controller	apxsr
	Ethernet	tntenet2 tntenet3 tntenet3nd
	HDLC	tnthdlc2 tnthdlc2ec
	T1-specific images	tnt8t1 tntt3 tntut1 tntpctfit
	APX 8000 modem images	tntcsmx tntcsm3v tnt-madd
apxrele.tar	Shelf controller	apxsre
	Ethernet	tntenet2 tntenet3 tntenet3nd
	HDLC	tnthdlc2 tnthdlc2ec
	E1-specific images	tnt8e1 tntue1 tnt-pct-fie
	APX 8000 modem images	tntcsmx tntcsm3v tnt-madd

The second tar file contains images for slot cards that are less commonly used (Table 1-2).

Table 1-2. Slot-card images in second tar file

Filename	Contents	
	Description	Slot-card images
tntrel2.tar	T1-specific images	tntstm0 tntuds3 tntds3atm tntds3atm2 tntoc3atm
	MAX TNT modem	tntamdm
	Serial WAN	tntswan
tntrele2.tar	E1-specific images	tnte3atm
	MAX TNT modem	tntamdm
	Serial WAN	tntswan

Table 1-2. Slot-card images in second tar file (continued)

Filename	Contents	
	Description	Slot-card images
apxrel2.tar	T1-specific images	tntstm0 tntuds3 tntds3atm tntds3atm2 tntoc3atm
	Serial WAN	tntswan
apxrele2.tar	E1-specific images	tnte3atm
	Serial WAN	tntswan

If the unit does not contain any of the slot cards supported in the second tar file, load only the first tar file. For example:

```
admin> load tar network 10.10.10.10 tntrel1.tar
```

If the unit contains slot cards supported in the second tar image, both files *must* be loaded on the same command line. For example:

```
admin> load tar network 10.10.10.10 tntrel1.tar tntrel2.tar
```

The system loads only the images required for slot cards installed in the system.



Caution: Do not load the second tar file alone. Loading the second tar file without the first tar file causes the system to delete necessary images from flash memory. Should such an event occur, enter the load command again, specifying both tar files on the command line.

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

```
admin> load config network 10.8.7.2 maxtnt.cfg
```

To load a software update for a T1 card from the PC you are using to flash-card-2:

```
admin> load t1-8 console 2 tntt1.ffs
```

When used to load a tar file, the Load command lists the filename of each code image in the file as the image is being extracted. For example:

```
admin> load tar network 10.10.10.10 tntrel1.tar
file tntrel1.tar...
untaring and loading image for...
shelf controller (tntsr/tntsr.ffs)...
8t1-card (tnt8t1/tnt8t1.ffs)...
skipping t3-card (tntt3/tntt3.ffs)...
skipping 4ether2-card (tntenet2/tntenet2.ffs)...
skipping hdlc2-card (tnthdlc2/tnthdlc2.ffs)...
skipping 4swan-card (tntswan/tntswan.ffs)...
done.
```


With the following command, the system loads the new boot loader to both controllers on an APX 8000 unit:

```
admin> load boot net 10.10.10.10 apxsrb.bin
loading code from 10.10.10.10
file apxsrb.bin...
done.

Attempting to write image(s) to other controller Transferring boot
image 2...
done.
```

With the following command, the system loads the boot loader to only the local controller (which can be either the primary or secondary controller):

```
admin> load -l boot net 10.10.10.10 apxsrb.bin
loading code from 10.10.10.10
file apxsrb.bin...
done.
```

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

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

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

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

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

Finally, the following error messages can also appear when you use the Load command:

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

The following error messages apply to DES encryption for configuration file transfer over TFTP:

`-e option:unknown encryption method method`

You specified an incorrect encryption method when you saved the configuration.

File is corrupted, Encryption tag not found

File is corrupted, Version tag not found

The configuration file is corrupted.

Wrong encryption password!!

Configuration is encrypted but the password is incorrect.

Configuration is encrypted

Configuration is encrypted but no password was provided.

Configuration is not encrypted!!

Configuration is not encrypted but a password was provided.

Encrypted protocol <ver> not supported!!

Encryption version mismatch occurred.

Dependencies: You can set parameters in the Load-Select profile to specify which slot-card images to load to flash memory when you use a Load Tar command. An explicit Load command for a particular card 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.

See Also: Dircode, Format, Fsock, Save

Log

Description: Specifies that the upper-right or lower-right portion of the status window (or both) must display a message from the TAOS 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 TAOS 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]]`

Option	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.

Option	Description
-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.

Example: With the `-p` option, the Log command displays the system log with the most recent log entry first. The following is sample output:

```
admin> log -p
```

Time	Date	Source	Level	Description
11:11:25	10/16/2000	shelf-1/controller	notice	Slot 1/10, state UP 2
11:11:20	10/16/2000	shelf-1/slot-10	info	Software version 9.0.0
11:11:20	10/16/2000	shelf-1/slot-10	info	Card serial number 914694348
11:10:15	10/16/2000	shelf-1/controller	notice	Slot 1/5, state UP 2
11:10:10	10/16/2000	shelf-1/slot-5	notice	100BaseT: Link down
11:10:10	10/16/2000	shelf-1/slot-5	notice	iel-5-3: Link down
11:10:10	10/16/2000	shelf-1/slot-5	notice	iel-5-2: Link down
11:10:10	10/16/2000	shelf-1/slot-5	notice	iel-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 PPP 1/7/14 19200	Serial number: 6201732 Version: 1.0F
002 timl MP 1/7/3 56000	
	Rx Pkt: 11185897
	Tx Pkt: 42460
	Col: 129
	09/26/2000 12:20:15 Up: 3 days, 21:47:32
	M: 29 L: info Src: shelf-1/controller
	48 out of 48 modems passed POST
	Issued: 16:48:02, 09/27/2000

[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:

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.

Level	Description
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 unit 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:

Informational message	Description
48 out of 48 modems passed POST	All of the modems on a card passed the power-on self test.
Incoming call	A call has been received but not yet routed.
Outgoing call	The TAOS unit has dialed a call.
Added Bandwidth	The TAOS unit has added bandwidth to an active call.
Ethernet up	The Ethernet interface has been initialized and is running.
LAN session up	A PPP session has been established.
LAN session down	A PPP session has been terminated.
Assigned to port	The TAOS 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 TAOS unit has removed bandwidth from an active call.
RADIUS config error	The TAOS 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
Busy	The phone number was busy when the call was dialed.
No connection	The remote end did not answer when the call was dialed.
Network problem	There are problems in the WAN or in the line configuration. The D channel might be getting an error message from the switch, or the telco might be experiencing a problem.
Call disconnected	The call has ended unexpectedly.
Far end hung up	The remote end terminated the call normally.
Incoming glare	The TAOS unit could not place a call because it saw an incoming <i>glare</i> signal from the switch. If you receive this error message, you have probably selected incorrect Line profile parameters. Check the Robbed-Bit-Mode setting.
LAN security error	A PPP session has failed authentication, another session by the same name already exists, or remote authentication timed out.
Call Refused	An incoming call could not be connected.

Press the Escape key to display a prompt below the status window. Then, to close the status window, enter the Status command:

```
admin> status
```

See Also: Connection, Line, Screen, Status, View

LS

Description: Lists files and directories on a flash card.

Permission level: System

Usage: `ls [socket [/path]]`

Option	Description
<i>socket</i>	Specify the flash card number.
<i>/path</i>	Specify a subdirectory on the flash card.

Example: To list the /current subdirectory on flash card 1, you would enter the following:

```
admin> ls 1/current
ls Flash card 1/current:
/current:
    tntsr.ffa                1859325 Mon Mar 13 11:29:26 2000 Version
9.0.0
    tnt8t1.ffa                272179 Mon Mar 13 11:29:32 2000 Version
9.0.0
```

See Also: Mkdir, MV, RM

Mkdir

Description: Creates a new directory.

Permission level: System

Usage: `mkdir socket/path`

Option	Description
<i>socket</i>	Specify the flash card number.
<i>path</i>	Specify a subdirectory on the flash card.

Example: To create the directory test on flash card 1, you would enter the following:

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

See Also: LS, MV, RM

Modem

Description: Displays information about digital modems in the TAOS unit.

Permission level: System

Usage: `modem -a | -d | -f | -g | -i | -m | -s`

Option	Description
-a	Display all available modems.
-d	Display disabled modems.
-f	Display failed or nonexistent modems.
-g	Display available good modems.
-i	Display in-use modems.
-m	Display all possible modems.
-s	Display suspect modems.

Example: To display all the good modems that are available for use, use the `-g` option:

```
admin> modem -g
Non-suspect modems available for use:
      (dvOp  dvUpSt  dvRq  sAdm  mDis )
Modem { 1 11  1 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11  2 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11  3 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11  4 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11  5 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11  6 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11  7 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11  8 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11  9 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11 10 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11 11 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11 12 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11 13 } (Up   Idle   UP   UP   ENABLE )
Modem { 1 11 14 } (Up   Idle   UP   UP   ENABLE )

[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

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

Column Description

dvOp	<p>The current operational state of the modem (also specified by Device-State):</p> <ul style="list-style-type: none"> Down indicates that the modem is in a nonoperational state. Up indicates that the modem is in normal operations mode.
dvUpSt	<p>The status of the modem in normal operations mode:</p> <ul style="list-style-type: none"> Idle indicates that the modem is not handling a call. Active indicates that the modem is handling a call.
dvRq	<p>The required state of the modem as specified by the Req'd-State setting:</p> <ul style="list-style-type: none"> Down indicates that the modem is required to be in a nonoperational state. Up indicates that the modem is required to be in normal operations mode.
sAdm	<p>The desired administrative state of the modem (also specified by Desired-State):</p> <ul style="list-style-type: none"> Down specifies that the modem should terminate operations and enter the down state. Up specifies that the modem should come up in normal operations mode. <p>The actual state of the modem 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 force a modem to the new state. It indicates that the TAOS unit should change the modem state gracefully.</p>
mDis	<p>Modem disable mode (as indicated by the LAN-Modem profile):</p> <ul style="list-style-type: none"> Enable specifies that the modem is operational. Disable specifies that the modem has been disabled.

See Also: Open, Show, Slot

MV

Description: Moves a file or directory.

Permission level: System

Usage: `mv socket1/path1 socket2/path2`

Option	Description
<i>socket1</i>	Specify the number of the flash card on which <i>path1</i> is found.
<i>socket2</i>	Specify the number of the flash card on which <i>path2</i> is found.
<i>path1</i>	Specify the file and/or directory to be moved.
<i>path2</i>	Specify the file and/or directory that replaces <i>path1</i> .

Example: To replace the /test1 directory on flash card 1 with the /test2 directory, you would enter the following:

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

See Also: LS, Mkdir, RM

Netstat

Description: Displays the TAOS unit's interface and routing tables, protocol statistics, and active sockets.

Permission level: System

Usage: `netstat [VRoutername] [-i] [-r[host]] [?] [-n | -d]
[-s identifiers] [-z]`

Option	Description
no arguments	Display UDP and TCP statistics.
<i>VRoutername</i>	The name of the Virtual Router (VRouter). If you specify a VRouter name, the command returns statistics only for the specified VRouter. If you do not specify a VRouter name, the system assumes the global VRouter.
-i	Display the IP interface table.
-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. This option is the default.
-d	Display symbolic names rather than numeric addresses.

Option	Description
-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. The valid identifiers are <code>udp</code> , <code>tcp</code> , <code>icmp</code> , <code>ip</code> , <code>igmp</code> , and <code>mcast</code> .
-z	Display Zombie routes created for 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 router to flush this route from their tables.

Displaying UDP and TCP statistics

To display both UDP and TCP statistics, do not specify any options. For example:

```
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
1/8	0	8	0	256	0		0
1/8	1	1019	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 contains the following information:

Column	Description
Socket	The shelf, slot, and socket corresponding to a local UDP or TCP port. The shelf number is always 1.
Local Port	The port on which the TAOS unit is listening for UDP packets.
InQLen	The number of packets in the input queue for the socket. The packets are waiting to be processed.
InQMax	The maximum number of packets that can reside in the input queue for the socket. A value of 0 (zero) means no limit. The TAOS unit drops excess packets.

Column	Description
InQDrops	The number of packets dropped from the input queue because the value of InQMax was reached.
Total Rx	The total number of packets received on the socket, including dropped packets.
Local	The 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 TAOS unit is listening for the start of a TCP session.
Remote	The 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 TAOS unit is listening for the start of a TCP session.
State	<p>The state of the session. The possible state values are:</p> <p>CLOSED—The socket is not in use.</p> <p>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.</p> <p>SYN_SENT—The socket is trying to establish a connection.</p> <p>SYN_RECEIVED—The connection is being synchronized.</p> <p>ESTABLISHED—The connection is established.</p> <p>CLOSE_WAIT—The remote side has shut down the connection, and the TAOS unit is waiting for the socket to close.</p> <p>FIN_WAIT_1—The socket is closed, and the TAOS unit is shutting down the connection.</p> <p>CLOSING—The socket is closed. The TAOS unit is waiting for acknowledgment that the remote end has shut down.</p> <p>LAST_ACK—The remote end has shut down and closed the socket, and it is waiting for an acknowledgment from the TAOS unit.</p> <p>FIN_WAIT_2—The socket is closed, and the TAOS unit is waiting for the remote end to shut down the connection.</p> <p>TIME_WAIT—The socket is closed, and the TAOS unit is waiting for a remote-shutdown retransmission.</p>

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
TACACS+	49
Finger	79

Displaying the interface table

The TAOS unit's interface table shows the address of each interface. To display the interface table, specify the `-i` option:

```
admin> netstat -i
```

The entries in the interface table associated with the TAOS unit's Ethernet interfaces use the following naming convention:

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

The shelf number is always 1.

For example, the following output shows an Ethernet-2 card 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 columns in the interface table contain the following information:

Column	Description
Name	<p>The name of the interface:</p> <ul style="list-style-type: none"> <code>ie0</code> or <code>ie[shelf]-[slot]-[item]</code> is an Ethernet interface. The shelf number is always 1. <code>lo0</code> is the loopback interface. <code>rj0</code> is the reject interface, used in network summarization. <code>bh0</code> is the blackhole interface, used in network summarization. <code>wanN</code> is a WAN connection, entered as it becomes active. <code>wanabe</code> indicates an inactive RADIUS dial-out profile.
MTU	(Maximum Transmission Unit) The maximum packet size allowed on the interface.
Net/Dest	The network or the target host this interface can reach.

Column	Description
Address	The address of this interface.
Ipkts	The number of packets received.
Ierr	The number of packets that contain errors.
Opkts	The number of packets transmitted.
Oerr	The number of transmitted packets that contain errors.

Displaying the routing table

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

```
admin> netstat -r
```

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

```

48610
11.168.6.0/24      11.168.6.96    ie1-12-1  *RGTM  100    8      0
48624
11.168.6.102/32   11.168.6.86    ie1-12-1  RGT     100    8      0
48601
11.168.6.115/32   11.168.6.116   ie1-12-1  RGT     100    8      0
48606
255.255.255.255/32-      ie0            CP        0      0      0
48630

```

The columns in the routing table contain the following information:

Column	Description
Destination	The route's target address. To send a packet to this address, the TAOS unit uses this route. If the target address appears more than once in the routing table, the TAOS unit uses the most specific route (having the largest subnet mask) that matches that address.
Gateway	The next hop router that can forward packets to the given destination. Direct routes (without a gateway) show a hyphen in this column.
IF	The name of the interface through which to send packets over this route: <ul style="list-style-type: none"> ie0 or ie[shelf]-[slot]-[item] is an Ethernet interface. The shelf number is always 1. lo0 is the loopback interface. rj0 is the reject interface, used in network summarization. bh0 is the blackhole interface, used in network summarization. wanN is a WAN connection, entered as it becomes active. wanabe indicates an inactive RADIUS dial-out profile. local indicates a single route targeted at the local machine. mcast indicates a route to a virtual device. The route encapsulates the multicast forwarder for the entire class D address space.
Flg	One or more of the following flags: <ul style="list-style-type: none"> C—a directly connected route, such as Ethernet I—an ICMP redirect dynamic route N—placed in the table via SNMP MIB II O—a route learned from OSPF R—a route learned from RIP r—a transient RADIUS-like route S—a static route ?—a route of unknown origin, which indicates an error G—an indirect route via a gateway P—a private route T—a temporary route M—a multipath route *—a backup static route for a transient RADIUS-like route

Column	Description
Pref	The preference value. See the description of the Preference parameter for information about defaults for route preferences.
Metric	A RIP-style metric for the route, with a range of 0-16. Routes learned from OSPF show a RIP metric of 10. OSPF cost-infinity routes show a RIP metric of 16.
Use	A count of the 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	The age of the route in seconds. RIP and ICMP entries are aged once every 10 seconds.

Displaying protocol statistics

You can include identifiers in the command line to display IP, UDP, TCP, ICMP, IGMP, and multicast protocol statistics. The system displays TCP statistics collected from slot cards as well as the shelf controller. All other types of statistics are collected for the shelf controller only. The following example contains 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
    0 disconnects while awaiting transmission
```

Note: There is no support for IP multicast on per-VRouter basis, so the IGMP and MCast statistics relate only to the global Virtual Router (VRouter).

See Also: NSlookup, Ping, Rlogin, Traceroute

Netware

Description: Displays IPX network and server information, data on IPX pings, and IPX statistics.

Permission level: User

Usage: **netware** [*Vroutername*] [**-n** | **-p** | **-s** | **-t**]

Option	Description
Vroutername	VRouter for which you want to display IPX network and server information.
-n	Display information about IPX networks, including the next router to each network, and the associated hop and tick count.
-p	Display the IPX ping packets transmitted and received by the TAOS unit.
-s	Display information about IPX servers that can be accessed from the TAOS unit, including the IPX address and server name, and the number of hops to the server.
-t	Display IPX statistics about received, forwarded, and dropped packets, along with statistics about packets with no associated route.

Example: To display IPX statistics, enter **netware -t**:

```
admin> netware -t
      3000 packets received.
      1500 packets forwarded.
      15 packets dropped exceeding maximum hop count.
      0 outbound packets with no route
```

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. However, depending on the profile type, the index chosen might affect the factory default values set in the profile. (For details, see page 1-77.)

Permission level: System

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

Syntax element	Description
profile-type	The type of profile you want to create.
profile-index	The 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 t1 {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 t1 {1 2 3}
T1/{ shelf-1 slot-2 3 } read

admin> list
[in T1/{ shelf-1 slot-2 3 } (new)]
physical-address* = { shelf-1 slot-2 3 }
line-interface = { no d4 ami eligible middle-priority inband +
```

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 = mpp
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 +
ppp-options = { "" "" stac 1524 no 600 600 }
mp-options = { 1 1 2 }
mpp-options = { "" quadratic transmit 1 1 15 5 10 70 }
tcp-clear-options = { "" 0 }
answer-options = { }
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 or Virtual Router (VRouter) by performing a Domain Name System (DNS) lookup.

Permission level: Diagnostic

Usage: `nslookup [-r Vroutername] [-s DNS_server] [-v] hostname`

Syntax element	Description
-r Vroutername	VRouter for which you want to obtain an IP address.
-s DNS_server	Specifies the IP address of the DNS server that the TAOS unit uses to resolve the hostname or VRouter name. If you do not specify the <code>-s</code> option, the system uses the DNS server that you configured locally.
-v	Specifies that the unit prints the details of the packet received from the DNS server.
hostname	Hostname for which you want to obtain an IP address.

Example: To look up the IP address of host-231 by means of the DNS server at 10.65.12.10:

```
admin> nslookup -s 10.65.12.10 host-231
Resolving host host-231.
IP address for host host-231 is 10.65.12.231.
```

Dependencies: Unless you use the `-s` option, your unit must be configured with the address of at least one DNS server.

See Also: ARPtable, Netstat

NVRAM

Description: Provides functions for managing or clearing onboard nonvolatile random access memory (NVRAM), and resets one or both redundant shelf controllers. The onboard NVRAM stores the system configuration. Clearing NVRAM initializes the system. It comes 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: **nvr**am [-f | -t | -u | -c | -?] [-r *controller*]

Option	Description
No options	Clear NVRAM. On an APX 8000 unit, using the NVRAM command with no options clears the memory of both redundant controllers, but only when you are logged in to the primary controller. (The primary controller continues to be primary.) If you are logged in to the secondary controller, the operation affects only the secondary controller. The secondary controller cannot clear the memory of the primary controller.
-f	Clear NVRAM as described in the previous entry, but without prompting for confirmation.
-t	Toggle module debug level.
-u	Display NVRAM usage statistics.
-c	Compact the NVRAM storage.
-?	Display a usage summary.
-r <i>controller</i>	Clear NVRAM and reboot one or both redundant controllers. For <i>controller</i> , you can specify one of the following: primary —Clear NVRAM and reboot the primary controller. secondary —Clear NVRAM and reboot the secondary controller. both —Clear NVRAM and reboot controllers.

Example: To display memory usage information, specify the **-u** option:

```
admin> nvr
```

If you are logged in to the primary controller of a system with dual controllers, the following command clears the memory of the secondary controller:

```
admin> nvr
```

The following command clears the memory of the primary controller:

```
admin> nvr
```

The following command clears nonvolatile RAM for the entire system:

```
admin> nvr
Clear configuration of Both controllers and reboot? [y/n] y
```

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

See Also: Load, Save, Reset

OAMloop

Description: Sends ATM Operation-And-Maintenance (OAM) loopback cells on an ATM interface.

Permission level: Diagnostic

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

Argument	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, which is in seconds. If this argument is not specified, the interval defaults to one second.
shelf	The shelf number is always 1.
slot	Specifies the slot in which the DS3-ATM card is located.
port	Specifies the port to use for the looped-back cells.
vpi	Specifies the Virtual Path Identifier (VPI) on which to transmit the looped-back cells.
vci	Specifies the Virtual Channel Identifier (VCI) on which to send the looped-back cells.

Example: Following is an example of an OAMloop command line and resulting 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
```

Open

Description: Each slot card has its own processor, memory, operating system, and set of debug commands. The Open command sets up a Telnet-like session across the control bus to one of the slot cards. Then you can execute commands on that slot card.

Permission level: Diagnostic

Usage: `open shelf [slot]`

Syntax element	Description
<i>shelf</i>	The shelf number (always 1).
<i>slot</i>	The number of the expansion slot you want to diagnose.

To open a session with a T1 card installed in slot 13:

```
admin> open 1 13
```

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

```
t1-1/13> ?
?                ( user )
auth             ( user )
cbcardif         ( debug )
checkd           ( debug )
clear            ( user )
clock-source     ( diagnostic )
debug            ( diagnostic )
fe-loop          ( diagnostic )
help             ( user )
open             ( diagnostic )
pools            ( debug )
priDisplay       ( diagnostic )
quit             ( user )
version          ( system )
whoami           ( user )
```

To return to the shelf controller:

```
t1-1/13> 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: Diagnostic

Usage: `ospf [options]`

where **options** can be one or more of the following:

Option	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 NSSA border routers.
<code>lsa area ls-type ls-id ls-orig</code>	<p>Display detailed information about OSPF Link-State Advertisements (LSAs).</p> <p>area is the area ID.</p> <p>ls-type is the LSA type. You can specify one of the following options for ls-type:</p> <ul style="list-style-type: none">• rtr (Type 1) is a router-LSA that describes the collected states of the router's interfaces.• net (Type 2) is network-LSA that describes the set of routers attached to the network.• sum (Types 3 and 4) describes routes to networks in remote areas, or AS boundary routers. <p>ls-id is the target address of the router.</p> <p>ls-orig is the address of the advertising router.</p>
<code>lsdb [area]</code>	Display an OSPF link-state database summary for an area. If you do not specify the area option, the summary for the first configured area (or for the only defined area) is displayed. If you specify the area option, the unit displays a summary for the specified area. The area 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 (AS) advertisements.
<code>rtab</code>	Display OSPF routing table.
<code>database ext</code>	Display OSPF database summary.

Option	Description
internal	Display OSPF internal routes.

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 Link State Advertisements (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 AS boundary routers.
AS External-LSAs (type-5)	Number of AS external 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.
Type 2 external routes	Number of external type-2 routes that are typically outside the scope of OSPF-IGP.

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 TAOS unit interfaces specified in the area.
#nets	Number of reachable networks in the area.
#rtrs	Number of reachable routers in the area.
#brdrs	Number of reachable area border routers in the area.
#intnr	Number of reachable internal routers in the area.

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 TAOS unit, which is typically the address specified for the Ethernet interface.
AS boundary capability	Yes if the TAOS unit functions as an ASBR or No if it does not function as an ASBR.
Attached areas	Number of areas to which this TAOS unit attaches.
Estimated # ext.(5) routes	Number of ASE-5 routes that the TAOS unit can maintain before it goes into an overload state.
OSPF packets rcvd	Total number of OSPF packets received by the TAOS unit.
OSPF packets rcvd w/ errs	Total number of OSPF errored packets received by the TAOS 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 TAOS unit allocates memory in blocks. The TAOS unit allocates queue headers from the memory blocks. When the unit frees all queue headers from a specific memory block, the TAOS unit returns the block to the pool of available memory blocks.
# Dijkstra runs	Number of times that the TAOS unit has run the Dijkstra algorithm (short path computation).
Incremental summ. updates	Number of summary updates that the TAOS 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 TAOS unit performs.
Buffer alloc failures	Number of buffer allocation problems that the TAOS 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 TAOS unit has aged and removed from its tables.

Field	Specifies
LS adv. flushed	Number of LSAs that the TAOS 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.

Displaying information about OSPF interfaces

To display either summarized information about all OSPF interfaces or specific information about a single interface, include the `intf` option with the OSPF command.

Displaying summarized information

To display summarized information on OSPF interfaces, enter the following command:

```
admin> ospf intf
```

Ifc Address	Phys	Assoc. Area	Type	State	#nbrs	#adjs	DInt
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 TAOS unit's Ethernet interface. To identify WAN links, use the Type and Cost fields.
Phys	Name of the interface or the Connection profile for WAN links.
Assoc. Area	Area in which the interface resides.
Type	Point-to-Point (P-P) or Broadcast (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 TAOS unit waits for a router update before removing the router's entry from its table. The interval is called the Dead Interval.

Displaying specific information about a specific interface

To display detailed information for a specific interface, enter the following command:

```
admin> 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 adjs.:   1
# Mcast floods: 1856 # Mcast acks:    1855
```

The fields in the output contain the following information:

Field	Specifies
Interface Address	IP address of the TAOS 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 TAOS unit sends Hello packets.
Rxmt interval	Retransmission interval.
Dead interval	Number of seconds that the TAOS 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.
Max pkt size	Maximum size of a packet that the TAOS unit can send to the interface.

Field	Specifies
TOS 0 cost	Type of Service normal (0) cost.
# neighbors	Number of neighbors.
# adjacencies	Number of adjacencies.
# Full adjs.	Number of fully-formed adjacencies.
# Mcast floods	Number of multicast floods on the interface.
# Mcast acks	Number of multicast acknowledgments on the interface.

Displaying OSPF link-state advertisements

To specify a link-state advertisement 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 AS-external-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, enter the following command:

```
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 Link-State Advertisement.
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.
cksum	Checksum for the LSA.
Net mask	Subnet mask of the LSA.
Tos	Type of Service 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)

Field	Specifies
Forwarding Address	Forwarding Address of the LSA (described in RFC 1583).
Tag	Tag of the LSA (described in the OSPF RFC).

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 TOS 0 are calculated.
LS type	Type of link as defined in RFC 1583: <ul style="list-style-type: none"> • 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 AS boundary routers. • Type 5 (ASE) are AS-external-LSAs that describe routes to destinations external to the AS. A default route for the AS can also be described by an AS-external-LSA.
LS ID (destination)	IP address of the advertisement's destination.

Field	Specifies
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 Autonomous System Border Router (ASBR) or Area Border Router (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: <ul style="list-style-type: none"> • TrnsNetwork (Transit Network)—A network that carries traffic that does not have its source or destination in the network itself. • Stub (Stub Network)—A network in which all external routes are summarized by a default route. • P-P (Point-to-Point)—A link over a serial line.
No. of metrics	Metric for TOS 0.
TOS	Type of Service 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.

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: <ul style="list-style-type: none"> 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 AS boundary routers. Type 5 (ASE) are AS-external-LSAs that describe routes to destinations external to the AS. A default route for the AS can also be described by an AS-external-LSA.
LS ID (destination)	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.

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: <ul style="list-style-type: none">• 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 AS 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.

Displaying OSPF neighbor information

To display information about OSPF neighbors to the TAOS 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 TAOS 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 TAOS unit and its neighbor.

Field	Specifies
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 TAOS 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.
Physical interface	The name of the interface on which the unit and the neighbor communicate: <ul style="list-style-type: none"> ie0 or ie[<i>shelf</i>]-[<i>slot</i>]-[<i>item</i>] is an Ethernet interface. The shelf number is always 1. wan<i>N</i> 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.

Field	Specifies
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 reset.

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

Displaying OSPF External AS advertisements

To display OSPF External AS 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.

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 0.0.0.170 170
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 0.0.0.170 170
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 (AS border route), or BR (area border route).
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.

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      Segno    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      Segno    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 TAOS 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: <ul style="list-style-type: none">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 AS boundary routers.Type 5 (ASE) are AS-external-LSAs that describe routes to destinations external to the AS. A default route for the AS can also be described by an AS-external-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.
Segno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.
# advertisements	Total number of entries in the database.
Checksum total	Checksum of the database.

Displaying internal OSPF routes

When the TAOS unit uses the internal routes feature, it exports routes by means of the router LSA (Type1), instead of by means of the usual ASE-5. If the TAOS 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:

```

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

Ping

Description: Sends ICMP echo_request packets to the specified host as a way to verify that the host is up 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|-v][-c count][-i delay][-s packetsize]`
`[-r VRoutername] [-f] hostname`

Syntax element	Description
-q	Quiet. Do not display informational messages. Just display the summary lines at the beginning and end of the command.
-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 one 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.
-r VRoutername	The name of the Virtual Router (VRouter). If you do not specify a VRouter name, the system assumes the global VRouter.
-f	Set the Don't Fragment (DF) bit in the IP header of Ping packets.
hostname	The station's IP address or Domain Name System (DNS) hostname.

Example: Pinging 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. To exchange only 3 packets, each of which contains only 16 bytes:

```
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
```

To exchange three packets and suppress the output for each exchange:

```
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 Rlogin, Telnet, Terminal-Server, Traceroute

Power

Description: Checks the status of the TAOS unit's redundant power supplies and displays the results.

Permission level: System

Usage: **power**

Example: To check the power supply on a MAX TNT unit:

```
admin> power
Power supply A present, OK
Power supply B not present
```

On an APX unit, the output looks like the following:

```
admin> power
Power supply A present, OK temp= OK
Power supply B not present
Power supply C not present
Power supply D present, OK temp= OK
```

PRIdisplay

Description: For a T1, E1, or T3 card, displays general PRI messages, shows a timestamp relative to the time the card booted, and identifies PRI messages that have bad CRCs or are too long.

You can use PRIdisplay on a T1, E1, or T3 card only. You must first execute the Open command to open a session with the card.

Permission level: Diagnostic

Usage: `pridisplay octets [line]`

Syntax element	Description
<i>octets</i>	The maximum number of octets to display per message. If you specify 0 (zero), the TAOS unit does not display any data.
<i>line</i>	The line whose D channel you want to monitor.

Example: To open a session with a T3 card in slot 15, and then display the first 160 bytes of PRI messages:

```
admin> open 1 15
t3-1/15> pridisplay 160
Display the first 160 bytes of PRI messages
PRI-XMIT-24: 01:38:53: 3 of 3 octets
1010A850: 00 01 7f
PRI-RCV-24: 01:38:55: 3 of 3 octets
10112C10: 00 01 7f
PRI-RBAD-22: 01:38:53: 2 of 2 octets
1010A850: 00 01
```

In the following example, the first command displays the first 32 bytes of PRI messages for line 12 only. The second command enables display of the first 32 bytes of messages for any line on the card, and the third command turns off the message display:

```
t3-1/15> prid 32 12
Display the first 32 bytes of PRI messages for line 12
t3-1/15> prid 32 0
Display the first 32 bytes of PRI messages
t3-1/15> prid 0
PRI message display terminated
```

To close the session with the card and return to the shelf controller:

```
t3-1/15> quit
admin>
```

PrtCache

Description: Displays statistics about cached RADIUS private-route profiles, and enables you to flush the cache.

Permission level: Diagnostic or Update

Usage: `prtcache -s [profile_name] | -f [-f] | -t`

Option	Description
<code>-s [profile_name]</code>	If <code>profile_name</code> is not specified, the command display statistics for all cached private-route profiles. If it is specified, the command displays statistics only for the specified private-route profile
<code>-f [-f]</code>	Flush all cached entries. The second <code>-f</code> flag specifies that all cached routes are flushed without waiting for confirmation.
<code>-t</code>	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

Output 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	Specifies whether the profile's cache time is refreshed if the profile is used.

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

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
```

Dependencies: 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.

Quiesce

Description: Allows you to Busy Out or take Out Of Service (OOS) individual ISDN T1 PRI lines or channels connected to the TAOS unit. These actions are known as *quiescing* the line or channel to make it available for maintenance. Quiescing the line does not tear down calls that are currently active on the line. When an active call disconnects, that channel is taken OOS.

Quiescing a line is equivalent to setting the Maintenance-State parameter in the T1 profile to Yes. Unquiescing the line sets the parameter to No. When the parameter is set to Yes, individual channels on that line cannot be restored. See Chapter 2, “Profile and Parameter Reference.” This setting is preserved across power ups.

Whether the command takes a channel or line out of service or busies it out depends on the type of switch.

Type of switch	Description
AT&T switches running Custom generics	AT&T Custom generics support Service Messages that allow the TAOS unit to tell the switch to take channels on an ISDN PRI line OOS. The line-status window displays the condition as an o in an OOS channel. When all channels on the line are OOS, the switch can route incoming calls to other lines in a particular hunt group.
AT&T switches running NI-2 generics and Northern Telecom switches	Neither AT&T nor Northern Telecom switches running NI-2 software support Service Messages to take channels OOS. There is no sure way for the TAOS unit to tell the switch to take a channel OOS. Because channels cannot be taken OOS, incoming calls are presented to the TAOS unit even if the ISDN T1 PRI line is quiesced. The TAOS unit rejects the call with a cause code of 17, User Busy. The user originating the call receives a busy signal. This situation can pose a problem for ISPs who would like to have the switch automatically route incoming calls to another, nonquiesced trunk in the hunt group.

Note: Restoring a quiesced line or channel can take up to 3.5 minutes. Only 1 service message per channel is sent to the switch, at the rate of one per second.

Permission level: System

Usage: `quiesce -d|-e|-r line|-q line|-t`

Option	Description
<code>-d</code>	Quiesce a single DS0 channel (a B channel on any T1 PRI line).
<code>-e</code>	Restore a single DS0 channel that has been quiesced.
<code>-r line</code>	Restore the specified T1 PRI line that has been quiesced.
<code>-q line</code>	Quiesce the specified T1 PRI line.
<code>-t</code>	Toggle debug display.

Example: To quiesce a T1 PRI line in port 4 of a card installed in slot 2:

```
admin> quiesce -q {1 2 4}
QUIESCE: line 1/2/4, enable=T, isPri=T
```

Dependencies: The specified T1 line must be enabled and configured for ISDN PRI.

See Also: Chapter 2, “Profile and Parameter Reference”

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%
```

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]

Syntax element	Description
<i>profile-type</i>	The type of profile to be read (or the profile itself if it does not require an index specification).
<i>profile-index</i>	The name or address that distinguishes a profile from others of the same type. To see profile indexes, enter the Dir command (<i>dir profile-type</i>).
-f	Do not prompt for confirmation when overwriting the unsaved contents of the edit buffer.

By default, when you issue a Read command that would 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 argument on the Read command line.

APX 8000 examples

To find the right index for an IP-Interface profile, read that profile, and list its contents:

```
admin> dir ip-interface
66  10/20/2000 14:02:02 { { shelf-1 slot-12 1 } 0 }
66  10/27/2000 16:34:40 { { shelf-1 slot-12 2 } 0 }
66  10/27/2000 16:34:47 { { shelf-1 slot-12 3 } 0 }
66  10/27/2000 16:34:54 { { shelf-1 slot-12 4 } 0 }
66  10/28/2000 00:21:06 { { shelf-1 left-controller 1 } 0 }

admin> read ip-int {{1 first 1} 0}
IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 } read

admin> list
[in IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 }]
interface-address* = { { shelf-1 left-controller 1 } 0 }
ip-address = 10.6.212.227/24
rip-mode = routing-send-and-recv
ospf = { no 0.0.0.0 normal 10 10 40 5 simple ***** 1 16777215 +
multicast-allowed = no
multicast-rate-limit = 100
rip2-use-multicast = yes
```

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 multicast-allowed = yes

admin> write
IP-INTERFACE/{ { shelf-1 left-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 executed other commands, you can still use the Get command to display the working profile:

```
admin> get .
[in IP-INTERFACE/{ { shelf-1 left-controller 1 } 0 }]
interface-address* = { { shelf-1 left-controller 1 } 0 }
ip-address = 10.6.212.227/24
rip-mode = routing-send-and-recv
ospf = { no 0.0.0.0 normal 10 10 40 5 simple ***** 1 16777215 +
multicast-allowed = yes
multicast-rate-limit = 100
rip2-use-multicast = yes
```

MAX TNT examples

To find the right index for an IP-Interface profile, read that profile, and list its contents:

```
admin> dir ip-interface
66 12/20/2000 14:02:02 { { shelf-1 slot-12 1 } 0 }
66 12/27/2000 16:34:40 { { shelf-1 slot-12 2 } 0 }
66 12/27/2000 16:34:47 { { shelf-1 slot-12 3 } 0 }
66 12/27/2000 16:34:54 { { shelf-1 slot-12 4 } 0 }
66 12/28/2000 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
ospf = { no 0.0.0.0 normal 10 10 40 5 simple ***** 1 16777215 +
multicast-allowed = no
multicast-rate-limit = 100
rip2-use-multicast = yes
```

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 multicast-allowed = yes

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 executed 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 = 10.6.212.227/24
rip-mode = routing-send-and-recv
ospf = { no 0.0.0.0 normal 10 10 40 5 simple ***** 1 16777215 +
multicast-allowed = yes
multicast-rate-limit = 100
rip2-use-multicast = yes
```

See Also: Get, List, New, Set, Write

Redundant-Controller-Switch

Description: Switches primary shelf controller functionality to the secondary shelf controller, causing the primary controller to give up bus (slot card) ownership and allowing the other controller to become primary. The switchover to the secondary controller occur only if the secondary controller is present. After the bus is released, the old primary shelf controller reboots and assumes the role of secondary controller.

Switchover takes place only if the following conditions are met:

- The secondary controller is present.
- The primary controller currently controls the bus.
- The secondary controller requests control of the bus, which is the normal operating state of the secondary controller. The secondary controller is ready to automatically gain bus ownership whenever the primary releases its ownership.

Permission level: System

Usage: `redundant-controller-switch [-f]`

Option	Description
-f	Force a switchover without prompting for confirmation.

Example: To switch primary controller functionality to the secondary controller without being prompted for confirmation, enter the following command:

```
admin> redundant-controller-switch -f
```

Dependencies: Consider the following:

- When the Redundant-Controller-Switch command is entered on the primary controller, controller functionality is switched to the secondary controller. When the switchover command is entered on the secondary controller, no switchover occurs.
- If the switchover command is entered on the primary controller when the secondary is not requesting control of the bus, no switchover occurs:

```
admin> redundant-controller-switch
The remote controller is not requesting the bus,
it cannot become PRIMARY!
```

- If the switchover command is entered on the primary controller when only one controller is present, a notice is displayed:

```
admin> redundant-controller-switch
There is no remote controller!
```

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`

Option	Description
-a	Refresh all types of configuration.
-n	Refresh nailed profiles configuration.
-p	Refresh address pools configuration.
-r	Refresh static routes configuration.
-t	Refresh terminal server configuration.
-s	Clears the current Source Auth information (purging all existing Source Auth entries from the cache) and reloads it from RADIUS.

Example: RADIUS profiles can support up to 50 IP address pools. To refresh the address pool configuration on the TAOS unit:

```
admin> refresh -p
Refreshing remote config.
```

Remote

Description: Enables you to remotely manage another unit. 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 TAOS 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 LCD menu.

Permission level: System

Usage: `remote station_name`

Argument	Description
<i>station_name</i>	Specifies the station name of the remote device. The value you enter must match the value of a Station parameter in a Connection profile, or the user ID at the start of a RADIUS profile.

Example: To remotely manage the unit called **allwyn**:

```
admin> remote allwyn
```

<pre>allwynp50 Edit Main Edit Menu Configure >00-000 System 20-000 Ethernet 30-000 Serial WAN</pre>	<pre>10-100 1 Link A B1 A B2</pre>	<pre>00-200 11:23:55 M31 Line Ch Outgoing Call</pre>
	<pre>20-100 Sessions >1 Active</pre>	<pre>20-500 DYN Stat Qual Good 01:23:44 OK 1 channel CLU 100% ALU 100%</pre>
	<pre>20-300 WAN Stat >Rx Pkt: 667435 ^ Tx Pkt: 3276757 CRC: 323v</pre>	<pre>20-400 Ether Stat >Rx Pkt: 99871435 Tx Pkt: 76876757 Col: 73298</pre>
	<pre>00-100 Sys Option >Security Prof:1 ^ Software +7.0+ S/N:4293801 v</pre>	<pre>00-400 HW Config >SWAN Interface Adrs: 00c05b45390 Enet I/F: AUI</pre>

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 an MP+ connection by hanging up all channels of the connection.

The TAOS 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 can appear:

Message	Description
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 <i>station</i>	No profile was found for the specified station name.
profile for <i>station</i> 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 <i>station</i>	The MP+ connection to the remote station could not be established.
<i>station</i> 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.
far end rejected session	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 reset 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.

Reset

Description: Resets the TAOS unit, one redundant shelf controller, or both redundant shelf controllers. When you reset the 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 because of a momentary loss of signaling or framing information. After a reset, the TAOS unit runs a POST (Power-On Self Test).

Permission level: Update

Usage: **reset** [-f][-a][-r *controller*]

Option	Description
No options	Reset the unit, one redundant controller, or both redundant controllers. On an APX 8000 unit, using the Reset command with no options resets both redundant controllers, but only when you are logged in to the primary controller. If you are logged in to the secondary controller, the operation affects only the secondary controller. The secondary controller cannot reset the primary controller.
-f	Force a reset without prompting for confirmation.
-a	Reset the shelf controller.
-r <i>controller</i>	Reset one or both redundant controllers. For <i>controller</i> , you can specify one of the following: primary —Reset the primary controller. secondary —Reset the secondary controller. both —Reset both controllers.

Example: To reset a MAX TNT unit:

```
admin> reset
```

If you are logged in to the primary controller of an APX 8000 system with dual controllers, the following command resets the secondary controller:

```
admin> reset -r secondary
```

The following command resets the primary controller:

```
admin> reset -r primary
```

The following command resets the system (both controllers):

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

```
Please stand by. System reset in progress...
```

See Also: NVRAM

Rlogin

Description: Opens a login session across the network with the specified host. The Rlogin command is supported only on digital modem and Hybrid Access cards. You must first execute the Open command to open a session with the card.

Permission level: Diagnostic

Usage: `rlogin [-l user][-ec] hostname`

Syntax element	Description
-l <i>user</i>	Log into the remote host using the specified username.
-ec	Define an escape character other than the default tilde. You can use the escape character to log out of the session.
<i>hostname</i>	The name of a networked host.

Example: Logging in across a network to a host named Host-231:

```
admin> open 1 7
modem-1/7> rlogin host-231
Password:
Last login: Wed Dec 18 10:31:36 from marcel.marceau
SunOS Release 4.1.4 (HOST-231-BQE) #1: Mon Sep 4 08:56:59 PDT 2000
host-231%
```

You can log out of the remote host by typing the escape sequence (tilde-dot). For example:

```
host-231% ~.
Connection closed.
```

Or, you can log out explicitly:

```
host-231% logout
Connection closed.
```

If your username is different on the TAOS unit and the remote host, you can specify a username on the Rlogin command line. For example:

```
modem-1/7> rlogin -l marcel host-231
Password:
```

If you wish, you can change the default escape character from a tilde to any other character.

See Also: Netstat, Ping, Telnet, Terminal-Server

RM

Description: Deletes a file or directory.

Permission level: System

Usage: `rm socket/path`

Option	Description
<i>socket</i>	Specify the flash card number.
<i>path</i>	Specify the subdirectory to be deleted.

Example: To remove the /test1 directory on flash card 1, enter the following:

```
admin> rm 1/test1
```

See Also: LS, Mkdir, MV

Save

Description: Saves all profiles, all profiles of a given type, or a specific profile to a file or PCMCIA flash card, or specifies a list of profiles to be included in or excluded from the Save operation. The file can reside either on the hard disk of the PC you are using to issue commands to the TAOS unit or on a networked host. The file is saved in a format that can be loaded into the TAOS unit to restore a configuration.

The Save command uses TFTP to transfer the configuration across the network. To save the TAOS unit's configuration on a remote host, you must have the necessary permissions in the directory.

Permission level: Update

Usage: `save [-a][-m][-e encryption_type password]`
`[target [profile-type [profile-index]] | network host filename`
`[-p profile1, profile2... | -x profile1, profile2...] target]`

Syntax element	Description
-a	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.
-m	Use MIB tags instead of field and value names, and use profile-type numbers rather than profile-type text names.
-e <i>encryption_type</i> <i>password</i>	Use encryption. The <i>encryption_type</i> argument specifies the method to be used for encryption and decryption. You can specify DES or MD5. The <i>password</i> argument specifies the password used to generate the key for encryption and decryption. The -e option supports only a network target.
<i>target</i>	The destination of the file to be saved. Valid specifications are: <ul style="list-style-type: none"> <i>network host filename</i>— A network hostname or IP address and the name of the file on that host. <i>console</i>— The PC you are using in a terminal session. <i>flash device/filename</i>—The PCMCIA flash card.
<i>profile-type</i>	The type of profile to be read, or the profile itself if it does not require an index specification.
<i>profile-index</i>	The name or address that distinguishes a profile from others of the same type. To see profile indexes, enter the Dir command (<code>dir <i>profile-type</i></code>).
<i>network host filename</i>	The hostname or IP address of the source network and the name of the file on that host.
-p <i>profile1, profile2...</i>	Save the specified list of profiles.
-x <i>profile1, profile2...</i>	Save all profiles, except those in the specified list.

Example: Saving all Connection profiles to a file on a PC's hard disk (after starting the capture utility in the VT100 emulation software):

```
admin> save console connection
; saving profiles of type CONNECTION
; profile saved Tue Jan 2 13:02:54 2001
new CONNECTION dallas
set active = yes
set ip-options remote-address = 10.122.99.1/24
write -f
;

; profile saved Tue Jan 2 13:02:54 2001
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
set ppp-options send-auth-mode = chap-ppp-auth
set ppp-options send-password = *****
set ppp-options recv-password = *****
set mp-options base-channel-count = 6
set mp-options minimum-channels = 6
set mp-options maximum-channels = 20
write -f
;
```

To save the file, stop the capture in the VT100 emulation software. 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. The following example shows how to save a specific profile to a file on a network host:

```
admin> save network host-231 ipglobal -p ip-g
configuration being saved to 10.65.12.231
file ipglobal...save
admin>
```

The following example shows how to specify a profile type by its internal number when saving:

```
admin> save -m console system
; saving profiles of type SYSTEM
; profile saved Fri Mar 31 13:29:42 2000
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, it is assumed to be a profile-type number.

To save a configuration in DES-encrypted format:

```
admin> save -e des john network 172.20.32.114 test.cfg
```

The following error messages apply to DES encryption for configuration file transfer over TFTP:

```
-e option:unknown encryption method method
```

You specified an incorrect encryption method when you saved the configuration.

```
File is corrupted, Encryption tag not found
```

```
File is corrupted, Version tag not found
```

The configuration file is corrupted.

```
Wrong encryption password!!
```

Configuration is encrypted but the password is incorrect.

```
Configuration is encrypted
```

Configuration is encrypted but no password was provided.

```
Configuration is not encrypted!!
```

Configuration is not encrypted but a password was provided.

```
Encrypted protocol <ver> not supported!!
```

Encryption version mismatch occurred.

See Also: Load, NVRAM

Screen

Description: Changes window display sizes for the current session only.

Permission level: Update

Usage: `screen screen-length [status-length] [-w width]`

Syntax element	Description
<i>screen-length</i>	The 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

Syntax element	Description
<i>status-length</i>	The 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 <i>status-length</i> value must be less than the <i>screen-length</i> by at least six lines
-w <i>width</i>	<p>The width of the screen. You can specify a value for <i>width</i> from 80 to 256. The default is 80.</p> <p>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 <code>admin></code> (a 6-character prompt followed by a space), the maximum number of visible characters in a command is 72. The user can scroll to the characters not currently visible by moving the cursor left or right.</p> <p>The control sequence <code>Ctrl-L</code>, <code>Ctrl-R</code> enables you to redraw the current line.</p>

If the Status window is open when you execute the Screen command, the window is resized dynamically. If it is not open, the Status window is resized when you next open it.

Example: `admin> screen 55 22`

If only the ***screen-length*** argument is specified, and the stored ***status-length*** is not less than the specified value by 6 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
```

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|?`

Syntax element	Description
<i>param-name</i>	Name of the parameter in the current or specified context of the working profile.
<i>param-index</i>	Parameter index, which might be required for some complex or array parameters. (See the Physical-Address example below.)

Syntax element	Description
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	Legal parameter value.
?	Display help text about the specified parameter.

Example: Enter the following commands to display help about a T1 line's physical address:

```
admin> read t1 {1 2 1}
T1/{ shelf-1 slot-2 1 } read

admin> list
[in T1/{ shelf-1 slot-2 1 }]
physical-address* = { shelf-1 slot-2 1 }
line-interface = { no d4 ami eligible middle-priority inband +

admin> set physical-address slot ?
slot: The number of the slot that the addressed physical device resides
on. Enumerated field, values:
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-8: Slot 8.
slot-9: Slot 9.
slot-10: Slot 10.
slot-11: Slot 11.
slot-12: Slot 12.
slot-13: Slot 13.
slot-14: Slot 14.
slot-15: Slot 15.
slot-16: Slot 16.
controller: The shelf-controller pseudo-slot.
```

The following example shows how to open the Line-Interface subprofile and set the phone number for channel 1:

```
admin> list line
[in T1/{ shelf-1 slot-2 1 }:line-interface]
enabled = no
frame-type = d4
encoding = ami
clock-source = eligible
clock-priority = middle-priority
signaling-mode = inband
robbed-bit-mode = wink-start
switch-type = att-pri
```

```

nfas-id = 0
call-by-call = 0
data-sense = normal
idle-mode = flag-idle
FDL = none
front-end-type = dsx
DSX-line-length = 1-133
CSU-build-out = 0-db
channel-config = [{ switched-channel 9 "" { any-shelf any-slot +
maintenance-state = no

admin> set channel 1 phone = 5551212

admin> write
T1/{ shelf-1 slot-2 1 } written

```

See Also: List, New, Read, Write

Show

Description: On an APX 8000 unit, displays information about installed slot cards and their status, as well as the communication status of the primary and secondary controllers. The Show command also indicates whether the controller is the primary or secondary shelf controller. On a MAX TNT unit, the Show command displays information about installed slot cards and their status.

Permission level: System

Usage: `show shelf-number [slot-number [item-number]]`

Syntax element	Description
<i>shelf-number</i>	The shelf number (always 1).
<i>slot-number</i>	The number of an expansion slot.
<i>item-number</i>	The number of a specific item (device or channel) on the slot card.

APX 8000 examples

In the following example, the Show command is executed on the primary controller while the left controller is primary:

```

admin> show

Controller { left-controller } ( PRIMARY ):

           Req'd  Oper   Slot Type
{ shelf-1 slot-1 0 } DOWN  RESET  8t1-card
{ shelf-1 slot-2 0 } DOWN  RESET  8t1-card
{ shelf-1 slot-3 0 } DOWN  RESET  ether3-card
{ shelf-1 slot-4 0 } DOWN  RESET  csmx-card
{ shelf-1 slot-19 0 } UP    UP      hse-card

```


In the following example, the Show command is executed on the secondary controller while the right controller is primary:

```
admin> show
Controller { left-controller } ( SECONDARY ):
      { right-controller }      UP      ( PRIMARY )
```

For each controller, the output includes (from left to right) the address of each slot in which an expansion slot card is installed, the required state of the card, the actual status of the card, and the type of card installed. The status can be one of the following:

Status	Description
UP	Normal operational mode. The card is up and running. The current controller can communicate with the other controller.
DOWN	Not in an operational mode. The card has shut down all functions and can be made inoperative by the shelf controller. For the secondary controller, DOWN specifies that the two controllers cannot communicate with each other.
POST	The download is complete, and the devices in the card are running power-on self tests.
BOOT	The card has been recognized by the shelf controller and has begun to execute the code in its boot ROM. Under normal conditions, the LOAD status follows.
LOAD	The card is loading code as part of coming up.
RESET	The card is being reset.
NONE	The card has been swapped out, but its configuration remains in flash memory space.
OCCUPIED	The card is using two slots.
ABSENT	The secondary controller is not present.
MAINT	The card is completely inactive but can be monitored with the Show command. The slot card maintains visibility but does not generate any unnecessary errors. When a slot card is out of maintenance state it is active. The slot card remains in or out of maintenance state until you change it.

MAX TNT examples

To display all installed expansion modules on a MAX TNT unit:

```
admin> show 1
  { shelf-1 slot-1 0 }      UP      8t1-card
  { shelf-1 slot-11 0 }     UP      4ether2-card
  { shelf-1 slot-12 }       OCCUPIED
  { shelf-1 slot-14 0 }     UP      4ether2-card
  { shelf-1 slot-15 }       OCCUPIED
```

The output includes the address of each slot in which an expansion slot card is installed, the status of the card, and the type of card installed. The status can be one of the following:

Status	Description
UP	Normal operational mode. The card is up and running.
DOWN	Not in an operational mode. The card has shut down all functions and can be made inoperative by the shelf controller.
POST	The download is complete, and the devices in the card are running power-on self tests.
BOOT	The card has been recognized by the shelf controller and has begun to execute the code in its boot ROM. Under normal conditions, the LOAD status follows.
LOAD	The card is loading code as part of coming up.
RESET	The card is being reset.
NONE	The card has been swapped out, but its configuration remains in flash memory.
OCCUPIED	The card is using two slots.
MAINT	The card is completely inactive.

See Also: Device, HDLC, Modem, Slot, T1channels

Slot

Description: Changes the administrative state of a slot card, 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]? [-all] [shelf-number]`
`[slot-number]`

Syntax element	Description
-u	Bring up the specified slot card.
-d	Bring down the specified slot card.
-r	Delete the profiles for a card that has been removed.
-t	Toggle module debug level.
-b	Force hardware reset.
-w	Change or display watchdog failure limit.
-m	Put the slot in a maintenance state. The card is completely inactive but can be monitored with the Show command. The slot card maintains visibility but does not generate any unnecessary errors. When a slot card is out of maintenance state it is active. The slot card remains in or out of maintenance state until you change it.

Syntax element	Description
option -all	Apply the specified command option to all the slot cards.
?	Display a usage summary.
shelf-number	The shelf number (always 1).
slot-number	The number of an expansion slot.

Note: The slot card state remains the same through a system reset or reboot until you change it. As long as the card stays in the same slot, it starts in the same state (up, down, or maintenance) in which it was last configured.

Bringing up a slot card

To bring up the expansion module in slot 5:

```
admin> slot -u 5
slot 1/5 state change forced
```

In the next example, a card has been removed, as indicated by a status of NONE in the output of the Show command:

```
admin> show 1 13
Shelf 1 ( standalone ):
  { shelf-1 slot-13 0 }      NONE      8t1-card:
    { shelf-1 slot-13 1 }      t1-line-1
    { shelf-1 slot-13 2 }      t1-line-2
    { shelf-1 slot-13 3 }      t1-line-3
    { shelf-1 slot-13 4 }      t1-line-4
    { shelf-1 slot-13 5 }      t1-line-5
    { shelf-1 slot-13 6 }      t1-line-6
    { shelf-1 slot-13 7 }      t1-line-7
    { shelf-1 slot-13 8 }      t1-line-8
```

The NONE status indicates that the card was removed but that its profiles have been saved. The TAOS unit remembers that a card was in that slot and saves its profiles until a card of a different type is installed in the same slot, or until you delete the profile:

```
admin> slot -r 13
slot 1/13 removed
```

Either action deletes all the old profiles associated with the slot. When you insert a different type of card, the system creates appropriate new profiles.

Syslog records

The TAOS unit generates Syslog records with a level of Warning when you use particular options associated with the Slot command. No Syslog record is generated if you reset the TAOS unit by means of the Reset command.

Syslog message when operator resets a card

When you use the **slot -b** command, the following Syslog record is generated:

```
LOG warning, Shelf shelf_num, Controller, Time: 14:27:20--  
Slot shelf_num/slot_num bounced
```

The shelf number is always 1. Suppose you specify the card in slot 6 by entering the following command:

```
admin> slot -b 1 6
```

The following Syslog record is generated:

```
LOG warning, Shelf 1 Controller, Time: 14:27:20--  
Slot 1/6 bounced
```

Syslog message when operator brings down a card

When you use the **slot -d** command, the following Syslog record is generated:

```
LOG warning, Shelf shelf_num, Controller, Time: 14:27:20--  
Slot shelf_num/slot_num down
```

The shelf number is always 1. Suppose you specify the card in slot 6 by entering the following command:

```
admin> slot -d 1 6
```

The following Syslog record is generated:

```
LOG warning, Shelf 1 Controller, Time: 14:27:20--  
Slot 1/6 down
```

Syslog message when operator brings up a card

When you use the **slot -u** command, the following Syslog record is generated:

```
LOG warning, Shelf shelf_num, Controller, Time: 14:27:20--  
Slot shelf_num/slot_num up
```

The shelf number is always 1. Suppose you specify the card in slot 6 by entering the following command:

```
admin> slot -u 1 6
```

The following Syslog record is generated:

```
LOG warning, Shelf 1 Controller, Time: 14:27:20--  
Slot 1/6 up
```

NVRAM log messages

The TAOS unit generates NVRAM records when you enter the `slot -b` or `slot -d` command. No NVRAM record is generated if a slot card is brought up by a `slot -u` command, or if the TAOS unit is reset by means of the Reset command.

NVRAM log message when operator resets a card

When you use the `slot -b` command, the following NVRAM record is generated:

```
SLOT CARD BOUNCED: Index: 220 Revision: 9.0 Slot shelf_num/slot_num
Date: 04/22/2000.      Time: 12:35:05
Card bounced by 10.40.40.94, user profile admin.
```

The shelf number is always 1. Suppose you specify the card in slot 6 by entering the following command:

```
admin> slot -b 1 6
```

The following NVRAM record is generated:

```
SLOT CARD BOUNCED: Index: 220 Revision: 9.0 Slot 1/6
Date: 04/22/2000.      Time: 12:35:05
Card bounced by 10.40.40.94, user profile admin.
```

NVRAM log message when operator brings down a card

Suppose you specify the card in slot 6 by entering the following command:

```
admin> slot -d 1 6
```

The following NVRAM record is generated:

```
SLOT CARD DOWN: Index: 221 Revision: 9.0 Slot 1/6
Date: 04/22/2000.      Time: 12:36:54
Card downed by 10.40.40.94, user profile admin.
```

Dependencies: Any time the `-u` (bring up), `-d` (bring down), or `-m` option is entered, a warning message is sent to the console as a reminder that the slot state change will be retained. For example:

```
admin> slot -m 1
```

```
Slot 1/1, state change forced
```

```
warning: new state will remain until next explicit management action.
```

Similarly, if you enter a `slot -d` command, the affected slot card remains down even after a system reset.

Any time a new slot card is installed in a slot, it starts up when the system reboots. Also, all cards return to an up state if the system nonvolatile RAM (NVRAM) is cleared.



Caution: If any errors occur during loading (for example, missing load images or corrupted images), the loader brings down the slot card in question. You must manually bring up the card by using the `slot -u` command, or by using a Set operation on the SNMP variable `slotAdminStatus`.

See Also: Device, HDLC, Open, Modem, Show, T1channels

snmpAuthPass

Description: Generates the authentication key of an SNMPv3 USM user.

Permission level: Update

Usage: `snmpauthpass username password`

Argument	Description
<i>username</i>	SNMPv3 USM user for whom an authentication key is generated.
<i>password</i>	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 an SNMPv3 USM user.

Permission level: Update

Usage: `snmpPrivPass username password`

Argument	Description
<i>username</i>	SNMPv3 USM user for whom a privacy key is generated.
<i>password</i>	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.

See Also: snmpAuthPass

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]`

Syntax 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 PPP 1/7/14 19200
002 timl MP 1/7/3 56000

Status
Serial number: 6201732      Version: 1.0F
Rx Pkt:      11185897
Tx Pkt:      42460
Col:         129

12/26/2000 12:20:15 Up:      3 days, 21:47:32
-----
M: 29 L: info Src: shelf-1/controller
48 out of 48 modems passed POST

Issued: 16:48:02, 09/27/2000

[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, Line, Log, View

SWANlines

Description: Displays all Serial WAN (SWAN) lines, including disabled, busy, and unused channels.

Permission level: System

Usage: `swanlines -a | -d | -f | -u`

Option	Description
-a	Display all channels.
-d	Display all disabled channels.
-f	Display all free channels.
-u	Display in-use channels.

Example: To display all SWAN channels:

```
admin> swanlines -a
```

All SWAN lines:

		(OperState	UpStatus	ReqState	AdminState)
Line {	1 14 1 }	(Down	Idle	UP	UP)
Line {	1 14 2 }	(Down	Idle	UP	UP)
Line {	1 14 3 }	(Down	Idle	UP	UP)
Line {	1 14 4 }	(Down	Idle	UP	UP)
Line {	1 14 5 }	(Down	Idle	UP	UP)
Line {	1 14 6 }	(Down	Idle	UP	UP)

The output contains the following fields:

Field	Description
OperState	The current operational state of the channel: <ul style="list-style-type: none"> Down indicates that the channel is in a nonoperational state. Up indicates that the channel is in normal operations mode.
UpStatus	The status of a channel in normal operations mode: <ul style="list-style-type: none"> Idle indicates that no call is on the channel. Active indicates that the channel is handling a call.
ReqState	The required state of the channel as specified by the ReqState setting: <ul style="list-style-type: none"> Down indicates that the channel is required to be nonoperational. Up indicates that the channel must be in normal operations mode.
AdminState	The desired administrative state of the channel: <ul style="list-style-type: none"> Down specifies that the channel should terminate all operations and enter the down state. Up specifies that the channel should come up in normal operations mode.

Note: The actual state of the channel 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 force a channel to the new state. It indicates that the TAOS unit should change the channel state gracefully.

T1channels

Description: Displays administrative information about T1 channels.

Permission level: System

Usage: `t1channels -a | -c | -d | -i`

Option	Description
-a	Display information about all available T1 channels.
-c	Display information about all possible T1 channels (all channels on all T1 cards).
-d	Display information about disabled T1 channels.
-i	Display information about all T1 channels that are currently in use.

The T1channels command displays the following information:

Column	Description
dvOp	The current operational state of the channel (also specified by Device-State): <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Idle indicates that no call is on the line. Busy indicates that the channel is handling a call.
dvRq	The required state of the channel as specified by Reqd-State: <ul style="list-style-type: none"> Down indicates that the channel must be in a nonoperational state. Up indicates that the channel is required to be in normal operations mode.
SAdm	The desired administrative state of the channel (also specified by Desired-State): <ul style="list-style-type: none"> Down specifies that the channel should terminate all operations and enter the down state. Up specifies that the channel should come up in normal operations mode.

Note: The actual state of the channel 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 force a channel to the new state. It indicates that the TAOS unit should change the channel state in a graceful manner.

Example: Include the `-a` option with the `T1channels` command to display information about all available T1 channels:

```
admin> t1 -a
T1 channels available for use:
```

					(dvOp	dvUpSt	dvRq	sAdm)
Channel	{	{	1 13 1 }	1 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	2 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	3 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	4 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	5 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	6 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	7 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	8 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	9 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	10 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	11 }	(UP	Idle	UP	UP)

If you suspect that some channels might be disabled, you can use the `-d` option to list any disabled channels. For example:

```
admin> t1 -d
Disabled T1 channels:
```

					(dvOp	dvUpSt	dvRq	sAdm)
Channel	{	{	1 13 1 }	12 }	(Down	Idle	UP	UP)
Channel	{	{	1 13 1 }	13 }	(Down	Idle	UP	UP)
Channel	{	{	1 13 1 }	14 }	(Down	Idle	UP	UP)

The following example shows how to display all T1 channels known to the system:

```
admin> t1 -c
All T1 channels:
```

					(dvOp	dvUpSt	dvRq	sAdm)
Channel	{	{	1 13 1 }	1 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	2 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	3 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	4 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	5 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	6 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	7 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	8 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	9 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	10 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	11 }	(UP	Idle	UP	UP)
Channel	{	{	1 13 1 }	12 }	(Down	Idle	UP	UP)
Channel	{	{	1 13 1 }	13 }	(Down	Idle	UP	UP)
Channel	{	{	1 13 1 }	14 }	(Down	Idle	UP	UP)

[More? <ret>=next entry, <sp>=next page, <^C>=abort]

The `-i` option displays information about which T1 channels are in use. For example:

```
admin> t1 -i
T1 channels allocated/in-use:

Channel { { 1 13 1 } 15 } (dvOp dvUpSt dvRq sAdm)
Channel { { 1 13 1 } 16 } (UP Busy UP UP )
Channel { { 1 13 1 } 17 } (UP Busy UP UP )
Channel { { 1 13 1 } 18 } (UP Busy UP UP )
Channel { { 1 13 1 } 19 } (UP Busy UP UP )
Channel { { 1 13 1 } 20 } (UP Busy UP UP )
Channel { { 1 13 1 } 21 } (UP Busy UP UP )
```

See Also: Line, Show, Slot

T1-Stats

Description: Reports DS1-level line errors on a T1 or T3 card. You must first execute the Open command to open a session with the card.

Permission level: Diagnostic

Usage: `t1-stats [-c] line`

Syntax element	Description
<code>-c</code>	Reset statistics to 0 (zero) after displaying them.
<code>line</code>	Line on the card.

Example: To open a session with a card in slot 13:

```
admin> open 1 13
```

Then, to display DS1-level statistics for the first line on the card:

```
t1-1/13> t1-stats 1
Line 1:
CRC Errors:          0
Frame Slips:         8
Framing Bit Errors:  0
Out of Frame Events: 0
Line Code Violations: 0
```

Finally, to display statistics for line 2, and reset the statistics to zero:

```
t1-1/13> t1-stats -c 2
Line 2:
CRC Errors:          2
Frame Slips:         3
Framing Bit Errors:  0
Out of Frame Events: 0
Line Code Violations: 3
Statistics cleared.
```

The output contains the following fields:

Field	Event that increments the field's value
CRC errors	Data corruption in the signal.
Frame slips	The TAOS unit received T1 data at a greater or less frequency than that of the internal line clock. In the process of realigning itself to the transmitter, the TAOS unit can skip or repeat a frame.
Framing bit errors	The TAOS unit detected a framing bit that was incorrect. T1 framing requires that certain bit positions (known as framing bits) have a fixed value in the signal. The framing bits enable the TAOS unit to determine where frames begin and end.
Out of Frame Events	The TAOS unit no longer detects a framing pattern in the receiving signal, or it detects a pattern at a different relative offset than expected.
Line Code Violations	The TAOS unit detected either a Bipolar Violation or Excessive Zeros, indicating that one of the low-level T1 rules for encoding data was violated in the received signal.
Statistics cleared	This field does not display a count. It simply indicates that the statistics have been reset to 0 (zero), because the command included the <code>-c</code> option.

Telnet

Description: Opens a Telnet session across the network to the specified host.

Permission level: Diagnostic

Usage: `telnet [-a|-b|-t] [-v Vroutername] [-l[e]|-r[e]] hostname [portnumber]`

Syntax element	Description
-a	ASCII mode, or standard 7-bit mode. In 7-bit mode, bit 8 is set to 0 (zero). This value is the default if no other mode is specified.
-b	Binary mode. The TAOS 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.
-v VRoutername	The name of the Virtual Router (VRouter). If you do not specify a VRouter name, the system assumes the global VRouter.
-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.
hostname	The IP address or Domain Name System (DNS) name of a networked host.
portnumber	A 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 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 TAOS unit by Telnet, you might want to change its escape sequence from Ctrl-] to a different setting.

See Also: Ping, Rlogin

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

** Lucent 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, Rlogin, 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 fantray intake.
- Shelf-controller temperature.
- High/Low/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.
- Fantray status, including the fantray operational mode, low-noise RPM, current fan mode, and RPMs.

Permission level: System

Usage: `thermalstatus`

Example: 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
```

See Also: Fanstatus

Tokencount

Description: Detects and reports the number of instances of a specified pattern (a token) in the TCP-Clear data stream sent by the unit. On the shelf controller, the command enables/disables the token-counting process, specifies up to four patterns, clears counters, and displays token information system wide. Updates to the command specified on the shelf controller are immediately propagated to the host cards.

Note: Running the token-counting process incurs a substantial system performance penalty. When token-counting is enabled, the system scans all outbound data sent to TCP-Clear sessions for a specified pattern, and increments a counter for each match. If the system resets, it loses the token information.

Permission level: Diagnostic

Usage: tokencount -argument [params]

Argument	Description
-a	Set token counters to 0 (zero). If the system resets, all token counters are set to 0 (zero). If a card resets, counters on that card are set to 0 (zero).
-c n	Set the counter for the specified token to 0 (zero).
-d	Disable the token-counting process.
-e	Enable the token-counting process.
-i	Display the current token-search information, including the number found of each defined token.
-u n	Define a token-search pattern and assign it the specified number.

Each pattern can contain up to 20 characters, but the first specified character cannot be repeated in the pattern more than eight times. You can specify the pattern as a combination of alphanumeric, hexadecimal, octal, and special characters, but output on the host is always in hexadecimal format. The following special characters are significant when you specify the pattern:

Characters	Meaning	ASCII value
\x##	Hex format	N/A. To insert a 2-digit hexadecimal number in the pattern, precede the number with \x.
\##	Octal format	N/A. To insert a 2-digit octal number, precede the number with a backslash.
\a	Alarm	7
\b	Backspace	8
\f	Form feed	12
\n	Newline	10
\r	Return	13
\t	Tab	9
\v	Vertical tab	11
\\	Backslash	92
\"	Quotation mark	34
\'	Apostrophe	44

Example: The following commands enable the token-counting process and define four token patterns:

```
admin> tokencount -e
admin> tokencount -u 1 \xB0\x35\xFF\x10\x01
admin> tokencount -u 2 LC\n
admin> tokencount -u 3 A1\12\15
admin> tokencount -u 4 \a\b\f\n\r\t\v\\\'\"
admin> tokencount -i
Tokencount is enabled
Number of "\xB0\x35\xFF\x10\x01" token received:0
Number of "LC\n" token received:0
Number of "A1\12\15" token received:0
Number of "\a\b\f\n\r\t\v\\\'\" token received:0
```


The next commands open a session with a card in slot 6 and display the token information gathered on that card:

```
admin> open 1 6
csm3-5/6> tokencount
Tokencount is enabled
"0xb00x350xff0x100x1" token received:0
"0x4c0x430xa" token received:0
"0x410x310xa0xd" token received:0
"0x70x80xc0xa0xd0x90xb0x5c0x270x22" received:0
```

When Tokencount is enabled, it can generate the following error messages:

error: token type index must be in the range of 1 to 4

The number specified in the **tokencount -u** command is out of the valid range of 1 to 4.

error: max. token size is 20

More than 20 characters were specified as a pattern in the **tokencount -u** command.

error: wrong token type index

The character immediately following **tokencount -u** was not numeric.

Traceroute

Description: Traces the route an IP packet follows by launching UDP probe packets with a low TTL (Time-To-Live) value and then listening for an ICMP *time exceeded* reply from a router. Probes start with a TTL of one and increase by one 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 there is no response within a 3-second timeout interval, the command output is an asterisk.

The destination host isn't 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*] [-r *VRoutername*] [-s *src_IPaddr*] *hostname* [*datasize*]

Syntax element	Description
-n	Print hop addresses numerically rather than symbolically and numerically (this eliminates a nameserver address-to-name lookup for each gateway found on the path).
-v	Verbose output. Include received ICMP packets other than Time Exceeded and ICMP Port Unreachable.

Syntax element	Description
-m max_ttl	Set the maximum time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops.
-p port	Set the 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	Set the maximum number of queries for each hop. The default is 3.
-w waittime	Set the time to wait for a response to a query. The default is 3 seconds.
-r VRoutername	The name of the Virtual Router (VRouter). If you do not specify a VRouter name, the system assumes the global VRouter.
-s src_IPaddr	The IP address of the source host.
hostname	The IP address or Domain Name System (DNS) name of a networked host.
datasize	Set the size of the data field of the UDP probe datagram sent by Traceroute. The default is 0. This 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 after the time field:

Annotation	Description
!H	Host reached.
!N	Network unreachable.
!P	Protocol unreachable.
!S	Source route failed. This event should not occur, and might indicate that there is a problem with the associated device.
!F	Fragmentation needed. This event should not occur, and might indicate that there is a problem with the associated device.
!h	Communication with the host is prohibited by filtering.
!n	Communication with the network is prohibited by filtering.
!c	Communication is otherwise prohibited by filtering.
!?	An ICMP subcode. This event should not occur.
!??	Reply received with inappropriate type. This event should not occur.

See Also: Ping, Netstat

UDS3lines

Description: Displays information regarding UDS3 lines.

Permission level: System

Usage: `uds3lines -a | -d | -f | -u`

Option	Description
-a	Show information about all UDS3 lines.
-d	Show disabled lines.
-f	Show all free lines.
-u	Show lines that are in use.

Example: In the following example, the UDS3lines command displays information about all UDS3 lines:

```
admin> uds3lines -a
```

All UDS3 lines:

		(dvOp	dvUpSt	dvRq	sAdm	na1lg)
Line	{ 1 13 1 }	(Up	Idle	UP	UP	00012)

The output displays the following information:

Column	Description
dvOp	The current operational state of the line (also specified by Device-State): <ul style="list-style-type: none"> 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 channel in normal operations mode: <ul style="list-style-type: none"> Idle indicates that no call is on the line. Busy indicates that the line is handling a call.
dvRq	The required state of the line as specified by Reqd-State: <ul style="list-style-type: none"> Down indicates that the line is required to be in a nonoperational state. Up indicates that the line is required to be in normal operations mode.
SAdm	The desired administrative state of the line (also specified by Desired-State): <ul style="list-style-type: none"> Down specifies that the line should terminate all operations and enter the down state. Up specifies that the line should come up in normal operations mode.
na1lg	The nailed group to which the line has been assigned.

See Also: ATMlines

Uptime

Description: On an APX 8000 unit, reports how long the primary controller and individual cards have been up. It also indicates the length of time since the secondary controller started communications with the primary. If a controller reboots or if communication between the two controllers is disrupted and then reestablished, the Uptime command reports the length of time since the secondary controller reestablished communications with the primary. Uptime does *not* report the version number of code used by the controllers, but reports the primary/secondary status of each controller. The code version for the controllers is obtained by using the Version command. The Uptime command shows only the code version number of all slot cards.

On a MAX TNT unit, the Uptime command reports how long the system has been up and how long individual cards have been up.

Permission level: System

Usage: `uptime` `[[-a] | [[shelf] slot]]`

Syntax element	Description
No arguments	Display the system uptime.
-a	For the primary controller on an APX 8000 unit, display the uptime for all slot cards. For the secondary controller, display the time that it started communicating with the primary controller. On a MAX TNT unit, display the uptime for all slot cards.
<i>slot</i>	Display the uptime for the specified slot card.
<i>shelf slot</i>	Display the uptime for the slot card specified by shelf and slot. The shelf number is always 1.

APX 8000 examples

For the primary controller, the following example shows the uptime for all slot cards in the Up state. (Cards that are not in the Up state are not reported.)

```
admin> uptime -a
18:25:52
{ shelf-1 slot-1 }      t3-card    2 days 00:40:31    9.0.0
{ shelf-1 slot-2 }      t3-card    2 days 00:40:31    9.0.0
{ shelf-1 slot-3 }      ether3-card 2 days 00:40:41    9.0.0
{ shelf-1 slot-4 }      ether3-card 2 days 00:40:41    9.0.0
{ shelf-1 slot-5 }      madd-card  2 days 00:39:47    9.0.0
{ shelf-1 slot-6 }      madd-card  2 days 00:39:47    9.0.0
{ shelf-1 slot-7 }      madd-card  2 days 00:39:47    9.0.0
{ shelf-1 slot-8 }      madd-card  2 days 00:39:47    9.0.0
{ shelf-1 slot-9 }      madd-card  2 days 00:39:47    9.0.0
{ shelf-1 slot-10 }     madd-card  2 days 00:39:47    9.0.0
{ shelf-1 slot-11 }     t3-card    2 days 00:40:31    9.0.0
{ shelf-1 slot-12 }     t3-card    2 days 00:40:31    9.0.0
```

```
{ shelf-1 slot-13 }      csmv-card    2 days 00:39:07    9.0.0
{ shelf-1 slot-14 }      csmv-card    2 days 00:39:07    9.0.0
{ shelf-1 slot-15 }      csmv-card    2 days 00:39:07    9.0.0
{ shelf-1 slot-16 }      csmv-card    2 days 00:39:07    9.0.0
{ shelf-1 slot-17 }      ether3-card   2 days 00:40:41    9.0.0
{ shelf-1 slot-18 }      ether3-card   2 days 00:40:41    9.0.0
{ shelf-1 slot-19 }      csmv-card    2 days 00:39:07    9.0.0
{ shelf-1 slot-24 }      ether3-card   2 days 00:40:41    9.0.0
{ shelf-1 slot-25 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-26 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-27 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-28 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-29 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-30 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-31 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-32 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-33 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-34 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-35 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-36 }      madd-card     2 days 00:39:47    9.0.0
{ shelf-1 slot-37 }      ether3-card   2 days 00:40:41    9.0.0
{ shelf-1 slot-38 }      ether3-card   2 days 00:40:41    9.0.0
{ shelf-1 slot-39 }      csmv-card    2 days 00:39:07    9.0.0
{ shelf-1 left-controller } shelf-controller 2 days 00:55:48
(PRIMARY )
{ shelf-1 right-controller } shelf-controller 2 days 00:39:40
(SECONDARY )
```

For the secondary controller, the following information is displayed:

```
admin> uptime -a
06:28:26
{ shelf-1 left-controller } [...] 0 days 00:40:37 ( SECONDARY )
{ shelf-1 right-controller } [...] 0 days 00:41:21 ( PRIMARY )
```

MAX TNT example

The following example shows the uptime for all slot cards in the Up state on a MAX TNT unit. (Cards that are not in the Up state are not reported.)

```
admin> uptime -a
19:15:26
{ shelf-1 slot-1 } 8t1-card 9 days 01:05:40 9.0.0
{ shelf-1 slot-2 } 4ether2-card 9 days 01:05:28 9.0.0
{ shelf-1 slot-3 } hdlc2-card 9 days 01:04:02 9.0.0
{ shelf-1 slot-4 } csmx-card 9 days 01:03:40 9.0.0
{ shelf-1 slot-6 } csmx-card 9 days 01:04:30 9.0.0
{ shelf-1 controller } shelf-controller 9 days 01:06:10 9.0.0
```

Userstat

Description: Displays user session status.

Permission level: System

Usage: `userstat [-s|-l|-d|-k sessionid | -a ipaddr | -u username | -o [format]]`

Syntax element	Description
-s	Show session information in an 80-character-wide format (the default).
-l	Show enhanced status information in a 140-character-wide format.
-d	Dump the output to the display, rather than show it one page at a time.
-k <i>sessionid</i>	Terminate a user session that uses PPP, SLIP, MP+, Telnet, Telnet binary, Raw TCP, or the terminal server. The -k option does not terminate Frame Relay or DTPT service types.
-a <i>ipaddr</i>	Show session information for a specified IP address.
-u <i>username</i>	Show session information for a specified username.
-o [<i>format</i>]	Restrict the output to specified fields. Following are the available formats: %i (Session ID) %l (Line/Channel) %s (Slot:Item) %r (Transmit Rate/Receive Rate) %d (Type of Service) %a (IP Address) %u (Username) %c (Connection Time) %t (Idle Time) %n (Dialed Number)

The default is %i %l %s %r %d %a %u %c %t %n.

Example: To display user session status:

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

The output contains the following fields:

Field	Description
SessionID	Unique ID assigned to the session.
Line/Chan	Physical address (<i>shelf.slot.line/channel</i>) of the network port on which the connection was established, such as a T1 line/channel. The shelf number is always 1.
Slot:Item	<i>Shelf:slot:item/logical-item</i> of the host port to which the call was routed. The shelf number is always 1.
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.) PPP (Point-to-Point Protocol) SLP (Serial Line IP) MPP (Multilink Protocol Plus™) MP (Multilink Protocol) FRY (Frame Relay) TLN (Telnet) BTN (Binary Telnet) TCP (raw TCP) TRM (Terminal Server) VCN (Virtual Connect) DTP (DTPT)
Address	IP address of the user.
Username	Name of the user.
Dialed# (displays only with -l option)	The number dialed to initiate this session.
ConnTime (displays only with -l option)	The amount of time (in hours:minutes:seconds format) since the session was established.
IdleTime (displays only with -l option)	The amount of time (in hours:minutes:seconds format) since data was last transmitted across the connection.

For an active TCP-Clear session, the login host's IP address is displayed in the Address field. For example:

```
admin> userstat

SessionID Line/Chan Slot:Item Tx/Rx Rate Svc Address Username
286993415 3.01.08/012 3:07:03/000 26400/26400 TCP 10.1.1.1 johnfan
<end user list> 1 active user(s)
```

Note: If the TCP-Clear connection fails (if the login attempt has not been successfully established between the TAOS unit and any of the specified login hosts), the Userstat command shows the zero address in the Address field.

If you use the **-o** option and indicate the codes for SessionID and Line/Channel information, the command shows only the following details:

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

Use the **-a** option to display information related to a known IP address. For example:

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

Use the **-u** option to display information related to a known username. For example:

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

If you have specified the **%f** for the Userstat-Format value, the caller's telephone number (if available) appears under the Calling# field of the command output. For example:

```
admin> userstat -l
SessionID Address Username Calling#
287695661 10.1.2.1 ed-p130 1119855014
<end user list> 2 active user(s)
```

To terminate a user session, include the **-k** option and session ID with the Userstat command. For example:

```
admin> userstat
SessionID Line/Chan Slot:Item Rate Svc Address Username
246986325 1.01.02/01 1:13:01/000 33600 PPP 100.100.8.2 100.100.8.2
<end user list> 1 active user(s)

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

Version

Description: Displays the current system software version.

Permission level: System

Usage: **version**

Example: To display the current system software version:

```
admin> version
Software version 1.2
```


View

Description: Changes the information displayed in the top or bottom status window.

Permission level: System

Usage: `view position status-type`

Syntax element	Description
position	The window position can be <code>top</code> , <code>bottom</code> , or <code>left</code> , indicating which area of the status window will be affected by the command.
status-type	<p>If the specified window position is <code>top</code> or <code>bottom</code>, the window can display one of the following types of status information:</p> <ul style="list-style-type: none"> • <code>general</code> (general status information) • <code>log</code> (the 32-message log buffer) • <code>line</code> (T1 line and channel status) <p>If the specified window position is <code>left</code>, the window can display one of the following types of status information:</p> <ul style="list-style-type: none"> • <code>connection</code> (WAN connection status) • <code>session</code> (management status)

Example: To display session information:

```
admin> view left session
```

```

4 Sessions
0 - serial - admin
1 - telnet - tommy
2 - telnet - super
3 - telnet - pubs

1/13/8   RA .....

M: 48 L: info Src: shelf-1/controller
48 out of 48 modems passed POST

Issued: 16:48:02, 09/27/2000

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

See Also: Connection, Line, Log, Status

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 NVRAM.

Note: If the working profile has an index field (a parameter followed by an asterisk), that parameter must have a value or the write is not allowed. 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]`

Syntax element	Description
<code>-f</code>	Force the write without prompting for confirmation, overwriting an existing profile if one exists with the same index.

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` flag on the Write command line. Note that the write always occurs if the profile has not been written previously.

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 = mpp
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 +
ppp-options = { "" "" stac 1524 no 600 600 }
mp-options = { 1 1 2 }
mpp-options = { "" quadratic transmit 1 1 15 5 10 70 }
tcp-clear-options = { "" 0 }
answer-options = { }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""

admin> write
CONNECTION/newyork written
```

See Also: List, New, Read, Set

Profile and Parameter Reference

2

Note: All references to redundant shelf controllers apply to APX 8000 units only.

Numeric	2-2
A.....	2-4
B.....	2-66
C.....	2-75
D.....	2-119
E.....	2-151
F.....	2-167
G.....	2-189
H.....	2-196
I	2-209
K.....	2-243
L.....	2-245
M	2-270
N.....	2-299
O.....	2-313
P.....	2-329
Q.....	2-365
R.....	2-367
S.....	2-394
T.....	2-455
U.....	2-499
V.....	2-509
W	2-521
X.....	2-523
Y.....	2-525

Numeric

1-Char-Sequence

Description: Specifies a character to be used as a trigger to forward data and the next character.

Usage: Specify a hexadecimal value. The default is 03.

Example: `set 1-char-sequence = 05`

Location: Connection *station* > Visa2-Options

See Also: 2-Char-Sequence

2-Char-Sequence

Description: Specifies two character values of a sequence to be used as a trigger to forward data, and the two characters following the sequence.

Usage: Specify a hexadecimal value. The default is 00:03 00:00.

Example: `set 2-char-sequence = 00:05:00:00`

Location: Connection *station* > Visa2-Options

See Also: 1-Char-Sequence

7-Even

Description: Specifies whether the TAOS unit applies 7-bit even parity to data it sends toward a dial-in terminal-server user.

Usage: Specify Yes or No. The default is No. Accept the default value for most applications.

- Yes enables the use of 7-bit even parity for data sent to dial-in terminal-server users.
- No specifies 8-bit communication, in which no parity bit applies.

Example: `set 7-even = no`

Dependencies: If terminal services are disabled, 7-Even does not apply.

Location: Terminal-Server > Modem-Configuration

See Also: Modem-Configuration

8E1

Description: Specifies the action to take when the code image for an E1 card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, T3, UDS3, UE1, Unknown-Cards, UT1

8T1

Description: Specifies the action to take when the code image for a T1 card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, T3, UDS3, UE1, Unknown-Cards, UT1

A

Acct-Drop-Stop-On-Auth-Fail

Description: Specifies whether Remote Authentication Dial-In User Service (RADIUS) Accounting Stop packets are dropped for connections that fail authentication.

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

- 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.

Example: `set acct-drop-stop-on-auth-fail = yes`

Location: External-Auth > Rad-Acct-Client

See Also: Acct-ID-Base, Acct-Key, Acct-Limit-Retry, Acct-Port, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Stop-Only, Acct-Timeout

Acct-Host

Description: Specifies a Remote Authentication Dial-In User Service (RADIUS) accounting server for the TAOS 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 TAOS 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 *station* > UsrRad-Options

See Also: Acct-ID-Base, Acct-Key, Acct-Port, Acct-Reset-Time, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Timeout, Acct-Type, UsrRad-Options

Acct-ID-Base

Description: Specifies whether the numeric base of the Remote Authentication Dial-In User Service (RADIUS) Acct-Session-ID attribute is 10 or 16. You can set Acct-ID-Base globally and for each connection.

Usage: Specify one of the following values:

- Acct-Base-10 (the default) specifies a decimal base.
- Acct-Base-16 specifies a hexadecimal base.

The value you specify controls how the TAOS unit presents the Acct-Session-ID attribute to the accounting server.

Example: `set acct-id-base = acct-base-10`

Dependencies: Consider the following:

- If Acct-Type does not specify RADIUS, Acct-ID-Base 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.
- The Acct-Session-ID attribute is defined in section 5.5 of the RADIUS accounting specification.

Location: Connection *station* > UsrRad-Options, External-Auth > Rad-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-Key, Acct-Limit-Retry, Acct-Port, Acct-Reset-Time, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Stop-Only, Acct-Timeout, Acct-Type, Rad-Acct-Client, UsrRad-Options

Acct-Key

Description: Specifies a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control Plus (TACACS+) shared secret. A shared secret acts as a password between the TAOS unit and the accounting server.

Usage: Specify the text of the shared secret. If you specify a null value, the system logs the following warning:

```
warning: acct-key is empty (bad for security)
```

Example: `set acct-key = unit1`

Dependencies: If Acct-Type does not specify RADIUS or TACACSPlus, Acct-Key does not apply.

Location: Connection *station* > UsrRad-Options, External-Auth > Rad-Acct-Client, External-Auth > TacPlus-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Limit-Retry, Acct-Port, Acct-Reset-Time, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Stop-Only, Acct-Timeout, Acct-Type, Rad-Acct-Client, TacPlus-Acct-Client, UsrRad-Options

Acct-Limit-Retry

Description: Specifies the maximum number of retries for Accounting packets.

When the TAOS unit is configured for Remote Authentication Dial-In User Service (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 TAOS 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 TAOS unit always makes at least one attempt. For example, if you set the number of retries to 10, the unit makes 11 attempts: the original attempt plus 10 retries.

Example: `set acct-limit-retry = 10`

Location: External-Auth > Rad-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Key, Acct-Port, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Stop-Only, Acct-Timeout

Acct-Port

Description: Specifies the UDP destination port to use for external accounting requests. When using Remote Authentication Dial-In User Service (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. For RADIUS, the default in a Connection profile is 1646, and the default in the External-Auth profile is 0 (zero). For Terminal Access Controller Access Control Plus (TACACS+), the default is 49.

Example: `set acct-port = 1500`

Dependencies: If Acct-Type does not specify RADIUS or TACACSPlus, Acct-Port does not apply.

Location: Connection *station* > UsrRad-Options, External-Auth > Rad-Acct-Client, External-Auth > TacPlus-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Limit-Retry, Acct-Key, Acct-Reset-Time, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Stop-Only, Acct-Timeout, Acct-Type, Rad-Acct-Client, TacPlus-Acct-Client

Acct-RADIUS-Compat

Description: Enables or disables vendor-specific attribute (VSA) compatibility mode when the unit is using Remote Authentication Dial-In User Service (RADIUS) for accounting purposes.

Usage: Specify one of the following settings:

- Old-Ascend (the default) specifies that the 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. All attributes are sent in standard RFC format.
- 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: At this time, only NavisRadius supports 16-bit VSAs.

Example: `set acct-radius-compat = vendor-specific`

Location: External-Auth > Rad-Acct-Client

See Also: Auth-RADIUS-Compat, Call-Log-RADIUS-Compat, RADIUS-Server-Compat

Acct-Reset-Time

Description: Specifies the number of seconds that must elapse before the TAOS unit returns to using the primary Remote Authentication Dial-In User Service (RADIUS) accounting server.

Usage: Specify the number of seconds. The default is 0 (zero), which specifies that the TAOS 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 Acct-Server-N.

Location: External-Auth > Rad-Acct-Client

See Also: Acct-ID-Base, Acct-Key, Acct-Port, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Timeout, Acct-Type, Rad-Acct-Client

Acct-Server-N

Description: Specifies the IP addresses of up to three external accounting servers. The TAOS 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 Acct-Type does not specify RADIUS or TACACSPlus, Acct-Server-N does not apply.
- If the TAOS unit connects to a server other than server #1, and Acct-Reset-Time is set to 0 (zero), the unit continues to use that server until it fails to service requests, even if the first server comes back online. If Acct-Reset-Time is set to a value other than 0 (zero), the TAOS 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, External-Auth > TacPlus-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Key, Acct-Limit-Retry, Acct-Port, Acct-Reset-Time, Acct-Sess-Interval, Acct-Src-Port, Acct-Stop-Only, Acct-Timeout, Acct-Type, Rad-Acct-Client, TacPlus-Acct-Client

Acct-Sess-Interval

Description: Specifies the number of seconds between Remote Authentication Dial-In User Service (RADIUS) accounting reports recording 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 Acct-Type does not specify RADIUS, Acct-Sess-Interval does not apply.

Location: External-Auth > Rad-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Key, Acct-Limit-Retry, Acct-Port, Acct-Reset-Time, Acct-Server-N, Acct-Src-Port, Acct-Stop-Only, Acct-Timeout, Acct-Type, Rad-Acct-Client

Acct-Src-Port

Description: Represents the UDP source port to use for Remote Authentication Dial-In User Service (RADIUS) accounting.

Usage: Specify a value from 0 to 65535. The default is 0 (zero), which specifies that the TAOS unit selects the source port from the nonprivileged port range (1024–2000).

Example: `set acct-src-port = 3278`

Dependencies: The TAOS unit uses the source port number to demultiplex the RADIUS reply packets to the appropriate slot cards. The system uses a separate source port for each slot card. On the TAOS unit, the actual source port is the value of Acct-Src-Port plus the slot number, where the slot number is 0 (zero) for the shelf controller. So, if you set Acct-Src-Port to 1000, packets originating from the shelf controller 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, External-Auth > TacPlus-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Key, Acct-Limit-Retry, Acct-Port, Acct-Reset-Time, Acct-Server-N, Acct-Sess-Interval, Acct-Stop-Only, Acct-Timeout, Acct-Type, Rad-Acct-Client, TacPlus-Acct-Client

Acct-Stop-Only

Description: Specifies whether the TAOS unit should send an Accounting Stop packet that does not contain a username. (At times, the unit can send an Accounting Stop packet to the Remote Authentication Dial-In User Service (RADIUS) server without having sent an Accounting Start packet. These Stop packets have no username.)

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

- Yes specifies that the TAOS unit should send an Accounting Stop packet even if it does not contain a username.
- No specifies that the TAOS unit should not send an Accounting Stop packet if it does not contain a username.

Example: `set acct-stop-only = no`

Location: External-Auth > Rad-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Key, Acct-Limit-Retry, Acct-Port, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Timeout

Acct-Timeout

Description: Specifies the amount of time (in seconds) that the TAOS unit waits for a response to a Remote Authentication Dial-In User Service (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 TAOS unit sends the accounting request to the next server specified by Acct-Server-N. If all RADIUS accounting servers are busy, the TAOS 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 60. The default for a Connection profile is 1. The default for the External-Auth profile is 0 (zero).

Example: `set acct-timeout = 5`

Dependencies: If Acct-Type does not specify RADIUS, Acct-Timeout does not apply. You use Acct-Timeout only for RADIUS accounting. Because Terminal Access Controller Access Control Plus (TACACS+) uses TCP, it has its own timeout method.

Location: Connection *station* > UsrRad-Options, External-Auth > Rad-Acct-Client

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Key, Acct-Limit-Retry, Acct-Port, Acct-Reset-Time, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Stop-Only, Acct-Type, Rad-Acct-Client, UsrRad-Options

Acct-Type

Description: Specifies whether to use Remote Authentication Dial-In User Service (RADIUS) accounting, Terminal Access Controller Access Control Plus (TACACS+) 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 (the default) disables accounting.
- RADIUS enables RADIUS accounting.
- TACACSPlus enables TACACS+ accounting.

To set accounting policy for a particular connection, specify one of the following values in the Connection profile:

- Global (the default) specifies that the TAOS unit sends accounting information to one of the accounting servers specified by the External-Auth profile.
- Local specifies that the TAOS unit sends accounting information to the accounting server specified by Acct-Host in the Connection profile.
- Both specifies that the TAOS unit sends accounting information to both the global and local servers.

Example: `set acct-type = acct-radius`

Dependencies: If you set Acct-Type to RADIUS or TACACSPlus, you must set Acct-Server to specify at least one accounting server, and that server must be running a version of the daemon that specifically supports accounting.

Location: Connection *station* > UsrRad-Options, External-Auth

See Also: Acct-ID-Base, Acct-Key, Acct-Port, Acct-Reset-Time, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Timeout, Rad-Acct-Client, TacPlus-Acct-Client

ACK-Threshold

Description: Specifies the threshold for triggering an acknowledgment while receiving data packets. As soon as the specified number of packets is received, the TAOS unit sends an acknowledgment back (regardless of the value of T1-Duration).

Usage: Specify an integer from 1 to 63. The default is 6.

Example: `set ack-threshold = 10`

Dependencies: The value you specify for ACK-Threshold cannot be greater than the value of Window-Size.

Location: SS7-Gateway > Transport-Options

See Also: Device-ID, Heart-Beat, T1-Duration, T2-Duration, T3-Duration, Window-Size

Action

Description: Specifies the action the TAOS unit takes when it finds a matching route in a route-filter specification.

Usage: Specify one of the following values:

- None (the default) specifies that the TAOS unit takes no action.
- Accept directs the TAOS unit to accept the route and allow it to affect the routing table.
- Deny directs the TAOS unit to deny the route and keep it from affecting the routing table.
- Add directs the TAOS unit to add the Add-Metric value to the route metric, and to accept the route.

Location: Filter > Input-Filters > Route-Filter *filter-name*,
Filter > Output-Filters > Route-Filter *filter-name*

See Also: Add-Metric, Input-Filters, Output-Filters, Route-Address, Route-Filter (subprofile), Route-Mask, Source-Address, Source-Address-Mask

Activation

Description: Selects the signals, at the serial WAN port, that indicate that the Data Circuit-terminating Equipment (DCE) is ready to connect. Flow control is always handled by the Clear To Send (CTS) signal.

Usage: Specify one of the following values:

- Static (the default) specifies that the TAOS unit does not use flow control signals because the DCE is always connected.
- DSR-Active specifies that the DCE raises the Data Set Ready (DSR) signal when it is ready.
- DCD-DSR-Active specifies that the DCE raises the DSR and Data Carrier Detect (DCD) signals when it is ready.

Example: `set activation = static`

Location: SWAN {shelf-*N* slot-*N* *N*} > Line-Config,
DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config

See Also: Call-Route-Info, Line-Config, Nailed-Group, Trunk-Group

Active

Description: Activates an interface, profile, route, or feature.

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

- Yes activates the interface, profile, route, or feature. In the BOOTP-Relay subprofile, setting Active to Yes enables the TAOS unit to forward BOOTP requests and responses between specified BOOTP servers and booting hosts on any of the TAOS unit's IP interfaces.
- No makes the interface, profile, route, or feature unavailable for use.

Example: `set active = yes`

Location: ATMSVC-Route *name*, Connection *station*,
Connection *station* > IP-Options > OSPF-Options,
Connection *station* > IP-Options > TOS-Options, Frame-Relay *fr-name*,
IP-Interface {{shelf-*N* slot-*N* *N*} *N*} > OSPF, IP-Global > BOOTP-Relay,
IP-Global > DHCP-Server, IPsec *name*, IPsec *name* > Send-AH, IPsec *name* > Recv-AH,
IP-Sec *name* > Send-ESP, IPsec *name* > Recv-ESP, Multi-Link-FR *name*,
VoIP {*x y*} > TOS-Options, VRouter *name*

See Also: Address-Prefix, BOOTP-Relay, BOOTP-Servers, Enabled, Interface-Address, Name, Tunnel-Address

Active-Enabled

Description: In an SNMPv3-Notifications or SNMPv3-Target-Param profile, specifies whether the profile is used to generate notifications. In a Trap profile, specifies whether traps are sent to the host specified by the profile. In a User or SNMPv3-USM-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.

Usage: Specify Yes or No.

- Yes specifies that the profile is used to generate notifications, that traps are sent, or that the profile is enabled.
- No (the default) specifies that the profile is not used to generate notifications, that traps are not sent, or that the profile is disabled.

Example: `set active-enabled = yes`

Location: SNMPv3-Notification *name*, SNMPv3-Target-Param *name*, SNMPv3-USM-User *name*, User *name*, Trap *name*

See Also: Auth-Protocol, Host-Port, Msg-Proc-Model, Name, Notify-Tag-List, Password, Priv-Protocol, Read-Write-Access, Security-Level, Security-Model, Security-Name, Tag, Target-Params-Name

Active-Route

Description: Specifies whether the TAOS unit adds a static route to the routing table.

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 causes the TAOS unit to add it to the routing table.
- No disables the route. An inactive route does not affect packet routing.

Example: `set active-route = yes`

Dependencies: The default route for an IP-Route profile always has 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 *name*, IPX-Route *name*

See Also: ASE-Tag, ASE-Type, Cost, Dest-Address, Dest-Network, Gateway-Address, Hops, Metric, Name, Preference, Private-Route, Profile-Name, Server-Node, Server-Socket, Server-Type, Third-Party, Ticks

Add-Metric

Description: Specifies the metric to add to the route metric for a route filter.

Usage: Specify a number. 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: Add-Metric does not apply unless Action is set to Add.

Location: Filter > Input-Filters > Route-Filter *filter-name*,
Filter > Output-Filters > Route-Filter *filter-name*

See Also: Action, Input-Filters, Output-Filters, Route-Address, Route-Filter (subprofile), Route-Mask, Source-Address, Source-Address-Mask

Add-Persistence

Description: Specifies the number of seconds that average line utilization (ALU) must persist beyond the Target-Utilization threshold before the TAOS unit adds bandwidth from available channels. When adding bandwidth, the unit adds the number of channels specified by Increment-Channel-Count.

Usage: Specify an integer from 1 to 300. The default is 5.

Example: `set add-persistence = 15`

Dependencies: When the Seconds-History value is high, Add-Persistence has little effect.

Location: Answer-Defaults > MPP-Answer, Connection *station* > MPP-Options

See Also: Bandwidth-Monitor-Direction, Base-Channel-Count, Decrement-Channel-Count, Dynamic-Algorithm, Increment-Channel-Count, Maximum-Channels, Minimum-Channels, MPP-Answer, MPP-Options, Seconds-History, Sub-Persistence, Target-Utilization

Address-Prefix

Description: Specifies the address prefix of the Asynchronous Transfer Mode (ATM) address assigned to the interface in an ATM-Interface profile.

Usage: For an ATM End System Address (AESA) format, specify a value for the first 26 digits of the 40-digit hexadecimal number. For an E.164 address, the prefix is the same as the entire address.

Example: `set address-prefix = 1234567890123456`

Location: ATMSVC-Route *name*

See Also: Interface-Address

Address-Pool

Description: Specifies the address pool from which the TAOS unit can assign a caller an IP address.

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 TAOS unit gets IP addresses from the first defined address pool.

Location: Connection *station* > IP-Options

See Also: Assign-Address, Assign-Count, IP-Options, Pool-Base-Address, Pool-Summary

Admin-State

Description: A profile that stores the desired state and Simple Network Management Protocol (SNMP) interface number of a device. The profile resides in NVRAM, so a physical device keeps the same interface number across system reset or power failures.

Usage: To make Admin-State the working profile and list its contents, use the Read and List commands. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make Admin-State profile for the device in slot 9 the working profile and list its contents:

```
admin> read admin-state {1 9 19}
ADMIN-STATE/{ shelf-1 slot-9 19 } read

admin> list
[in ADMIN-STATE/{ shelf-1 slot-9 19 }]
device-address* = { shelf-1 slot-9 19 }
slot-type = madd-card
snmp-interface = 189
modem-table-index = 0
desired-state = admin-state-up
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ADMIN-STATE written
```

Dependencies: At system startup, the TAOS unit reads the Admin-State profiles. If the addressed device is not present in the system and has been replaced by a device of another type, the TAOS unit deletes the profile associated with the device. The next time the system is reset or power cycled, the old device's SNMP interface number is made available for reassignment. Removing a slot card and leaving the slot empty does not, however, free up interface numbers. If you reinstall the slot card, the TAOS unit reassigns the same interface number.

In addition, removing a slot card and replacing it with a slot card of another type does not immediately free up the old interface numbers. New numbers are assigned to the new slot card, and the old numbers are made available at the next power cycle or system reset.

See Also: Desired-State, Device-Address, Modem-Table-Index, Slot-Type, SNMP-Interface

Admin-State-Perm-If

Description: A profile that holds information about the TAOS unit's nailed-up interfaces. The system creates a profile for an active nailed-up interface and assigns it an interface index.

Usage: To make Admin-State-Perm-If the working profile and list its contents, use the Read and List commands. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Admin-State-Perm-If profile frswan1 the working profile and list its contents:

```
admin> read admin-state-perm-if frswan1
ADMIN-STATE-PERM-IF/frswan1 read

admin> list
[ in ADMIN-STATE-PERM-IF/frswan1 ]
station* = frswan1
snmp-interface = 19
desired-state = admin-state-up
desired-trap-state = trap-state-enabled
inet-profile-type = 1
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ADMIN-STATE-PERM-IF written
```

See Also: Desired-State, Desired-Trap-State, Inet-Profile-Type, SNMP-Interface, Station

Admin-State-Phys-If

Description: A profile that holds information about the system's physical interfaces. The system creates a profile for each of its physical interfaces. The Admin-State-Phys-If profile contains only read-only settings.

Usage: To make Admin-State-Phys-If the working profile and list its contents, use the Read and List commands.

Example: To make the Admin-State-Phys-If profile for the device in slot 13 the working profile and list its contents:

```
admin> read admin-state-phys-if {1 13 1}
ADMIN-STATE-PHYS-IF/{ shelf-1 slot-13 1 } read
```

```
admin> list
[in ADMIN-STATE-PHYS-IF/{ shelf-1 slot-13 1 }]
device-address* = { shelf-1 slot-13 1 }
slot-type = hdlc2-card
snmp-interface = 0
modem-table-index = 0
desired-state = admin-state-up
desired-trap-state = trap-state-enabled
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ADMIN-STATE-PHYS-IF written
```

See Also: Desired-State, Desired-Trap-State, Device-Address, Modem-Table-Index, Slot-Type, SNMP-Interface

Advanced-Agent-Enabled

Description: Indicates whether the Advanced MIB is in use. The Advanced MIB is the name of the SNMP MIB previously called the WAN MIB.

Usage: The Advanced-Agent-Enabled setting is read only. Yes indicates that the Advanced MIB is in use. No indicates that the Advanced MIB is not in use.

Example: advanced-agent-enabled = yes

Location: Base

See Also: AIM-Enabled, Countries-Enabled, Data-Call-Enabled, D-Channel-Enabled, Firewalls-Enabled, Frame-Relay-Enabled, MAXLink-Client-Enabled, Modem-Dialout-Enabled, Multi-Rate-Enabled, Network-Management-Enabled, PHS-Support, R2-Signaling-Enabled, Selectools-Enabled, Serial-Number, Shelf-Number, Software-Level, Software-Revision, Software-Version, Switched-Enabled, Toggle-Screen

AESA-Address

Description: A subprofile that enables you to configure an ATM End System Address (AESA).

Usage: With an ATM-Interface profile as the working profile, enter `list svc-options atm-address aesa-address`. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the AESA-Address subprofile:

```
admin> list svc-options atm-address aesa-address
[in ATM-INTERFACE/{any-shelf any-slot 0} 0]:svc-options:+
format = undefined
idp-portion = { " " " " }
dsp-portion = { " " " " " " }
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options > ATM-Address, Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr, Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr

See Also: DSP-Portion, Format, IDP-Portion

AFI

Description: Specifies the hexadecimal code that identifies the kind of ATM End System Address (AESA), such as DCC, ICD, or the E.164 part of the AESA address, as well as the syntax of the rest of the address.

Usage: The AFI you specify is one byte, which contains two hex digits. For example, 0x39 specifies DCC-AESA, 0x47 specifies ICD-AESA, and 0x45 specifies E164-AESA. The default is null.

Example: `set afi = dcc-aesa`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options > ATM-Address > AESA-Address > IDP-Portion, Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr > AESA-Address > IDP-Portion, Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr > AESA-Address > IDP-Portion

See Also: IDI

Agent-Mode

Description: Specifies whether the TAOS unit operates as a Foreign Agent, a Home Agent, or both on a tunnel-by-tunnel basis in an Ascend Tunnel Management Protocol (ATMP) configuration.

Usage: Specify one of the following values:

- Tunnel-Disabled (the default) disables ATMP.
- Home-Agent specifies that the TAOS unit operates as a Home Agent.
- Foreign-Agent specifies that the TAOS unit operates as a Foreign Agent.
- Home-And-Foreign-Agent specifies that the TAOS unit 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

See Also: Agent-Type, Password, Retry-Limit, Retry-Timeout, UDP-Port

Agent-Type

Description: Specifies whether the TAOS unit communicates with the home network as a gateway or a router in an Ascend Tunnel Management Protocol (ATMP) configuration.

Usage: Specify one of the following values:

- Gateway-Home-Agent (the default) specifies that the Home Agent delivers tunneled data to the home network without routing. The tunneled data does not bring up a connection to the home network, so the connection between the Home Agent and the home network must already be up, as in a nailed-up connection.
- Router-Home-Agent specifies that the Home Agent routes tunneled data to the home network.

Example: `set agent-type = router-home-agent`

Dependencies: You must set Agent-Mode to Home-Agent for the Agent-Type setting to apply.

Location: ATMP

See Also: Agent-Mode, Password, Retry-Limit, Retry-Timeout, UDP-Port

Aggregate

Description: Enables or disables aggregation of the Bit-Rate values of multiple Virtual Circuits (VCs) using this shaper.

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

- Yes specifies that if N VCs are using this shaper, the throughput of each VC is Bit-Rate/ N .
- No specifies that aggregation is not used.

Example: `set aggregate = yes`

Location: DS3-ATM {shelf- N slot- N N } > Line-Config > Traffic-Shapers > Traffic-Shapers N ,
OC3-ATM {shelf- N slot- N N } > Line-Config > Traffic-Shapers > Traffic-Shapers N

See Also: Bit-Rate, Enabled, Max-Burst-Size, Peak-Rate, Priority

AH-Type

Description: Specifies the type of authentication transform to use.

Usage: Specify one of the following values:

- None (the default) specifies that authentication is not in use.
- MD5 specifies MD5 mode, described in RFC 1828.
- SHA1 specifies SHA1 mode, described in RFC 1852.
- MD5-HMAC specifies version-2 MD5, currently in draft.
- SHA1-HMAC specifies version-2 SHA1, currently in draft.

Example: `set ah-type = md5`

Location: IPSec *name* > Recv-AH, IPSec *name* > Send-AH

See Also: Active, Key, Replay-Protection, SPI

AIM-Enabled

Description: Indicates whether the unit enables Ascend Inverse Multiplexing (AIM).

Usage: The AIM-Enabled setting is read only. Yes indicates that AIM is enabled. No indicates that AIM is not enabled.

Example: aim-enabled = yes

Location: Base

See Also: Data-Call-Enabled, Frame-Relay-Enabled, MAXLink-Client-Enabled, Modem-Dialout-Enabled, Multi-Rate-Enabled, R2-Signaling-Enabled, Switched-Enabled

AIS-Receive

Description: Indicates whether the remote end is sending an Alarm Indication Signal (AIS) on the T1 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. True indicates that the remote end is sending an AIS. False indicates that the remote end is not sending an AIS.

Example: ais-receive = False

Location: T1-Stat {shelf-*N* slot-*N* *N*}, T3-Stat {shelf-*N* slot-*N* *N*}

See Also: Yellow-Receive

Alarm-Enabled

Description: Specifies whether the TAOS unit traps alarm events and sends a traps Protocol Data Unit (PDU) to the Simple Network Management Protocol (SNMP) manager when one of the following events occurs:

- ColdStart
- WarmStart
- LinkDown
- LinkUp
- FRLinkUp
- FRLinkDown
- EventOverwrite
- McastMonitor
- LanModem
- Dirdo
- PowerSupply
- ConfigChange
- SysClockDrifted

PrimaryEmpty
SecondaryEmpty
SuspectAccessResrc
WatchdogWarning
Controllerswitchover
WanLineStateChange
CallLogDroppedPkt
MegacoLinkStatus
CntrReduAvail
PctfiTrunkStatusChange
NoResourceAvailable
slotCardReset
atmpAgentErrorSent
sysLastRestartReason

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

- Yes specifies that the TAOS unit sends alarm-event traps to the host specified by the Host-Address parameter.
- No specifies that the TAOS unit does not send alarm-event traps.

Example: `set alarm-enabled = yes`

Location: Trap *host-name*

See Also: Community-Name, Host-Address, Host-Name, Port-Enabled, Security-Mode

Alarm-Temperature-Trigger

Description: Specifies a temperature threshold setting.

Usage: Specify a number from 0 to 60 degree Celsius. The default is 55.

Example: `set alarm-temperature-trigger = 50`

Dependencies: If the temperature passes the Alarm-Temperature-Trigger threshold, the system generates an Alarm event, the Alarm Relay on the shelf controller is turned on, and the Alarm LED on the front panel of the fantray is lit.

Location: Thermal

See Also: High-Temperature-Trigger, Low-Temperature-Trigger

Alert-Progress-Indicator

Description: Specifies the type of call-progress events captured and reported by the MultiVoice gateway in the Q.931 Alert message progress-indicator information element (IE).

Usage: Specify one of the following values:

- No-Progress-Indicator (the default) disables alert reporting of call-routing events on the egress switched telephone network.
- None-End2End-ISDN specifies that the egress MultiVoice gateway reports when calls are connected to an egress switched telephone network that does not use ISDN signaling. The egress switched telephone network can support robbed-bit or detectable DTMF.
- Dest-Non-ISDN specifies that the egress MultiVoice gateway reports when calls are connected to an egress switched telephone network that does not use ISDN signaling (for example, a transit network or private network) and that does not return call-progress signals to the MultiVoice gateway.
- Orig-Non-ISDN specifies that the ingress MultiVoice gateway reports when calls are received from a local switched telephone network that does not use ISDN signaling (for example, a transit network or private network) and that does not provide call-progress signals to the MultiVoice gateway.
- Return-To-ISDN specifies that the egress MultiVoice gateway reports when calls connected across a transit network are routed back on to a trunk supporting ISDN signaling.
- Interworking-Occurred specifies that the egress MultiVoice gateway reports whether interworking occurs upon connection to the switched telephone network. Internetworking events occur when the selected bearer capability is not supported or when a resource or route with the preferred capability is not available.
- Inband-Info-Available specifies that the egress MultiVoice gateway reports whether inband call-progress signaling or other supported non-ISDN signaling is available from the switched telephone network for the connected call.

Example: `set alert-progress-indicator = dest-non-isdn`

Location: VoIP { x y } > Pstn-Attribute

See Also: Proceed-Progress-Indicator

All-Calls-Are-Fax

Description: Specifies whether the TAOS unit handles all incoming calls as IP fax calls.

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

- Yes specifies that the TAOS unit handles all incoming calls as IP fax calls.
- No specifies that the TAOS unit authenticates the call on the basis of Direct Inward Dialing (DID) numbers or Dialed Number Information Service (DNIS) numbers, depending on the value specified by Fax-Incoming-Call-Type.

Example: `set all-calls-are-fax = yes`

Dependencies: A TAOS unit authenticates a call on the basis of the values specified by the All-Calls-Are-Fax and Fax-Incoming-Call-Type parameters as follows:

All-Calls-Are-Fax	Fax-Incoming-Call-Type	TAOS unit behavior
Yes	Redialer	Receives all incoming calls as redialer-type fax calls.
Yes	DID	Treats all incoming calls as DID-type fax calls.
No	DID	Authenticates the call against the DID numbers in the Fax-DID array.
No	Redialer	Authenticates the call against the DNIS numbers in the Fax-DNIS array.

Location: IP-Fax

See Also: Fax-Incoming-Call-Type

Allow-As-Client-DNS-Info

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

A client DNS configuration defines DNS server addresses that the TAOS unit or the Virtual Router (VRouter) presents to WAN connections during IP Control Protocol (IPCP) negotiation. The client DNS configuration provides a way to protect your local DNS information from WAN users. Client DNS has two levels: a global configuration (in the IP-Global profile) that applies to all PPP connections, and a connection-specific configuration (in a Connection profile). The TAOS unit or VRouter uses the global client addresses only if none are specified for the particular connection.

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

- Yes specifies that the TAOS unit or the VRouter makes the local DNS servers accessible to PPP connections if the client DNS servers are unavailable.
- No specifies that the TAOS unit or the VRouter does not make local DNS servers accessible to PPP connections if the client DNS servers are unavailable. To isolate local network information for the VRouter, specify No.

Example: `set allow-as-client-dns-info = no`

Location: IP-Global, VRouter *name*

See Also: Client-DNS-Addr-Assign, Client-DNS-Primary-Addr, Client-DNS-Secondary-Addr, Client-Primary-DNS-Server, Client-Secondary-DNS-Server, Connection, DNS-Primary-Server, DNS-Secondary-Server

Allow-Auth-Config-Rqsts

Description: Specifies whether the TAOS unit sends external authentication requests to the Remote Authentication Dial-In User Service (RADIUS) server.

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

- Yes specifies that the unit sends external authentication requests to the RADIUS server.
- No specifies that the unit does not send external authentication requests to the RADIUS server.

Example: `set allow-auth-config-rqsts = no`

Location: External-Auth > Rad-Auth-Client

See Also: Auth-RADIUS-Compat

Allow-Code

Description: Enables or disables permission to upload code to the TAOS unit and use the following code-level commands:

- Format (to prepare a flash card for use)
- Fsck (to check the file system on a flash card)

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

- Yes grants permission to upload code to the TAOS unit.
- No denies permission to upload code to the TAOS unit.

Example: `set allow-code = yes`

Location: User *name*

See Also: Allow-Diagnostic, Allow-Password, Allow-System, Allow-Termserve, Allow-Update

Allow-Coder-Fallback

Description: Enables or disables selection of an alternate codec if the gateway is unable to select its preferred codec (the codec specified by Packet-Audio-Mode).

Normally, an H.323 stack advertises a list of supported audio codecs. If the preferred codec is present on a list received from a remote gateway, that codec is always selected. Otherwise, the system selects an alternate codec that matches one from its supported list. You can use the Allow-Coder-Fallback value to override the default system behavior and force the gateway to reject the call if it is unable to select its preferred codec.

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

- Yes enables selection of an alternate codec.
- No disables selection of an alternate codec.

Example: `set allow-coder-fallback = no`

Dependencies: Consider the following:

- If Allow-Coder-Fallback is set to Yes, you can prevent the system from selecting a G.711 codec as an alternate codec by setting Allow-G711-Fallback to No. The system terminates the call if G.711 is the only available choice and it is not the preferred codec.
- The Allow-Coder-Fallback value affects Voice over IP (VoIP), fax, and transparent modem calls.

Location: VoIP {x y}

See Also: Allow-G711-Fallback

Allow-Diagnostic

Description: Enables or disables permission to use the following diagnostic commands:

Command	Description
Callroute	Display the call routing database.
Clock-Source	Display clock-source statistics.
Debug	Enable or disable diagnostic output.
Device	Bring a device up or down.
DS3link	Carry out a diagnostic session with an unchannelized DS3 card.
E1-Stats	Report DS1-level line errors on E1 cards.
Ether-Display	Display the contents of received Ethernet packets.
FE-Loop	Perform a line loopback for a T1 or E1 card.
FWALLdblog	Display firewall messages. (The FWALLdblog command is not supported at this time.)
FWALLversion	Display the firewall versions supported by the current system software. (The FWALLversion command is not currently supported.)
If-Admin	Administer an interface.
NSlookup	Perform a Domain Name System (DNS) lookup.
Open	Start a session with a slot card.
Ping	Ping the specified host.
PRIdisplay	Display general PRI messages.
Rlogin	Open an Rlogin session.
Slot	Administer a slot card.
T1-Stats	Report DS1-level line errors on T1 and T3 cards.
Telnet	Open a Telnet session.
Traceroute	Display route statistics.
Uptime	Report how long the system has been up and how long individual cards have been up.

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

- Yes grants permission to use diagnostic commands.
- No denies permission to use diagnostic commands.

Example: `set allow-diagnostic = yes`

Location: User *name*

See Also: Allow-Code, Allow-Password, Allow-System, Allow-Termserve, Allow-Update

Allow-G711-Fallback

Description: Enables or disables selection of the G.711 codec in the event that the gateway is unable to select its preferred codec.

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

- Yes enables selection of the G.711 codec.
- No disables selection of the G.711 codec.

Example: `set allow-g711-fallback = no`

Dependencies: Consider the following:

- Allow-G711-Fallback does not apply if Allow-Coder-Fallback is set to No.
- If Allow-Coder-Fallback is set to Yes, you can prevent the system from selecting a G.711 codec as an alternate codec by setting Allow-G711-Fallback to No. The system terminates the call if G.711 is the only available choice and it is not the preferred codec.

Location: VoIP {*x y*}

See Also: Allow-Coder-Fallback, G711-Transparent-Data

Allow-Password

Description: Enables or disables permission to view passwords.

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

- Yes grants permission to view passwords.
- No denies permission to view passwords.

Example: `set allow-password = yes`

Location: User *name*

See Also: Allow-Code, Allow-Diagnostic, Allow-System, Allow-Termserve, Allow-Update

Allow-System

Description: Enables or disables permission to use the following system commands:

Command	Description
ARPtable	Display or modify the TAOS unit's ARP table.
Clr-History	Clear the fatal-error log.
Connection	Display the connection-status window.
Dir	List profiles and profile types.
Dircode	Show the contents of the PCMCIA card code.
DNStab	Display the local Domain Name System (DNS) table.
Fatal-History	List the fatal-error log.
Get	Display settings in a profile.
HDLC	Display High-Level Data Link Control (HDLC)-channel information.
IGMP	Display IGMP multicast statistics.
IPcache	Display IP-route caches.
IP-Pools	Display the status of the IP address pools configured in the IP-Global profile.
IProute	Add or delete IP routes.
Line	Display the line-status window.
List	List settings in the working profile.
Log	Display and control the event-log window.
Modem	Display modem information.
Netstat	Display the routing or interface tables.
New	Create a new profile.
OSPF	Display information related to Open Shortest Path First (OSPF) routing.
Power	Display power-supply statistics.
Quiesce	Temporarily disable a modem or DS0 channel.
Read	Make the specified profile the working profile.
Refresh	Refresh the remote configuration.
Set	Specify a value.
Show	Show slots or items.
Status	Display the system status or hide the status window.
SWANlines	Display the status of all Serial WAN (SWAN) lines and channels.
T1channels	Display T1-channel information.
Userstat	Display user session status.
Version	Display software-version information.
View	Change the contents of a status window.

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

- Yes grants permission to use system commands.
- No denies permission to use system commands.

Example: `set allow-system = yes`

Location: User *name*

See Also: Allow-Code, Allow-Diagnostic, Allow-Password, Allow-Termserve, Allow-Update

Allow-Termserve

Description: Enables or disables permission to use the terminal server and its commands.

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

- Yes grants permission to use the terminal server and its commands.
- No denies permission to use the terminal server and its commands.

Example: `set allow-termserve = yes`

Location: User *name*

See Also: Allow-Code, Allow-Diagnostic, Allow-Password, Allow-System, Allow-Update

Allow-Update

Description: Enables or disables permission to use the following update commands:

Command	Description
Date	Set the system date.
Delete	Delete the specified profile.
Load	Load code or saved configuration to flash.
NVRAM	Clear the configuration and reboot the system.
Reset	Reboot the system.
Save	Save a profile for a future restore.
Write	Store the working profile and save changes.

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

- Yes grants permission to use update commands.
- No denies permission to use update commands.

Example: `set allow-update = yes`

Location: User *name*

See Also: Allow-Code, Allow-Diagnostic, Allow-Password, Allow-System, Allow-Termserve

AMDM

Description: Specifies the action to take when the code image for an Analog Modem card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, T3, UDS3, UE1, Unknown-Cards, UT1

Analog-Encoding

Description: Specifies the encoding standard for digitized analog data. The TAOS unit uses the value you specify for all codecs on the TAOS unit.

Usage: Specify one of the following values:

- U-Law specifies U-Law encoding, the default for T1.
- A-Law specifies A-Law encoding, the default for E1.

Example: `set analog-encoding = u-law`

Location: System

See Also: E1, T1

Answer-Defaults

Description: A profile containing system defaults for incoming calls. The TAOS unit uses the values in this profile until a caller passes authentication and the TAOS unit retrieves a copy of the caller's profile. In addition, you can use the Answer-Defaults profile to supply defaults for profiles retrieved from remote authentication servers.

Usage: Use the Read and List commands to make Answer-Defaults the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make Answer-Defaults the working profile and list its contents:

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

admin> list
[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 any-ppp-auth none yes 0 none 1524 no 600 600+
mp-answer = { yes 1 2 no }
mpp-answer = { yes quadratic transmit 1 1 15 5 10 70 }
fr-answer = { yes }
tcp-clear-answer = { yes }
ara-answer = { no }
v120-answer = { yes 256 }
ip-answer = { yes yes no 1 no }
ipx-answer = { no router-peer }
session-info = { " " no no 120 no-idle 120 0 }
x75-answer = { yes 7 10 1000 1024 }
framed-only = no
hdlc-nrm-answer = { no }
visa2-answer = { no }
atm-answer = { no }
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ANSWER-DEFAULTS written
```

See Also: ARA-Answer, ATM-Answer, CLID-Auth-Mode, CLID-Selection, Force-56Kbps, FR-Answer, Framed-Only, HDLC-NRM-Answer, IP-Answer, MP-Answer, MPP-Answer, PPP-Answer, Profiles-Required, Session-Info, TCP-Clear-Answer, Use-Answer-For-All-Defaults, V120-Answer, Visa2-Answer, X75-Answer

Answer-Delay

Description: Specifies the number of milliseconds the TAOS unit waits before answering an incoming R2 call.

Usage: Specify a number from 100 to 3000. The default is 200. Change the value if the TAOS unit answers calls too quickly.

Example: `set answer-delay = 500`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface, Signaling-Mode

Answer-Originate

Description: Specifies whether the Connection profile enables incoming calls, outgoing calls, or both.

Usage: Specify one of the following values:

- **Ans-And-Orig** (the default) specifies that the TAOS unit can both initiate and receive calls over the connection defined in the profile.
- **Orig-Only** specifies that the profile can be used only for outgoing calls. The TAOS unit will not answer calls from the profile.
- **Ans-Only** specifies that the profile can be used only for incoming calls. The TAOS unit will not initiate calls from the profile.

Example: `set answer-originate = ans-and-orig`

Dependencies: Answer-Originate does not apply to nailed-up call types.

Location: Connection *station* > Telco-Options

See Also: Call-Type, Telco-Options

AppleTalk-Options

Description: A subprofile containing settings for AppleTalk connections.

Usage: With a Connection profile as the working profile, list the AppleTalk-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, following by a space and two periods.

Example: To list the AppleTalk-Options subprofile:

```
admin> list appletalk-options
[in CONNECTION/tim:appletalk-options]
atalk-routing-enabled = no
atalk-static-ZoneName = " "
atalk-static-NetStart = 0
atalk-static-NetEnd = 0
atalk-peer-mode = router-peer
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: Atalk-Peer-Mode, Atalk-Routing-Enabled, Atalk-Static-NetEnd, Atalk-Static-NetStart, Atalk-Static-ZoneName

Apply-To

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

Usage: Specify one of the following values:

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

Example: `set apply-to = both`

Dependencies: You must set Active to Yes in the TOS-Options subprofile for the Apply-To setting to apply.

Location: Connection *station* > IP-Options > TOS-Options, VoIP {*x y*} > TOS-Options

See Also: Active, Precedence, Type-of-Service

ARA-Answer

Description: A subprofile that lets you enable AppleTalk Remote Access (ARA) for incoming calls.

Usage: With Answer-Defaults as the working profile, list the ARA-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, following by a space and two periods.

Example: To list the contents of the ARA-Answer subprofile:

```
admin> list ara-answer
[in ANSWER-DEFAULTS:ara-answer]
enabled = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Enabled

ARA-Enabled

Description: Enables or disables AppleTalk Remote Access (ARA) processing for the connection.

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

- Yes enables ARA processing.
- No disables ARA processing.

Example: `set ara-enabled = yes`

Dependencies: For ARA-Enabled to apply, you must set Enabled to Yes in the ARA-Answer subprofile. You do not need to enable AppleTalk routing for ARA connections.

Location: Connection *station* > ARA-Options

See Also: Maximum-Connect-Time

ARA-Options

Description: A subprofile that enables you to configure AppleTalk Remote Access (ARA) connections.

Usage: With a Connection profile as the working profile, list the ARA-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, following by a space and two periods.

Example: To list the contents of the ARA-Options subprofile:

```
admin> list ara-options
[in CONNECTION/tim:ara-options]
ara-enabled = no
maximum-connect-time = 0
recv-password = "
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: ARA-Enabled, Maximum-Connect-Time, Recv-Password

Area

Description: Specifies the Open Shortest Path First (OSPF) area 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 *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF

See Also: Area-Type, ASE-Tag, ASE-Type, IP-Options, OSPF, OSPF-ASE-Pref,
OSPF-Options, OSPF-Pref, Third-Party

Area-Type

Description: Specifies the type of Open Shortest Path First (OSPF) area the connection or interface belongs to. In a large network, the size of the database, the time required for route computation, and any related network traffic can all become excessive. You can partition an autonomous system (AS) into areas to provide hierarchical routing connected by a backbone. The backbone area is special and always has the area number 0.0.0.0. Other areas have area numbers that are unique within the AS.

Usage: Specify one of the following values:

- Normal (the default) specifies that the router maintains information about external routes.
- Stub specifies that 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 specifies an OSPF NSSA.

Example: `set area-type = normal`

Dependencies: You must set Area-Type consistently on all OSPF routers within the area.

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF

See Also: Area, ASE-Tag, ASE-Type, IP-Options, OSPF, OSPF-ASE-Pref, OSPF-Options, OSPF-Pref, Third-Party

AS-Boundary-Router

Description: Specifies whether the TAOS unit performs Autonomous System Boundary Router (ASBR) calculations.

ASBRs perform calculations related to external routes. Normally, when the TAOS 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 TAOS unit from performing ASBR calculations.

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

- Yes specifies that the TAOS unit performs ASBR calculations.
- No specifies that the TAOS unit does not perform ASBR calculations.

Example: `set as-boundary-router = no`

Location: IP-Global > OSPF-Global

See Also: OSPF-Global

Ascend-Enabled

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

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

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

Example: `set ascend-enabled = no`

Dependencies: If you set Ascend-Enabled to Yes, you must also set Port-Enabled to Yes.

Location: Trap *host-name*

See Also: Port-Enabled

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.

Usage: Specify a 32-bit hexadecimal number. The default is c0:00:00:00.

Example: `set ase-tag = c8000000`

Dependencies: The ASE-Tag setting is not used by the OSPF protocol itself. Area border routers can use it to filter a record.

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { { shelf-*N* slot-*N* *N* } *N* } > OSPF, IP-Route *name*

See Also: Area, Area-Type, ASE-Type, IP-Options, OSPF, OSPF-ASE-Pref, OSPF-Options, OSPF-Pref, Third-Party

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 *station* > IP-Options > OSPF-Options,
IP-Interface { { shelf-*N* slot-*N* *N* } *N* } > OSPF, IP-Route *name*

See Also: Area, Area-Type, ASE-Tag, IP-Options, OSPF, OSPF-ASE-Pref, OSPF-Options, OSPF-Pref, Third-Party

Assign-Address

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

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

- Yes enables the TAOS unit to assign dynamic IP addresses to incoming calls.
- No disables dynamic IP address assignment.

Example: `set assign-address = yes`

Dependencies: The TAOS unit must have at least one configured pool of IP addresses. You can configure the pool locally or in Remote Authentication Dial-In User Service (RADIUS).

Location: Answer-Defaults > IP-Answer

See Also: Assign-Count, Address-Pool, IP-Answer, Must-Accept-Address-Assign, Pool-Base-Address

Assign-Count

Description: Specifies the number of contiguous host addresses contained in each of up to 128 address pools. The defined pool of addresses is available for dynamic assignment to PPP software during negotiation of a connection.

Usage: For each pool, specify a number from 0 to 65535. The default is 0 (zero).

Example: `set 3 = 254`

Dependencies: The pool's initial address must be specified by Pool-Base-Address. 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, VRouters can share the address pools defined in the IP-Global profile.

Location: IP-Global, VRouter

See Also: Assign-Address, Must-Accept-Address-Assign, Pool-Base-Address, Pool-Summary, VRouter-IP-Address

Assignment-ID

Description: Specifies the name assigned to tunnels in order to allow grouping sessions.

Usage: Specify up to 31 characters. The default is null.

Example: `set assignment-id = xyzserver`

Dependencies: The Assignment-ID value has local significance only. It is not transmitted to the remote tunnel end point.

Location: Connection *station* > Tunnel-Options

See Also: Client-Auth-ID, Server-Auth-ID

Async-Drop

Description: Specifies whether the TAOS unit drops asynchronous I-frames it receives from a secondary station when the TAOS unit is the primary station.

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

- Yes specifies that the TAOS unit drops asynchronous I-frames it receives from a secondary station.
- No specifies that the TAOS unit processes I-frames normally. Specifying No enables back-to-back testing on the TAOS unit.

Example: `set async-drop = no`

Location: Connection *station* > HDLC-NRM-Options

See Also: Primary

Atalk-Default-Zone

Description: Specifies the zone assigned to an AppleTalk service on the interface if the service does not select a zone in which to reside.

Usage: Specify the name of an AppleTalk zone. You can enter up to 32 characters. The default is null.

Example: `set atalk-default-zone = Alameda`

Dependencies: If Atalk-Routing-Enabled is set to No, Atalk-Router is set to Atlk-Router-Off, or Atalk-Router is set to Atlk-Router-Non-Seed, Atalk-Default-Zone does not apply.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}

See Also: Atalk-Net-End, Atalk-Net-Start, Atalk-Router, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, Hint-Zone, Interface-Address

Atalk-Dialin-Pool-End

Description: Specifies the end of the network range for an AppleTalk network. A network range is a contiguous range of integers. Each network range must be unique. No two networks can use the same range, and no two network ranges can overlap. Each number in the range can be associated with up to 253 nodes, so the range determines how many clients can dial in.

Usage: Specify an integer from 1 to 65,199. The default is 200.

Example: `set atalk-dialin-pool-end = 300`

Location: Atalk-Global

See Also: Atalk-Dialin-Pool-Start

Atalk-Dialin-Pool-Start

Description: Specifies the beginning of the network range for an AppleTalk network. A network range is a contiguous range of integers. Each network range must be unique. No two networks can use the same range, and no two network ranges can overlap. Each number in the range can be associated with up to 253 nodes, so the range determines how many clients can dial in.

Usage: Specify an integer from 1 to 65,199. The default is 100.

Example: `set atalk-dialin-pool-start = 250`

Location: Atalk-Global

See Also: Atalk-Dialin-Pool-End

Atalk-Global

Description: A profile that enables you to define a virtual AppleTalk network.

Usage: Use the Read and List commands to make Atalk-Global the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Atalk-Global profile the working profile and list its contents:

```
admin> read atalk-global
ATALK-GLOBAL read

admin> list
[in ATALK-GLOBAL]
atalk-dialin-pool-start = 100
atalk-dialin-pool-end = 200
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ATALK-GLOBAL written
```

See Also: Atalk-Dialin-Pool-End, Atalk-Dialin-Pool-Start

Atalk-Interface

Description: A profile in which you enable AppleTalk routing and specify whether the TAOS unit operates as a seed router or a nonseed router on the interface. Only the built-in Ethernet interface on the shelf controller can be configured as an AppleTalk interface.

Usage: Use the Read and List commands to make Atalk-Interface the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Atalk-Interface profile the working profile and list its contents:

```
admin> read atalk-interface { { 1 c 1 } 0 }
ATALK-INTERFACE/ { { shelf-1 controller 1 } 0 } read
```

```
admin> list
[in ATALK-INTERFACE/ { { shelf-1 controller 1 } 0 }]
interface-address* = { { shelf-1 controller 1 } 0 }
atalk-routing-enabled = yes
hint-net-lo = 1001
hint-net-hi = 1010
hint-net-node = 0
hint-zone = "SLC Engineering"
atalk-Router = atlk-router-seed
atalk-Net-Start = 1001
atalk-Net-End = 1010
atalk-Default-Zone = "SLC Engineering"
atalk-Zone-List = [ "SLC Engineering" "SLC Test 1" "SLC Test" +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ATALK-INTERFACE/ { { shelf-1 controller 1 } 0 } written
```

See Also: Atalk-Default-Zone, Atalk-Net-End, Atalk-Net-Start, Atalk-Router, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, Hint-Zone, Interface-Address

Atalk-Net-End

Description: Specifies the end of the network range for an AppleTalk network. A network range is a contiguous range of integers. Each network range must be unique. No two networks can use the same range, and no two network ranges can overlap. Each number in the range can be associated with up to 253 nodes, so the range determines how many clients can dial in.

Usage: Specify an integer from 1 to 65,199. The default is 0 (zero).

Example: `set atalk-net-end = 300`

Dependencies: If Atalk-Routing-Enabled is set to No, Atalk-Router is set to Atlk-Router-Off, or Atalk-Router is set to Atlk-Router-Non-Seed, Atalk-Net-End does not apply.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}

See Also: Atalk-Default-Zone, Atalk-Net-Start, Atalk-Router, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, Hint-Zone, Interface-Address

Atalk-Net-Start

Description: Specifies the beginning of the network range for an AppleTalk network. A network range is a contiguous range of integers. Each network range must be unique. No two networks can use the same range, and no two network ranges can overlap. Each number in the range can be associated with up to 253 nodes, so the range determines how many clients can dial in.

Usage: Specify an integer from 1 to 65,199. The default is 0 (zero).

Example: `set atalk-net-start = 150`

Dependencies: If Atalk-Routing-Enabled is set to No, Atalk-Router is set to Atlk-Router-Off, or Atalk-Router is set to Atlk-Router-Non-Seed, Atalk-Net-Start does not apply.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}

See Also: Atalk-Default-Zone, Atalk-Net-End, Atalk-Router, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, Hint-Zone, Interface-Address

Atalk-Peer-Mode

Description: Specifies whether the remote site is a dial-in AppleTalk Remote Access (ARA) client or another AppleTalk router.

Usage: Specify one of the following values:

- Router-Peer (the default) specifies a routed connection. The TAOS unit acquires the remote site's network information during session negotiation.
- Dialin-Peer specifies that the TAOS unit negotiates a routing session with the dial-in ARA client by assigning the client a node address on the virtual AppleTalk network defined in the Atalk-Global profile. The client must accept the network number the TAOS unit assigns.

Example: `set atalk-peer-mode = dialin-peer`

Dependencies: If Atalk-Routing-Enabled is set to No in the Atalk-Interface profile or in the AppleTalk-Options subprofile of the Connection profile, or if Enabled is set to No in the ARA-Answer subprofile, Atalk-Peer-Mode has no effect.

Location: Connection *station* > AppleTalk-Options

See Also: Atalk-Routing-Enabled, Atalk-Static-NetEnd, Atalk-Static-NetStart, Atalk-Static-ZoneName

Atalk-Router

Description: Specifies whether the AppleTalk router is a seed router or a nonseed router.

Usage: Specify one of the following values:

- Atlk-Router-Off (the default) specifies that no AppleTalk router exists.
- Atlk-Router-Seed specifies a seed router. A seed router has its own hard-coded network and zone configuration.
- Atlk-Router-Non-Seed specifies that the router is not a seed router. A nonseed router acquires its network and zone configuration from another router on the network.

Example: `set atalk-router = atlk-router-seed`

Dependencies: Consider the following:

- If there are other AppleTalk routers on the LAN interface and you set Atalk-Router to Atalk-Router-Seed, you must specify the network range (using Atalk-Net-Start and Atalk-Net-End), zone list (using Atalk-Zone-List), and default zone (using Atalk-Default-Zone). The information you specify must be completely consistent with the corresponding specifications for other AppleTalk routers on the interface.
- If you set Atalk-Router to Atalk-Router-Non-Seed, a seed router must be available at startup time, or the TAOS unit cannot come up in AppleTalk routing mode. If the unit comes up without AppleTalk routing enabled because no seed routers were available at startup, you must reset the system after a seed router is up.
- To optimize the process by which a nonseed router acquires a configuration across the network after a system reset or power cycle, you can set the Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, and Hint-Zone values to known good information.
- If Atalk-Routing-Enabled is set to No, Atalk-Router does not apply.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}

See Also: Atalk-Default-Zone, Atalk-Net-End, Atalk-Net-Start, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, Hint-Zone, Interface-Address

Atalk-Routing-Enabled

Description: Specifies whether AppleTalk routing is enabled:

- In the Atalk-Interface profile, Atalk-Routing-Enabled specifies whether AppleTalk routing is enabled on the shelf-controller Ethernet interface.
- In a Connection profile, Atalk-Routing-Enabled specifies whether AppleTalk routing is enabled for the connection.

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

- Yes enables AppleTalk routing.
- No disables AppleTalk routing.

Example: `set atalk-routing-enabled = yes`

Dependencies: Consider the following:

- If Atalk-Routing-Enabled is set to No in the Atalk-Interface profile, or if Enabled is set to No in the ARA-Answer subprofile, Atalk-Routing-Enabled has no effect in a Connection profile.
- AppleTalk routing must be enabled for incoming PPP connections, but it is not required for ARA client connections.
- You must reset the TAOS unit in order to begin AppleTalk routing.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}, Connection *station* > AppleTalk-Options

See Also: AppleTalk-Options, Atalk-Default-Zone, Atalk-Net-End, Atalk-Net-Start, Atalk-Peer-Mode, Atalk-Router, Atalk-Static-NetEnd, Atalk-Static-NetStart, Atalk-Static-ZoneName, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, Hint-Zone, Interface-Address

Atalk-Static-NetEnd

Description: Specifies the end of the network range for packets that the TAOS unit routes to a remote site for a dial-out AppleTalk connection.

A network range is a contiguous range of integers. Each network range must be unique. No two networks can use the same range, and no two network ranges can overlap. Each number in the range can be associated with up to 253 nodes, so the range determines how many clients can dial in.

Usage: Specify an integer from 1 to 65,199. The default is 0 (zero).

Example: `set atalk-static-netend = 300`

Dependencies: If Atalk-Routing-Enabled is set to No in the Atalk-Interface profile or in the AppleTalk-Options subprofile, Atalk-Static-NetEnd does not apply.

Location: Connection *station* > AppleTalk-Options

See Also: Atalk-Peer-Mode, Atalk-Routing-Enabled, Atalk-Static-NetStart, Atalk-Static-ZoneName

Atalk-Static-NetStart

Description: Specifies the beginning of the network range for packets that the TAOS unit routes to a remote site for a dial-out AppleTalk connection. A network range is a contiguous range of integers. Each network range must be unique. No two networks can use the same range, and no two network ranges can overlap. Each number in the range can be associated with up to 253 nodes, so the range determines how many clients can dial in.

Usage: Specify an integer from 1 to 65,199. The default is 0 (zero).

Example: `set atalk-static-netstart = 200`

Dependencies: If Atalk-Routing-Enabled is set to No in the Atalk-Interface profile or in the AppleTalk-Options subprofile, Atalk-Static-NetStart does not apply.

Location: Connection *station* > AppleTalk-Options

See Also: Atalk-Peer-Mode, Atalk-Routing-Enabled, Atalk-Static-NetEnd, Atalk-Static-ZoneName

Atalk-Static-ZoneName

Description: Specifies the zone name the TAOS unit uses when routing packets to a remote site for a dial-out AppleTalk connection.

Usage: Specify a zone name of up to 32 characters. The default is null.

Example: `set atalk-static-zonename = myzone`

Dependencies: If Atalk-Routing-Enabled is set to No in the Atalk-Interface profile or in the AppleTalk-Options subprofile, Atalk-Static-ZoneName does not apply.

Location: Connection *station* > AppleTalk-Options

See Also: Atalk-Peer-Mode, Atalk-Routing-Enabled, Atalk-Static-NetEnd, Atalk-Static-NetStart

Atalk-Zone-List

Description: Specifies a list of AppleTalk zone names for the local network.

Usage: Specify a list of up to 32 space-delimited zone names. Each name can consist of up to 32 characters, including embedded spaces. Enclose each name in quotation marks. The characters must be in the standard printing character set, and must not include an asterisk (*). Enclose the list in brackets, with a space after the opening bracket and before the closing bracket. The default is null.

Example: `set atalk-zone-list = ["Alameda" "WC" "LA"]`

Dependencies: If Atalk-Routing-Enabled is set to No, Atalk-Router is set to Atlk-Router-Off, or Atalk-Router is set to Atlk-Router-Non-Seed, Atalk-Zone-List does not apply.

Location: Atalk-Interface {shelf-*N* slot-*NN*}

See Also: Atalk-Default-Zone, Atalk-Net-End, Atalk-Net-Start, Atalk-Router, Atalk-Routing-Enabled, Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, Hint-Zone, Interface-Address

AT-Answer-String

Description: Specifies extra AT commands in the answer string of the system's modem configuration:

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

Example: The following example sets AT-Answer-String to S37 to 11:

```
admin> read terminal-server
TERMINAL-SERVER read
admin> set modem-configuration AT-answer-string = S37 = 11
admin> write
TERMINAL-SERVER written
```

The new AT-Answer-String setting causes the following string to be sent to the modem:

```
ATS37 = 11A
```

When the modem receives this string, it forces a V.32bis 14400 connection.

Dependencies: Consider the following:

- Do not begin the string with the characters *AT*. These two characters are automatically added to the beginning of the string before the TAOS unit sends the commands to the modem.
- Do not include an A (answer) or a D (dial) command anywhere in the string. An A command is automatically added to the end of the string. A D command in the answer string causes the call to fail.
- The answer string is the last of four strings sent to the modem when the TAOS unit answers a call. Therefore, the commands you enter can overwrite settings specified elsewhere. For example, if Max-Baud-Rate sets the maximum baud rate and the AT-Answer-String setting specifies a +MS command with a different baud rate, the AT-Answer-String value overwrites the Max-Baud-Rate value.
- Be very careful when entering AT commands for AT-Answer-String. The system does not prevent you from entering incorrect strings.

Location: Terminal-Server > Modem-Configuration

See Also: 7-Even, Cell-Level, Cell-Mode-First, Max-Baud-Rate, Modem-Transmit-Level, V42/MNP

ATM1483Type

Description: Specifies the type of AAL5 multiplexing for the connection.

Usage: Specify one of the following values:

- AAL5-LLC (the default) specifies AAL5 using LLC encapsulation for routed protocols.
- AAL5-VC specifies AAL5 using VC-based multiplexing.

Location: Connection > ATM-Options

See Also: VCI, VPI

ATM-Address

Description: A subprofile that enables you to set an ATM End System Address (AESA) or E.164 Asynchronous Transfer Mode (ATM) address.

Usage: With an ATM-Interface profile as the working profile, enter `list svc-options atm-address` to display the ATM-Address subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To make the ATM-Interface profile with the index `{ {any-shelf any-slot 0 } 0 }` the working profile and list the contents of the ATM-Address subprofile:

```
admin> read atm-interface { { any-shelf any-slot 0 } }  
ATM-INTERFACE/{ { any-shelf any-slot 0 } } read
```

```
admin> list svc-options atm-address
[ in ATM-INTERFACE/{ {any-shelf any-slot 0} 0 } :svc-options: +
numbering-plan = undefined
el64-native-address = " "
aesa-address = { undefined { " " " " } { " " " " " " } }
svc-address-info = " "
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options

See Also: AESA-Address, El64-Native-Address, Numbering-Plan, SVC-Address-Info

ATM-Answer

Description: A subprofile that lets you specify whether the system accepts incoming Asynchronous Transfer Mode (ATM) Switched Virtual Circuit (SVC) calls.

Usage: With the Answer-Defaults profile as the working profile, list the ATM-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the ATM-Answer subprofile:

```
admin> list atm-answer
[ in ANSWER-DEFAULTS: atm-answer ]
svc-enabled = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: SVC-Enabled

ATM-Direct-Enabled

Description: Specifies whether ATM-direct is enabled.

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

- Yes specifies that ATM-direct is enabled.
- No specifies that ATM-direct is disabled.

Example: `set atm-direct-enabled = yes`

Location: Connection *station* > ATM-Options

See Also: ATM-Direct-Profile

ATM-Direct-Profile

Description: Specifies the name of the Connection profile to which ATM data is switched.

Usage: Specify a text string. The default is null.

Example: `set atm-direct-profile = myprof`

Dependencies: If ATM-Direct-Enabled is set to Yes, you must specify a value for ATM-Direct-Profile.

Location: Connection *station* > ATM-Options

See Also: ATM-Direct-Enabled

ATM-Interface

Description: A profile that enables you to configure a logical Asynchronous Transfer Mode (ATM) interface associated with a physical ATM port.

Usage: Use the Read and List commands to make ATM-Interface the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the ATM-Interface profile with the index `{ { shelf-1 slot-2 1 } 0 }` the working profile and list its contents:

```
admin> read atm-interface { { 1 2 1 } 0 }
ATM-INTERFACE/{ { shelf-1 slot-2 1 } 0 } read

admin> list
[in ATM-INTERFACE/{ { shelf-1 slot-2 1 } 0 }]
interface-address* = { { shelf-1 slot-2 1 } 0 }
name = ""
svc-options = { no uni-3.1 { undefined "" { undefined { "" "" +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ATM-INTERFACE/{ { shelf-1 slot-2 1 } 0 } written
```

See Also: Interface-Address, Name, SVC-Options

ATM-Options

Description: A subprofile containing options for configuring an Asynchronous Transfer Mode (ATM) connection.

Usage: With a Connection profiles as the working profile, list the ATM-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the ATM-Options subprofile:

```
admin> list atm-options
[in CONNECTION:atm-options]
atm1483type = aal5-llc
vpi = 0
vci = 32
atm-enabled = yes
atm-direct-enabled = no
atm-direct-profile = ""
vc-fault-management = none
vc-max-loopback-cell-loss = 1
svc-options = { no { undefined "" { undefined { "" "" } { "" ""}+
fr-08-mode = translation
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection

See Also: ATM1483Type, ATM-Direct-Enabled, ATM-Direct-Profile, FR-08-Mode, SVC-Options, VC-Fault-Management, VCI, VC-Max-Loopback-Cell-Loss, VPI

ATMP

Description: A profile that enables you to configure an Ascend Tunnel Management Protocol (ATMP) tunnel.

Usage: Use the Read and List commands to make ATMP the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the ATMP profile the working profile and list its contents:

```
admin> read atmp
ATMP read
admin> list
[in ATMP]
agent-mode = home-agent
agent-type = gateway-home-agent
udp-port = 5150
home-agent-password = my-password
atmp-sap-reply = no
retry-timeout = 3
retry-limit = 10
idle-timer = 30
mtu-limit = 0
force-fragmentation = no
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ATMP written
```

Dependencies: You must reset the TAOS unit in order to begin ATMP operations.

See Also: ATMP-SAP-Reply, Agent-Mode, Agent-Type, Force-Fragmentation, Home-Agent-Password, MTU-Limit, Password, Retry-Limit, Retry-Timeout, UDP-Port

ATMP-HA-RIP

Description: Specifies whether to use Routing Information Protocol version 2 (RIP-v2) for the Home Agent's gateway profile in an Ascend Tunnel Management Protocol (ATMP) configuration.

Usage: Specify one of the following values:

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

Example: `set atmp-ha-rip = rip-send-v2`

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

Location: Connection *station* > Tunnel-Options

See Also: Home-Network-Name, Max-Tunnels, Password, Primary-Tunnel-Server, Profile-Type, Secondary-Tunnel-Server, Tunneling-Protocol, UDP-Port

ATM-Protocol

Description: Specifies the Asynchronous Transfer Mode (ATM) signaling protocol.

Usage: Specify one of the following settings:

- UNI-3.0
- UNI-3.1 (the default)

Example: `set atm-protocol = uni-3.0`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options

See Also: ATM-Address

ATMP-SAP-Reply

Description: Enables or disables a Home Agent's ability to reply to the Mobile Client's IPX Nearest Server Query if the Home Agent knows about a server on the home network. ATMP-SAP-Reply is used only when accessing the TAOS unit as a Home Agent.

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

- Yes enables the TAOS unit configured as an Ascend Tunnel Management Protocol (ATMP) Home Agent to reply to a Mobile Client's Nearest Server Query with the address of a server on the home network.
- No means the TAOS unit does not respond to these queries from a Mobile Client.

Example: `set atmp-sap-reply = yes`

Location: ATMP

See Also: Agent-Mode, Agent-Type

ATMSVC-Route

Description: A profile that enables you to configure a static Asynchronous Transfer Mode (ATM) route.

Usage: Use the Read and List commands to make ATMSVC-Route the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the ATMSVC-Route profile `route1` the working profile and list its contents:

```
admin> read atmsvc-route route1
ATMSVC-ROUTE/route1 read

admin> list
[in ATMSVC-ROUTE/route1]
name* = route1
active = no
address-prefix = ""
interface-address = { { any-shelf any-slot 0 } 1 }
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
ATMSVC-Route/route1 written
```

See Also: Active, Address-Prefix, Interface-Address, Name

AT-String

Description: Specifies an AT string that indicates the required modem timings, modulation types, speed, and other modem values. When a transaction call is initiated or answered by a modem, the TAOS unit must train the modem before establishing the connection. To enable dial-in terminals for transaction processing to connect quickly with as little modem training as possible, you can specify an AT string.

Usage: Specify one or more valid AT commands, up to a limit of 58 characters. The default is null, which specifies that the system performs modem training as usual.

Example: `admin> set AT-string = B1+MS=69, 1, 1200, 1200;`

This AT-String setting causes the following string to be sent to the modem, forcing it to answer as a Bell 212A type modem in automode:

`ATB1+MS=69, 1, 1200, 1200;`

Dependencies: Consider the following:

- Do not begin the string with the characters *AT*. These two characters are automatically added to the beginning of the string before the TAOS unit sends the commands to the modem.
- Do not include an A (answer) or a D (dial) command anywhere in the string. An A command is automatically added to the end of the string. A D command in the answer string causes the call to fail.
- Be very careful when entering AT commands for AT-String. The system does not prevent you from entering incorrect strings.

Location: Connection *station*

See Also: AT-Answer-String

Auth-Attribute-Type

Description: Specifies the attribute(s) used for session matching.

Usage: Specify one of the following values:

- Rad-Serv-Attr-Any (the default) specifies that the first Remote Authentication Dial-In User Service (RADIUS) attribute is used for session matching.
- 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 Rad-Serv-Enable is set to No, Auth-Attribute-Type does not apply.

Location: External-Auth > Rad-Auth-Server

See Also: Rad-Auth-Server, Rad-Serv-Enable

Auth-Boot-Host

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 primary Remote Authentication Dial-In User Service (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 = 200.54.6.78`

Location: External-Auth > Rad-Auth-Client

See Also: Auth-Boot-Host-2, Auth-Boot-Port

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 Remote Authentication Dial-In User Service (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`

Location: External-Auth > Rad-Auth-Client

See Also: Auth-Boot-Host, Auth-Boot-Port

Auth-Boot-Port

Note: This setting is for a customer-specific application outside of the United States. It is not intended for general use.

Description: Specifies the port on the Remote Authentication Dial-In User Service (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 a port number. The default is 0 (zero).

Example: `set auth-boot-port = 200`

Location: External-Auth > Rad-Auth-Client

See Also: Auth-Boot-Host, Auth-Boot-Host-2

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 Rad-Serv-Enable 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

See Also: Auth-Key, Auth-Netmask *N* (*N* = 1–9), Auth-Port, Auth-Server-*N*, Auth-Src-Port, Auth-Timeout, Rad-Auth-Server, Rad-Serv-Enable

Authentication-Enabled

Description: Specifies whether the system generates a trap when an authentication failure occurs.

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

- Yes specifies that the system generates a trap when an authentication failure occurs.
- No specifies that the system does not generate a trap when an authentication failure occurs.

Example: `set authentication-enabled = no`

Location: Trap *host-name*

See Also: Auth-Type

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 values:

- 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 TAOS 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 (the default) 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.

- MD5 specifies that the TAOS 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 = simple`

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF

See Also: Auth-Key, IP-Options, Key-ID, MD5-Authen-Key, MD5-Auth-Key, OSPF, OSPF-Options

Auth-For-Async-Framed-User

Description: Enables or disables the authentication requirement for incoming asynchronous framed users.

Usage: Specify one of the following settings:

- Required (the default) enables the authentication requirement for incoming asynchronous framed users.
- Not-Required disables the authentication requirement. Users without authentication are automatically assigned to an IP address pool set aside for their use.

Example: `set auth-for-async-framed-user = not-required`

Dependencies: Consider the following:

- If Auth-For-Async-Framed-User is set to Not-Required, you must assign a pool number with the Pool-For-Async-Framed-User parameter to provide IP addresses for incoming asynchronous framed users without authentication.
- A read-only copy of the Auth-For-Async-Framed-User setting appears in the IP-Options subprofile.
- You can set the Max-PAP-Auth-Retry parameter to enable users to retry PAP authentication after an authentication failure.

Location: Answer-Defaults > PPP-Answer, Connection *station* > PPP-Options

See Also: Max-PAP-Auth-Retry

Auth-Frm-Adr-Start

Description: Specifies whether to send a second Remote Authentication Dial-In User Service (RADIUS) Accounting Start record when the RADIUS Framed-Address value is assigned.

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

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

Example: `set auth-frm-adr-start = yes`

Location: External-Auth > Rad-Auth-Client

See Also: Rad-Auth-Client

Auth-ID-Fail-Return-Busy

Description: Specifies whether the TAOS 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 Yes or No. The default is No.

- Yes specifies that the TAOS unit returns User Busy (decimal 17) when CLID or called-number authentication fails.
- No specifies that the TAOS unit returns Normal Call Clearing (decimal 16) when CLID or called-number authentication fails.

Example: `set auth-id-fail-return-busy = yes`

Location: External-Auth > Rad-Auth-Client

See Also: Auth-ID-Timeout-Return-Busy

Auth-ID-Timeout-Return-Busy

Description: Specifies whether the TAOS 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 times out.

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

- Yes specifies that the TAOS unit returns User Busy (decimal 17) when CLID or called-number authentication times out.
- No specifies that the TAOS unit returns Normal Call Clearing (decimal 16) when CLID or called-number authentication times out.

Example: `set auth-id-timeout-return-busy = yes`

Location: External-Auth > Rad-Auth-Client

See Also: Auth-ID-Fail-Return-Busy

Auth-Keep-User-Name

Description: Specifies User-Name attribute handling.

Usage: Specify one of the following settings:

- Change-Name (the default) specifies that the name provided by the server is used for the status display and for Remote Authentication Dial-In User Service (RADIUS) accounting purposes.
- Keep-Name specifies that the TAOS unit does not use the User-Name returned by the server. If a name has been specified—that is, if Calling-Line ID (CLID) or Dialed Number Information Service (DNIS) authentication is not used—the system uses that name. Otherwise, it 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 (for example, if it contains one of the characters @\ / %), the system behaves as if Auth-Keep-User-Name were set to Keep-Name. Otherwise, the system behaves as if Change-Name were specified.

Example: `set auth-keep-user-name = keep-name`

Dependencies: A user authenticated by CLID or 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.

Location: External-Auth > Rad-Auth-Client

See Also: Auth-Realm-Delimiters

Auth-Key

Description: Specifies an authentication key that appears in Open Shortest Path First (OSPF), IP Security (IPSec), SNMPv3 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 IPSec, the value of Auth-Key is a 64-byte text string that matches the key specified in the IPSec Encapsulating Security Payload version 2 (ESP-v2) configuration on the L2TP Network Server (LNS).
- For Remote Authentication Dial-In User Service (RADIUS), the value is a string of up to 22 characters. Because the TAOS 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.
- If the TAOS unit is acting as a Terminal Access Controller Access Control (TACACS) or Terminal Access Controller Access Control Plus (TACACS+) client, the value of Auth-Key is a password that the unit supplies to the server.

Usage: Specify a string of up to nine characters (for OSPF), up to 16 characters (for IPSec), or up to 22 characters (for RADIUS). The default for OSPF is `ascend0`. The default for IPSec and RADIUS 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)`

In most SNMPv3 USM configurations, you 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.

If you change the value of Auth-Key directly, keep in mind that the length of the escape sequence must be 10 (16D in hexadecimal) if Message Digest 5 (MD5) is in use and 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 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.

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 an IPsec configuration, Version must be set to 2 for Auth-Key to have any effect.
- 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 MD5 to 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.
- For SNMPv3 USM configurations, Auth-Key does not apply if Auth-Protocol is set to No-Auth.

Location: Connection *station* > IP-Options > OSPF-Options,
External-Auth > Rad-Auth-Client, External-Auth > Rad-Auth-Server,
External-Auth > Tac-Auth-Client, External-Auth > TacPlus-Auth-Client,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF,
IPSec *name* > Recv-ESP, IPSec *name* > Send-ESP,
SNMPv3-USM-User *name*

See Also: Authen-Type, Auth-Netmask *N* (*N* = 1–9), Auth-Port, Auth-Protocol,
Auth-Server-*N*, Auth-Src-Port, Auth-Timeout, ESP-Type, IP-Options, OSPF, OSPF-Options,
Rad-Auth-Client, Rad-Auth-Server, Tac-Auth-Client, TacPlus-Auth-Client, Version

Auth-Netmask N (N = 1–9)

Description: Specifies up to nine subnet masks. The TAOS 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 Rad-Serv-Enable 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

See Also: Auth-Client N, Auth-Key, Auth-Port, Auth-Server-N, Auth-Src-Port, Auth-Timeout, Rad-Auth-Server, Rad-Serv-Enable

Auth-Pool

Description: Enables or disables dynamic address assignment for RADIUS-authenticated IP-routing connections.

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

- Yes enables the TAOS unit to assign dynamic IP addresses to RADIUS-authenticated IP-routing connections.
- No prevents dynamic address assignment for RADIUS-authenticated IP-routing connections.

Example: `set auth-pool = no`

Dependencies: The RADIUS server must be configured with at least one pool of addresses for assignment. If Auth-Type does not specify RADIUS, Auth-Pool does not apply.

Location: External-Auth > Rad-Auth-Client

See Also: Auth-Type, Rad-Auth-Client

Auth-Port

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

Usage: Specify a UDP port number. Make sure that the number you specify matches the value that the external authentication daemon uses on the server.

- If the TAOS unit is acting as a Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control (TACACS), or Terminal Access Controller Access Control Plus (TACACS+) client, 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). The default for TACACS or TACACS+ is 49.
- If the TAOS unit is acting as a RADIUS server, specify the UDP port to use for the accepting client requests. The default is 1700.

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

See Also: Auth-Client N, Auth-Server-N, Rad-Auth-Client, Rad-Auth-Server, Tac-Auth-Client, TacPlus-Auth-Client

Auth-Protocol

Description: Specifies whether or not the TAOS unit can authenticate Simple Network Management Protocol (SNMP) messages on behalf of the SNMPv3 User-based Security Model (USM) user, and specifies the type of authentication protocol the unit uses.

Usage: Specify one of the following settings:

- No-Auth specifies that no authentication is in use.
- MD5-Auth (the default) specifies that the TAOS unit uses the MD5 protocol to authenticate incoming and outgoing messages.
- SHA-Auth specifies that the TAOS unit uses the SHA protocol to authenticate incoming and outgoing messages.

Example: `set auth-protocol = md5-auth`

Location: SNMPv3-USM-User *name*

See Also: Active-Enabled, Name, Password, Priv-Protocol, Read-Write-Access

Auth-RADIUS-Compat

Description: Enables or disables vendor-specific attribute (VSA) compatibility mode when the unit is using Remote Authentication Dial-In User Service (RADIUS) for authentication and authorization purposes.

Usage: Specify one of the following settings:

- Old-Ascend (the default) specifies that the 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. All attributes are sent in standard RFC format.
- 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: At this time, only NavisRadius supports 16-bit VSAs.

Example: `set auth-radius-compat = vendor-specific`

Location: External-Auth > Rad-Auth-Client

See Also: Acct-RADIUS-Compat, Call-Log-RADIUS-Compat, RADIUS-Server-Compat

Auth-Realm-Delimiters

Description: Specifies the characters to be recognized as delimiters in a username. The delimiters are used to define realms in RADIUS Access-Accept packets and the boundaries of characters to be stripped from the username in Access-Request packets.

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 were 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

See Also: Auth-Keep-User-Name, Auth-Req-Delim-Count, Auth-Req-Strip-Side

Auth-Req-Delim-Count

Description: Specifies the number of delimiter characters to delete.

Usage: Specify a number. The default is 0 (zero). When you accept the default, no characters are stripped from the username.

Example: `set auth-req-delim-count = 5`

Dependencies: If the number of delimiters in the username is greater than or equal to the value of the Auth-Req-Delim-Count setting, the unit strips the characters to the left or right (as specified in the Auth-Req-Strip-Side setting) and sends the remaining string in the RADIUS User-Name attribute-value pair. If the number of delimiters in the username is *less than* the value of the Auth-Req-Delim-Count setting, the unit sends the entire username to RADIUS without stripping any characters.

Location: External-Auth > Rad-Auth-Client

See Also: Auth-Realm-Delimiters, Auth-Req-Strip-Side

Auth-Req-Strip-Side

Description: Specifies the direction in which to strip characters from a username.

Usage: Specify one of the following settings:

- None specifies that the unit removes no characters before sending the User-Name attribute-value pair.
- Left specifies that the unit strips the delimiter character and the characters to the left of it.
- Right specifies that the unit strips the delimiter character and characters to the right of it.

Example: `auth-req-strip-side = left`

Location: External-Auth > Rad-Auth-Client

See Also: Auth-Realm-Delimiters, Auth-Req-Delim-Count

Auth-Reset-Time

Description: Specifies the authentication-timeout period in seconds, after which the TAOS unit returns to the primary Remote Authentication Dial-In User Service (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 TAOS 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

See Also: Auth-Server-N, Auth-Timeout, Rad-Auth-Client

Auth-Retries

Description: Specifies the number of times the TAOS unit attempts to connect to a backup Terminal Access Controller Access Control Plus (TACACS+) server.

Usage: Specify a number. The default is 0 (zero), which specifies that the TAOS unit does not attempt to connect to a backup TACACS+ server.

Example: `set auth-retries = 2`

Location: External-Auth > TacPlus-Auth-Client

See Also: Auth-Key, Auth-Port, Auth-Server-N, Auth-Src-Port, Auth-Timeout-Time, TacPlus-Auth-Client

Auth-Rsp-Required

Description: Specifies how the TAOS unit responds if an authentication request times out after a call has been Calling-Line ID (CLID) authenticated.

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

- Yes specifies that the TAOS unit drops calls that have passed CLID authentication.
- No specifies that the TAOS 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, and CLID-Auth-Mode must be set to Required.

Location: External-Auth > Rad-Auth-Client

See Also: CLID, CLID-Auth-Mode, Rad-Auth-Client

Auth-Send67

Description: Specifies whether the TAOS 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: Specify Yes or No. The default is No.

- 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.

Example: `set auth-send67 = yes`

Location: External-Auth > Rad-Auth-Client

See Also: Rad-Auth-Client

Auth-Server-N

Description: Specifies the IP address of an external authentication server.

The TAOS unit first tries to connect to server #1. If it receives no response, it tries to connect to server #2. If it still receives no response, it tries server #3. If the TAOS unit connects to a server other than server #1, it continues to use that server until it fails to service requests, even if the first server 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 character. 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 specifies 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

See Also: Auth-Key, Auth-Port, Auth-Src-Port, Auth-Timeout, Auth-Type, Rad-Auth-Client, Tac-Auth-Client, TacPlus-Auth-Client

Auth-Sess-Interval

Description: Specifies the number of seconds between Remote Authentication Dial-In User Service (RADIUS) authentication reports concerning 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 auth-sess-interval = 15`

Dependencies: Auth-Sess-Interval applies only if Auth-Type is set to RADIUS.

Location: External-Auth > Rad-Auth-Client

See Also: Auth-Type, Rad-Auth-Client

Auth-Session-Key

Description: Enables or disables session-key assignments.

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

- Yes enables session-key assignments.
- No disables session-key assignments.

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

See Also: Rad-Serv-Enable

Auth-Src-Port

Description: Identifies the UDP source port to use for external authentication.

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 (1024–2000).

Dependencies: The TAOS unit uses the source port number to demultiplex the Remote Authentication Dial-In User Service (RADIUS) reply packets to the appropriate slot cards. A separate source port is used for each slot card. On the TAOS unit, the actual source port is the value of Auth-Src-Port plus the slot number, where the shelf controller has a slot number of 0 (zero). So, if Auth-Src-Port is set to 1000, packets originating from the shelf controller have a source port value of 1000, while packets originating from slot 6 have a source port value of 1006.

Location: External-Auth > Rad-Auth-Client, External-Auth > Tac-Auth-Client, External-Auth > TacPlus-Auth-Client

See Also: Auth-Key, Auth-Port, Auth-Server-N, Auth-Timeout, Auth-Type, Rad-Auth-Client, Rad-Auth-Server, Tac-Auth-Client, TacPlus-Auth-Client

Auth-TS-Secure

Description: Acts as a flag to prevent access to the terminal-server interface when the Remote Authentication Dial-In User Service (RADIUS) Login-Host value is not specified.

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

- Yes specifies that the terminal server must be secure. If the Login-Host is not specified, the TAOS unit drops the call.
- No specifies that if the Login-Host is not specified, the TAOS unit allows the dial-in connection to access the terminal-server interface.

Example: `set auth-ts-secure = yes`

Location: External-Auth > Rad-Auth-Client

See Also: Rad-Auth-Client

Auth-Timeout

Description: Sets the number of seconds between attempts to reach an external authentication server. The TAOS unit waits the specified number of seconds for a response to a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control (TACACS) authentication request. If it does not receive a response within that time, it times out and sends the authentication request to the next authentication server (for example, the server specified by Auth-Server-2).

Usage: Specify an integer from 1 to 60. The default is 1.

Example: `set auth-timeout = 5`

Dependencies: If Auth-Type is set to None, Auth-Timeout does not apply.

Location: External-Auth > Rad-Auth-Client, External-Auth > Tac-Auth-Client

See Also: Auth-Key, Auth-Server-N, Auth-Type, Rad-Auth-Client, Tac-Auth-Client

Auth-Timeout-Time

Description: Specifies the number of seconds that must elapse before the TAOS unit attempts to connect to a backup Terminal Access Controller Access Control Plus (TACACS+) server.

Usage: Specify the number of seconds. The default is 0 (zero), which specifies that the TAOS unit does not attempt to use a backup TACACS+ server.

Example: `set auth-timeout-time = 60`

Location: External-Auth > TacPlus-Auth-Client

See Also: Auth-Key, Auth-Port, Auth-Retries, Auth-Server-N, Auth-Src-Port

Auth-Type

Description: In the External-Auth profile, specifies the type of external authentication server to access for incoming connections. In the IPSec profile, specifies the type of authentication transform to use when Encapsulating Security Payload version 2 (ESP-v2) is in use.

Usage: In the External-Auth profile, specify one of the following values:

- None (the default) disables the use of an authentication server.
- TACACS specifies that the TAOS unit accesses a Terminal Access Controller Access Control (TACACS) server. TACACS supports Password Authentication Protocol (PAP), but not Challenge Handshake Authentication Protocol (CHAP) authentication.
- TACACSPlus specifies that the TAOS unit accesses a Terminal Access Controller Access Control Plus (TACACS+) server. TACACS+ supports PAP, but not CHAP authentication. It also provides more extensive accounting statistics and a higher degree of control than does TACACS authentication.
- RADIUS specifies that the TAOS unit accesses a Remote Authentication Dial-In User Service (RADIUS) server. In a RADIUS query, the 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, packet filtering, destination-specific static routes, and usage restrictions for the user. RADIUS supports PAP and CHAP, and terminal-server validation.

In the IPSec profile, specify one of the following values:

- None (the default) specifies that no authentication is in use.
- MD5 specifies MD5 mode, as described in RFC 1828.
- SHA1 specifies SHA1 mode, as described in RFC 1852.
- MD5-HMAC specifies version-2 MD5, currently in draft.
- SHA1-HMAC specifies version-2 SHA1, currently in draft.

Example: `set auth-type = radius`

Dependencies: If Auth-Type is set to a value other than None in the External-Auth profile, you must specify at least one authentication server address. For an IP Security (IPSec) configuration, Version must be set to 2 for Auth-Type to have any effect.

Location: External-Auth, IPSec *name* > Recv-ESP, IPSec *name* > Send-ESP

See Also: Auth-Server-N, ESP-Type, Version

Auto-Logout

Description: Specifies whether or not to log out the current User profile and go back to default privileges upon loss of Data Transmit Ready (DTR) from the serial port.

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

- Yes specifies that the TAOS unit automatically logs out the current User profile if DTR is lost on the serial port.
- No specifies that the current User profile remains logged in.

Example: `set auto-logout = yes`

Location: Serial {shelf-*N* slot-*N* *N*}

See Also: Idle-Logout, User (profile)

Auto-Telnet

Description: Causes the terminal server to interpret an unknown command as the name of a host for a Telnet session.

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

- Yes specifies that a user can omit the keyword `Telnet` and specify a hostname in order to initiate a Telnet session.
- No specifies that if a user enters only a hostname at the terminal-server prompt, the TAOS unit rejects it as an unknown command.

Example: `set auto-telnet = yes`

Dependencies: When terminal services are disabled, Auto-Telnet does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration > Telnet-Options

See Also: Telnet, Telnet-Options, Terminal-Mode-Configuration

Auto-Update

Description: Specifies whether the local Domain Name System (DNS) table is automatically updated by regular successful DNS queries.

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

- Yes specifies that when a regular DNS query succeeds, the system makes a lookup on that hostname to the local table. If there is an entry for the hostname, the system replaces the entry's IP address(es) with the query response. Therefore, you can use the Auto-Update setting to build the local table.
- No specifies that the contents of the local DNS table are not affected by successful DNS queries.

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.

Location: IP-Global > DNS-Local-Table

See Also: DNS-List-Attempt, DNS-List-Size, Enabled, Table-Config N

Auxiliary-Syslog

Description: A subprofile that specifies event-logging settings for the second and third data 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: With a Log profile as the working profile, list one of the Auxiliary-Syslog subprofiles. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the Auxiliary-Syslog [1] subprofile:

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

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Log

See Also: Facility, Host, Port, Syslog-Enabled, Syslog-Level

Aux-Send-Password

Description: Specifies the password the TAOS 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 Remote Authentication Dial-In User Service (RADIUS) user profile for the TAOS unit.

Example: `set aux-send-password = unit0`

Dependencies: For Aux-Send-Password to apply, the call must use MP+.

Location: Connection *station* > MPP-Options

See Also: MPP-Options, Send-Password

Available-Metric

Description: Specifies a number from 0 to 255 to use as a transaction server's current metric if it sends a Quick Transaction Protocol (QTP) Status Message with a Flow Control Attribute set to Available.

Usage: Specify a number from 0 to 255. The default is 1.

Example: `set available-metric = 5`

Location: Transaction-Server

See Also: Congested-Metric, Partly-Congested-Metric, Shutdown-Metric

B

Back-To-Back

Description: Specifies whether the E1 line is connected back-to-back with another TAOS unit.

Usage: Specify True or False. False is the default.

- True specifies that the E1 line is connected back-to-back with another TAOS unit.
- False specifies that the E1 line is not connected back-to-back with another TAOS unit.

Example: `set back-to-back = false`

Location: E1 {shelf-*N* slot-*N* *N*}

See Also: E1

Backup

Description: Specifies the name of a backup Connection profile for a nailed-up connection. The backup connection can be a switched PPP link or a Frame Relay Permanent Virtual Connection (PVC). 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 TAOS unit then brings it down.

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 datalink-layer backup interface is that when a nailed-up interface specifies a backup interface, the routes to the nailed-up 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 (such as filters or firewalls) from the profile for the primary nailed-up connection.

Location: Connection *station* > Session-Options

See Also: Call-Type, Session-Options

BACP-Enable

Description: Enables or disables Bandwidth Allocation Control Protocol (BACP) for Multilink Protocol (MP) connections.

Usage: Specify one of the following settings:

- Yes enables BACP. In the Answer-Defaults profile, the Yes setting enables the system to accept an MP call that requests BACP bandwidth management. In a Connection profile, the Yes setting enables a specific connection to use BACP bandwidth management.
- No (the default) disables BACP.

Example: `set bacp-enable = yes`

Dependencies: Consider the following:

- BACP is described in RFC 2125. It provides dynamic bandwidth allocation based on a utilization threshold, using criteria that are very similar to those used by the bandwidth-on-demand feature in Multilink Protocol Plus (MP+).
- BACP can be used with digital or analog links.
- For dynamic bandwidth allocation to work on an MP connection, both sides of the connection must support BACP.
- BACP shares the parameters used by MP+ to specify criteria for adding or subtracting bandwidth. Following are the relevant parameters, shown with default settings:

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

Location: Answer-Defaults > MP-Answer, Connection *station* > MP-Options

See Also: Add-Persistence, Bandwidth-Monitor-Direction, Decrement-Channel-Count, Increment-Channel-Count, Seconds-History, Sub-Persistence, Target-Utilization

Bandwidth-Monitor-Direction

Description: Specifies the direction in which the TAOS unit monitors link utilization for multilink PPP calls.

Usage: Specify one of the following values:

- None (the default) turns off bandwidth monitoring.
- Transmit specifies that the TAOS unit monitors link utilization on transmitted packets only.
- Transmit-And-Receive specifies that the TAOS unit monitors link utilization in both directions.

Example: `set bandwidth-monitor-direction = none`

Location: Answer-Defaults > MPP-Answer, Connection *station*

See Also: Add-Persistence, Base-Channel-Count, Decrement-Channel-Count, Dynamic-Algorithm, Increment-Channel-Count, Maximum-Channels, Minimum-Channels, MPP-Answer, MPP-Options, Seconds-History, Sub-Persistence, Target-Utilization

Banner

Description: Specifies the terminal-server login banner.

Usage: Specify the banner text. You can enter up to 255 alphanumeric characters.

Example: `set banner = "Welcome to the Terminal Server"`

Dependencies: If terminal services are disabled, Banner does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Host-N, Remote-Configuration, Terminal-Mode-Configuration, Text-N

Banner N

Description: Indicates the menu banners for terminal-server logins in menu mode, downloaded from Remote Authentication Dial-In User Service (RADIUS).

Usage: This setting is read only.

Example: `banner [1] = "Welcome to the Terminal Server"`

Location: Ext-Tsrv

See Also: Hosts-Info N, Init-Banner N

Base

Description: A read-only profile that displays the software versions in use, the enabled features, network interfaces, and other system information.

Usage: Use the Get command to display the Base profile values.

```
admin> get base
[in BASE]
shelf-number = 1
software-version = 1
software-revision = 0
software-level = E
d-channel-enabled = yes
aim-enabled = yes
switched-enabled = yes
multi-rate-enabled = yes
frame-relay-enabled = yes
maxlink-client-enabled = enabled
data-call-enabled = yes
```



```
r2-signaling-enabled = no
serial-number = 6201734
countries-enabled = 511
modem-dialout-enabled = yes
firewalls-enabled = no
network-management-enabled = no
advanced-agent-enabled = no
phs-support = no
selecttools-enabled = no
hardware-level = 0
voip-enabled = no
voip-max-capacity-allowed = no
xcom-ss7 = enabled
network-mgmt-voip-enabled = no
fgd-signaling-enabled = yes
```

See Also: Advanced-Agent-Enabled, AIM-Enabled, Countries-Enabled, Data-Call-Enabled, D-Channel-Enabled, Fgd-Signaling-Enabled, Firewalls-Enabled, Frame-Relay-Enabled, Hardware-Level, MAXLink-Client-Enabled, Modem-Dialout-Enabled, Multi-Rate-Enabled, Network-Management-Enabled, Network-Mgmt-VoIP-Enabled, PHS-Support, R2-Signaling-Enabled, Selecttools-Enabled, Serial-Number, Shelf-Number, Software-Level, Software-Revision, Software-Version, Switched-Enabled, Toggle-Screen, VoIP-Enabled, VoIP-Max-Capacity-Allowed, XCOM-SS7

Base-Channel-Count

Description: Specifies the number of channels the TAOS unit uses when setting up a connection. If the session uses Multilink Protocol (MP), Base-Channel-Count specifies the total number of channels to use for the call. If the session uses Multilink Protocol Plus (MP+), Base-Channel-Count specifies the initial number of channels to use for the call.

Usage: Specify a number from 0 (zero) to the value of Maximum-Channels. The default is 1.

Example: `set base-channel-count = 3`

Dependencies: If the Base-Channel-Count value exceeds the Maximum-Channels value or falls below the Minimum-Channels value, an error results.

Location: Connection *station* > MP-Options

See Also: Maximum-Channels, Minimum-Channels, MP-Options

Bay-ID

Description: Specifies an ASCII string that the TAOS unit sends to the media gateway controller in the device registration message when Control-Protocol is set to IPDC-0.x. The TAOS unit does not interpret the value. Interpretation on the signaling gateway is gateway dependent.

Usage: Specify a text string. The default is null.

Example: `set bay-id = 121dj45`

Location: SS7-Gateway

See Also: Control-Protocol

Bearer-Capability

Description: Specifies the request for a specific bearer service from the egress switched circuit network for outbound VoIP calls. This request is transmitted to the switched telephone network in the bearer service information element of the call setup message sent by the MultiVoice gateway.

Usage: Specify one of the following values:

- Speech (the default) requests switched network routing over a channel that supports speech bearer capability.
- Unrestricted-Digital-Info requests switched network routing over a channel that supports unrestricted digital information (UDI) bearer capability.
- Restricted-Digital-Info requests switched network routing over a channel that supports restricted digital information (RDI) bearer capability.
- Audio-3100hz requests switched network routing over a channel that supports digital audio bearer capability up to 3.1kHz.
- Video requests switched network routing over a channel that supports video signaling bearer capability.

Example: `set bearer-capability = audio-3100hz`

Location: VoIP { *x y* } > PSTN-Attribute

See Also: Cause-Code-Transparency

BER-Receive

Description: Indicates whether the bit-error rate threshold has been reached.

Usage: The BER-Receive setting is read only. True indicates that the threshold has been reached. False indicates that the threshold has not been reached.

Example: `ber-receive = true`

Location: T1-Stat {shelf-*N* slot-*N* *N*}

See Also: AIS-Receive, Yellow-Receive

Bi-Directional-Auth

Description: Specifies whether Challenge Handshake Authentication Protocol (CHAP) authentication must be bidirectional.

Usage: Specify one of the following values:

- None (the default) specifies that authentication is unidirectional. The called device identifies the calling device. The TAOS unit prevents the authentication in which the calling party identifies the called party.

- Allowed specifies that authentication can be bidirectional.

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

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

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

Example: `set bi-directional-auth = allowed`

Dependencies: Consider the following:

- If you specify Allowed or Required, and the second authentication is attempted, it must be successful. Otherwise, the TAOS unit rejects the call (in the case of an incoming call) or tears down the call (in the case of an outgoing call).
- Bidirectional authentication is applicable only if the authentication mode is CHAP, MS-CHAP, or Cache-Token.
- When Receive-Auth-Mode is set to Any or Either, and Password Authentication Protocol (PAP) authentication is negotiated, bidirectional authentication is automatically disabled, even if Bi-Directional-Auth is set to Required. For example, suppose you set Receive-Auth-Mode to Any-PPP-Auth and Bi-Directional-Auth to Required. If an incoming call occurs and the authentication negotiated is PAP, the authentication takes place in one direction only.

Location: Answer-Defaults > PPP-Answer, Connection *station* > PPP-Options

See Also: Substitute-Recv-Name

Billing-Number

Description: Specifies a telephone number that the TAOS unit uses for billing purposes.

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

Example: `set billing-number = 510-555-1972`

Dependencies: Consider the following:

- For nailed-up Frame-Relay datalink connections, Billing-Number does not apply.
- If you specify a value for Billing-Number, there is no guarantee that the telephone company will send it to the answering device.

Location: Connection *station* > Telco-Options, Frame-Relay *fr-name*

See Also: CalledNumber, CLID, CLID-Auth-Mode, Telco-Options

Bit-Rate

Description: For a DS3-ATM2 or E3-ATM card, specifies the maximum sustainable effective bit rate (in Kbps) for transmitting traffic to the network. For a DS3-ATM or OC3-ATM card, specifies the average bit rate (in Kbps).

Usage: Specify an integer. For DS3-ATM interfaces, the valid range is from 0 to 37920. For E3-ATM, the valid range is from 0 to 34368. For OC3-ATM, the valid range is from 0 to 135631. The default is 1000 (1 Mbps).

Example: `set bit-rate = 500`

Dependencies: The Bit-Rate setting applies only to Variable Bit Rate (VBR) traffic.

Location: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*, E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*, OC3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*

See Also: Enabled, Max-Burst-Size, Peak-Rate, Priority

Boot-File-Path

Description: Specifies the pathname of the directory containing Dynamic Host Configuration Protocol (DHCP) client configuration files on the TFTP server.

Usage: Specify a pathname.

Example: `set boot-file-path = /tftpboot/config`

Location: IP-Global > DHCP-Server

See Also: Active, Default-Lease-Duration, Default-Max-Lease, Default-Pool, Lease-Duration, Server-Address, Static-Address, TFTP-Host-Name

BOOTP-Enabled

Description: Specifies whether the TAOS unit uses BOOTP to get settings and check for a new software load.

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

- Yes enables the TAOS unit to use BOOTP.
- No disables the use of BOOTP.

Example: `set bootp-enabled = yes`

Location: IP-Global

See Also: SLIP-BOOTP

BOOTP-Relay

Description: A subprofile containing options for configuring the BOOTP relay feature.

Usage: With IP-Global as the working profile, list the BOOTP-Relay subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the BOOTP-Relay subprofile:

```
admin> list bootp-relay
[in IP-GLOBAL:bootp-relay]
active = no
bootp-servers = [ 0.0.0.0 0.0.0.0 ]
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IP-Global

See Also: Active, BOOTP-Servers

BOOTP-Servers

Description: Specifies the IP address of up to two BOOTP servers. If you specify more than one BOOTP server, the TAOS unit uses the first server until it becomes unavailable. When the TAOS unit starts using the second BOOTP server, it continues to use that server until it becomes unavailable, at which time the unit switches to using the first server again.

Usage: For each BOOTP-Servers setting, 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

See Also: Active, BOOTP-Relay

Boot-SR-Version

Description: Displays the version of the current tntsrbin file (the boot loader).

Usage: The Boot-SR-Version value is read only. The boot loader updates this setting with its version at every system reset.

Example: `boot-sr-version = 2.1`

Location: System

See Also: System

Bottom-Status

Description: Specifies the default contents of the bottom-right portion of the status window.

Usage: Specify one of the following values:

- General-Info causes the TAOS unit to display general information and statistics for the system.
- Log-Window (the default) causes the TAOS unit to display saved system-event log entries.
- Line-Status causes the TAOS unit to display the status of the system telephony interfaces.

Example: `set bottom-status = general-info`

Location: User *name*

See Also: Default-Status, Left-Status, Top-Status

Buffer-Chars

Description: Specifies whether the TAOS unit buffers input characters in a terminal-server session, or processes each character as you enter it.

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

- Yes specifies that the TAOS unit buffers input characters for 100 ms.
- No specifies that the TAOS unit processes each input character as you enter it.

Example: `set buffer-chars = yes`

Dependencies: If terminal services are disabled, Buffer-Chars does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Terminal-Mode-Configuration

C

Call-Ack-Decrement

Description: Specifies a number by which to decrease a transaction server's metric if the server sends a Quick Transaction Protocol (QTP) Call Ack in response to a QTP Connect Request sent by the TAOS unit—that is, if a QTP connection attempt succeeds.

Usage: Specify a number from 0 to 255. The default is 1.

Example: `set call-ack-decrement = 5`

Location: Transaction-Server

See Also: Call-Reject-Increment

Callback

Description: Enables or disables callback security. When you enable callback security, the TAOS unit hangs up after receiving a call and calls back the calling device by using the Dial-Number value.

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

- Yes causes the TAOS unit to hang up on a dial-in connection and dial back the device specified in the profile.
- No specifies that the TAOS unit does not hang up and call back, but authenticates the connection as usual.

Example: `set callback = yes`

Dependencies: If you are using nailed-up call types, or if Answer-Originate does not enable outgoing calls, Callback does not apply. In addition, you must specify a value for Dial-Number.

Location: Connection *station* > Telco-Options

See Also: Answer-Originate, Call-Type, Dial-Number

Call-By-Call

Description: In a T1 profile, specifies the Call-By-Call signaling value to set for routing calls from a local device through the TAOS unit to the network. In a Connection profile, specifies the Call-By-Call signaling value for PRI lines.

Usage: Specify a number from 0 to 65535, corresponding to the type of Call-By-Call service in use. The default is 0 (zero), which disables Call-By-Call service.

The following Call-By-Call services are available if the service provider is AT&T:

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

The following VPN and GVPN Call-By-Call services are available if the service provider is Sprint:

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

The following Call-By-Call services are available if the service provider is MCI:

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

Example: `set call-by-call = 7`

Location: Connection *station* > Telco-Options, T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Call-By-Call-ID, Line-Interface, Telco-Options

Call-By-Call-ID

Description: Specifies the PRI service to use when placing a call.

Usage: Specify a number from 0 to 65535, corresponding to the type of Call-By-Call-ID service in use. The default is 0, which disables Call-By-Call-ID service. The following Call-By-Call-ID services are available if the service provider is AT&T:

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

The following VPN and GVPN Call-By-Call-ID services are available if the service provider is Sprint:

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

The following Call-By-Call-ID services are available if the service provider is MCI:

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

Example: `set call-by-call-id = 7`

Location: Frame-Relay *fr-name*

See Also: Call-By-Call

CalledNumber

Description: For called-number authentication, specifies the number the remote end called to establish the connection. In many cases, the number will be the same as the Dial-Number setting, but without a trunk group or dial prefix.

Usage: Specify the called number. The default is null.

Example: `set callednumber = 5551212`

Dependencies: For Dialed Number Information Service (DNIS) Callback, you must specify a value for CalledNumber.

Location: Connection *station*

See Also: CLID-Auth-Mode

Called-Number-Type

Description: Specifies the type of telephone number in the Connection profile or Frame-Relay profile. When the TAOS unit dials an outgoing call on a T1 PRI line, the carrier uses the value of Called-Number-Type in a Connection profile to interpret the dialed telephone number.

Usage: Specify one of the following values:

- Unknown specifies that the telephone number is of an unknown type.
- International specifies telephone numbers outside the U.S.
- National (the default) specifies telephone numbers within the U.S.
- Local specifies telephone numbers within your Centrex group.
- Abbrev specifies add-on numbers only.
- Network-Specific specifies that the dialed network interprets the telephone number.

Example: `set called-number-type = international`

Dependencies: Called-Number-Type does not apply to nailed-up connections. When you write a Connection profile with Circuit-Type set to SVC, the unit automatically sets Called-Number-Type to International.

Location: Connection *station*, Frame-Relay *fr-name*

See Also: Circuit-Type, Dial-Number, Trunk-Group

Caller-ID

Description: Specifies whether the unit requests the Calling Line ID (CLID) from the switch.

Usage: Specify one of the following values:

- No-Caller-ID (the default) specifies that the TAOS unit does not request the CLID from the switch.
- Get-Caller-ID specifies that the TAOS unit requests the CLID from the switch.

Example: `set caller-id = get-caller-id`

Dependencies: The following Signaling-Mode settings require that you set Caller-ID to Get-Caller-ID for CLID authentication to work:

E1-Chinese-Signaling
E1-Argentina-Signaling
E1-Philippine-Signaling
E1-Brazil-Signaling
E1-Malaysia-Signaling
E1-Indian-Signaling
E1-New-Zealand-Signaling
E1-Thailand-Signaling
E1-Israel-Signaling
E1-Mexico-Signaling
E1-Kuwait-Signaling

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: CLID, CLID-Auth-Mode, Line-Interface, Signaling-Mode

Call-Filter

Description: Specifies the name of a call filter to apply to a connection. The TAOS unit uses a call filter to determine whether or not a packet should cause the unit to reset the idle timer or place a call. If you apply both a call filter and data filter to a connection, the unit applies the call filter after applying the data filter. Only those packets that the data filter forwards can reach the call filter.

Usage: Specify the filter name. The default is null, which specifies that the TAOS unit does not apply a call filter.

Example: `set call-filter = ignore-bcast`

Dependencies: If all channels of a link are nailed up, or if the Filter-Name setting does not specify a call filter, Call-Filter does not apply.

Location: Answer-Defaults > Session-Info, Connection *station* > Session-Options

See Also: Data-Filter, Filter, Filter-Name, Filter-Persistence, Idle-Timer, Session-Info, Session-Options

Call-Hairpin

Description: Specifies whether the TAOS unit connects calls by means of the Public Switched Telephone Network (PSTN) if it cannot register with a MultiVoice™ gatekeeper. The technique of turning the call back from the MultiVoice gateway to the PSTN is called *hairpin dialing*.

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

- Yes specifies that the TAOS unit connects calls by means of the PSTN if it cannot register with a MultiVoice gatekeeper.
- No specifies that the TAOS unit does not connect calls by means of the PSTN if it cannot register with a MultiVoice gatekeeper. New calls requests are rejected until the unit successfully registers with a gatekeeper.

Example: `set call-hairpin = yes`

Dependencies: Hairpin dialing works only when a second Digital Signal Processor (DSP) is available on the same TAOS unit and can handle the outgoing call to the PSTN. The DSP can be on the same card or on a second card.

Location: VoIP {x y}

Call-Info

Description: Specifies whether, at the time an authenticated call ends, the TAOS 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 = ( "c jones-p50" 5106785291->? PPP 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 (for numerals).

Usage: To specify that the TAOS unit reports the information to Syslog, specify End-Of-Call. To specify that the unit does not report the information, specify None (the default).

Dependencies: Use Call-Info only for diagnosing session problems. The reports to Syslog rely on the UDP protocol, which does not guarantee delivery. Therefore, you should not use Call-Info for billing purposes.

Location: Log

See Also: Facility, Host, Port, Save-Level, Save-Number, Syslog-Enabled

Call-Inter-Digit-Timeout

Description: Specifies the maximum amount of time (in milliseconds) that the TAOS unit waits for a caller to enter a single digit when two-stage dialing is in use.

Usage: Specify a number from 300 to 20000. The default is 6000. The timer is decremented by one second each time the caller enters a digit. When the timer expires, the unit considers the call complete and the call proceeds. If the calling device finishes dialing before the timer expires, the caller can wait up to 16 seconds, or press the pound (#) key, before the gateway continues processing the call.

Example: `set call-inter-digit-timeout = 15`

Dependencies: The timer setting applies to PIN entries and digits dialed after entering the telephone number.

Location: VoIP {x y}

See Also: Call-Keep-Alive-Timeout

Call-Keep-Alive-Timeout

Description: Specifies how often a MultiVoice gateway polls a remote device during a Voice over IP (VoIP) call in order to verify that the device is still functioning and that the gateway can connect to it over an IP network.

Usage: Specify a number in seconds from 1 to 32767. The default is 0 (zero), which disables the feature.

Example: `set call-keep-alive-timeout = 60`

Dependencies: Changes to Call-Keep-Alive-Timeout take effect with the next VoIP call.

Location: VoIP {x y}

See Also: Gatekeeper-Keepalive

Call-Log-Dropped-Pkt-Enabled

Description: Specifies whether the unit sends a trap when a change in status is detected with regard to dropping call-logging packets.

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

- Yes specifies that the system generates a trap when the value of the `callLoggingDroppedPacketCount` variable in the call-logging MIB is changed from 0 to 1 (which indicates that packets are being dropped) or from 1 to 0 (which indicates that packets are no longer being dropped). Simple Network Management Protocol (SNMP) management stations can obtain the value of the variable at any time by using SNMP Get.
- No specifies that the system does not generate a trap when a change in status is detected with regard to dropping call-logging packets.

Example: `set call-log-dropped-pkt-enabled = no`

Dependencies: Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Trap *name*

See Also: Call-Logging

Call-Log-Enable

Description: Enables or disables call logging.

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

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

Example: `set call-log-enable = yes`

Dependencies: Consider the following:

- 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.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Host-*N*, Call-Log-ID-Base, Call-Log-Key, Call-Log-Limit-Retry, Call-Log-Port, Call-Log-Reset-Time, Call-Log-Stop-Only, Call-Log-Timeout

Call-Logging

Description: A profile that enables you to configure the TAOS unit to communicate with one or more call-log hosts.

Usage: Use the Read and List commands to make Call-Logging the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To read the Call-Logging profile and list its contents:

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

admin> list
[in CALL-LOGGING]
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 = 0
call-log-key = ""
call-log-timeout = 0
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
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

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

Dependencies: Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

See Also: Call-Log-Enable, Call-Log-Host-N, Call-Log-ID-Base, Call-Log-Key, Call-Log-Limit-Retry, Call-Log-Port, Call-Log-Reset-Time, Call-Log-Server-Index, Call-Log-Stop-Only, Call-Log-Timeout

Call-Log-Host-N

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

The TAOS 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 TAOS 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:

- If Call-Log-Enable is set to No, Call-Log-Host-N does not apply.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Enable, Call-Log-ID-Base, Call-Log-Key, Call-Log-Limit-Retry, Call-Log-Port, Call-Log-Reset-Time, Call-Log-Stop-Only, Call-Log-Timeout

Call-Log-ID-Base

Description: Specifies whether the TAOS unit presents a session ID to the call-log host in base 10 or base 16.

Usage: Specify one of the following values:

- Acct-Base-10 (the default) specifies a decimal base.
- 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.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Enable, Call-Log-Host-N, Call-Log-Key, Call-Log-Limit-Retry, Call-Log-Port, Call-Log-Reset-Time, Call-Log-Stop-Only, Call-Log-Timeout

Call-Log-Key

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

Usage: Specify the text of the shared secret. The value you specify must match the value configured on Access Watch. The default is null.

Example: `set call-log-key = unit0`

Dependencies: Consider the following:

- If Call-Log-Enable is set to No, Call-Log-Key does not apply.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Enable, Call-Log-Host-N, Call-Log-ID-Base, Call-Log-Limit-Retry, Call-Log-Port, Call-Log-Reset-Time, Call-Log-Stop-Only, Call-Log-Timeout

Call-Log-Limit-Retry

Description: Specifies the maximum number of retries for call-logging packets. When the TAOS unit is configured for call logging, it sends Start and Stop packets to the call-log host in order to record connections. If the host does not acknowledge a packet within the number of seconds you specify for Call-Log-Timeout, the TAOS unit tries again, resending the packet until the host responds, or dropping the packet if the queue of packets to be resent is full. You can limit the number of retries by setting a maximum.

Usage: To set the maximum number of retries for Start and Stop packets, set 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`

Dependencies: Consider the following:

- The TAOS unit always makes at least one attempt. For example, if you set the number of retries to 10, the unit makes 11 attempts: the original attempt plus 10 retries.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Enable, Call-Log-Host-N, Call-Log-ID-Base, Call-Log-Key, Call-Log-Port, Call-Log-Reset-Time, Call-Log-Stop-Only, Call-Log-Timeout

Call-Log-Multi-Packet

Description: Specifies whether the TAOS unit can deliver multiple requests in a single call-logging packet to a call-logging data receiver that supports the Lucent 16-bit Vendor-Specific Attributes (VSAs).

Usage: Specify Yes or No.

- Yes specifies that multiple call-logging requests are sent in a single packet.
- No specifies that multiple call-logging requests are not sent in a single packet.

Example: `set call-log-multi-packet = yes`

Dependencies: If you specify Yes for Call-Log-Multi-Packet, you must set Call-Log-Radius-Compat to 16-Bit-Vendor-Specific.

Location: Call-Logging

See Also: Call-Log-RADIUS-Compat

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-log host. The default of 0 (zero) indicates any UDP port.

Example: `set call-log-port = 1500`

Dependencies: Consider the following:

- If Call-Log-Enable is set to No, Call-Log-Port does not apply.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Enable, Call-Log-Host-N, Call-Log-ID-Base, Call-Log-Key, Call-Log-Limit-Retry, Call-Log-Reset-Time, Call-Log-Stop-Only, Call-Log-Timeout

Call-Log-RADIUS-Compat

Description: Enables or disables vendor-specific attribute (VSA) compatibility mode when the unit is using Remote Authentication Dial-In User Service (RADIUS) for call logging to the NavisAccess™ manager.

Usage: Specify one of the following settings:

- 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: At this time, only NavisRadius supports 16-bit VSAs.

Location: Call-Logging

See Also: Acct-RADIUS-Compat, Auth-RADIUS-Compat, RADIUS-Server-Compat

Call-Log-Reset-Time

Description: Specifies the number of seconds that must elapse before the TAOS 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 TAOS unit does not return to using the primary call-log host.

Example: `set call-log-reset-time = 60`

Dependencies: Consider the following:

- For Call-Log-Reset-Time to apply, you must set Call-Log-Enable to Yes and specify at least one value for Call-Log-Host-N.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Enable, Call-Log-Host-N, Call-Log-ID-Base, Call-Log-Key, Call-Log-Limit-Retry, Call-Log-Port, Call-Log-Stop-Only, Call-Log-Timeout

Call-Log-Serv-Change-Enabled

Description: Enables or disables trap 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 Yes or No. The default is No.

- Yes specifies that the unit generates a trap when the call-logging server changes.
- No 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 name

See Also: VoIP-GK-Change-Enabled, WAN-Line-State-Change-Enabled

Call-Log-Server-Index

Description: Specifies which Call-Log-Host is used as the active call-logging server.

Usage: Specify one of the following settings:

- Host-1 (the default) specifies the server indicated by Call-Log-Host-1.
- Host-2 specifies the server indicated by Call-Log-Host-2.
- Host-3 specifies the server indicated by Call-Log-Host-3.

Example: `set call-log-server-index = host-2`

Dependencies: Consider the following:

- If the unit cannot authenticate the specified server, it attempts to use the next configured server.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Host-N

Call-Log-Stop-Only

Description: Specifies whether the TAOS unit should send a Stop packet that does not contain a username. (At times, the unit can send a Stop packet to the call-log host without having sent a Start packet. Such a Stop packet has no username.)

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

- Yes specifies that the TAOS unit should send a Stop packet even if it does not contain a username.
- No specifies that the TAOS unit should not send a Stop packet that does not contain a username.

Example: `set call-log-stop-only = no`

Dependencies: Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Enable, Call-Log-Host-N, Call-Log-ID-Base, Call-Log-Key, Call-Log-Limit-Retry, Call-Log-Port, Call-Log-Reset-Time, Call-Log-Timeout

Call-Log-Timeout

Description: Specifies the amount of time (in seconds) that the TAOS unit waits for a response to a call-logging request. If it does not receive a response within the specified time, the TAOS unit sends the request to the next host specified by Call-Log-Host-N. If all call-logging hosts are busy, the TAOS 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 0 (zero), which disables the timer.

Example: `set call-log-timeout = 5`

Dependencies: Consider the following:

- If Call-Log-Enable is set to No, Call-Log-Timeout does not apply.
- Call logging is available with NavisRadius only. For information, see the NavisRadius documentation.

Location: Call-Logging

See Also: Call-Log-Enable, Call-Log-Host-N, Call-Log-ID-Base, Call-Log-Key, Call-Log-Limit-Retry, Call-Log-Port, Call-Log-Reset-Time, Call-Log-Stop-Only

Call-Reject-Increment

Description: Specifies a number by which to increase a transaction server's current metric if it sends a Quick Transaction Protocol (QTP) Call Reject in response to a QTP Connect Request sent by the TAOS unit—that is, if a QTP connection attempt fails.

Usage: Specify a number from 0 to 255. The default is 4.

Example: `set call-reject-increment = 10`

Location: Transaction-Server

See Also: Call-Ack-Decrement

Call-Route

Description: A profile that the TAOS 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: Use the Read and List commands to make a Call-Route profile the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Call-Route profile with the index { { 1 9 33 } 0 } 0 the working profile and list its contents:

```
admin> read call-route { { { 1 9 33 } 0 } 0 }  
CALL-ROUTE/{ { { shelf-1 slot-9 33 } 0 } 0 } read
```

```
admin> list
[in CALL-ROUTE/{ { { shelf-1 slot-9 33 } 0 } 0 }]
index* = { { { shelf-1 slot-9 33 } 0 } 0 }
trunk-group = 0
phone-number = " "
preferred-source = { { shelf-1 slot-13 0 } 0 }
call-route-type = any-call-type
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
CALL-ROUTE/{ { { shelf-1 slot-9 33 } 0 } 0 } written
```

See Also: Call-Route-Type, Index, Phone-Number, Preferred-Source, Trunk-Group

Call-Route-Info

Description: A deprecated setting that specifies a device to which the TAOS unit should route calls received on a particular channel. Call-Route-Info indicates “route any call received on this channel to the specified device.” This value is a mirror-image of the Preferred-Source setting in a Call-Route profile, which indicates “route any call received on the specified T1 channel to me (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 TAOS unit. 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: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
E1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line Config,
SWAN {shelf-*N* slot-*N* *N*} > Line-Config,
T1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*

See Also: Call-Route, Channel-Config, Line-Config, Preferred-Source

Call-Route-Type

Description: Specifies the type of call that the TAOS unit can route to a host device.

Usage: Specify one of the following values:

- Any-Call-Type specifies that the TAOS unit can route any type of call to a host device.
- Voice-Call-Type specifies that the TAOS unit can route voice bearer calls, not including 3.1 Khz audio, to a host device.
- Digital-Call-Type specifies that the TAOS unit can route general digital calls, including 3.1 Khz audio bearer channel calls, to a host device. As far as the TAOS unit is concerned, 3.1 Khz audio calls are voice-bearer. The TAOS unit routes them to a modem, not a High-Level Data Link Control (HDLC) controller.

- Trunk-Call-Type (trunk calls) specifies that the TAOS unit routes calls to a trunk device.
- VoIP-Call-Type specifies that the TAOS 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 calls.
- V110-Call-Type specifies digital calls recognized as containing V.110 rate adapted bearer channels.
- WORMARQ-Call-Type specifies that WORM-ARQ calls are routed to the MultiDSP cards in the system.

Example: `set call-route-type = any-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) license has been enabled, the system creates a new Call-Route profile for each installed MultiDSP card that supports VoIP. The new Call-Route profile sets the Call-Route-Type value to VoIP-Call-Type. The VoIP-Call-Type setting enables the system to route VoIP calls to the MultiDSP card.

Location: Call-Route { { {shelf-*N* slot-*N* *N*} *N*} *N*}

See Also: Call-Route, Index, Phone-Number, Preferred-Source, Trunk-Group

Call-Routing-Sort-Method

Description: Specifies whether to use the old slot-first call-routing sort method or the new item-first sort method for analog calls.

When the system resets, the TAOS unit creates the call-routing database by sorting the list of all installed devices. During active use, the TAOS 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 cards. In previous software releases, the order in which the TAOS unit sorted device addresses caused all channels of a host card to be grouped together, forcing a single card to be completely full before the unit started using another card.

The old sort-order default processed the components of device addresses in the following order:

shelf slot item logical-item

The shelf number is always 1. The current sort-order default provides load balancing across cards by ordering device-address components in the following manner:

item shelf slot logical-item

The shelf number is always 1. This sort order causes the channels of different cards to be interspersed, resulting in load balancing across all cards, even after a system reset.

Usage: Specify one of the following values:

- Item-First (the default) specifies that the TAOS unit sorts by item number, then shelf, and then slot number. This setting tends to distribute incoming calls evenly across multiple host cards.
- Slot-First specifies that the TAOS unit sorts by shelf and slot number, and then by item number. This setting tends to concentrate incoming calls on one host card at a time.

Example: `set call-routing-sort-method = slot-first`

Location: System

See Also: Call-Route, Call-Route-Info, Call-Route-Type, Digital-Call-Routing-Sort-Method

Call-Type

Description: Specifies nailed-up-channel usage for a connection.

Usage: Specify one of the following values:

- Off (the default) specifies that the connection does not use any nailed-up channels.
- FT1 specifies that the connection uses only nailed-up channels.
- FT1-MPP specifies that the TAOS unit might augment nailed-up channels with switched channels for increased bandwidth during a Multilink Protocol Plus (MP+) call.
- FT1-BO specifies that a nailed-up connection can use switched channels, both for additional bandwidth and for a backup method of reaching the site if the nailed-up connection is down.

Example: `set call-type = off`

Dependencies: If Nailed-Groups is set to 0 (zero), Call-Type does not apply.

Location: Connection *station* > Telco-Options

See Also: Nailed-Groups, Telco-Options

Carrier-Established

Description: Indicates whether error conditions exist on the T1 line.

Usage: The Carrier-Established setting is read only. True indicates that no error conditions exist. False indicates error conditions on the line.

Example: `carrier-established = true`

Location: T1-Stat {shelf-*N* slot-*N* *N*}

See Also: AIS-Receive, BER-Receive, Loss-Of-Carrier, Loss-Of-Sync, Yellow-Receive

Cause-Code-Transparency

Description: Enables or disables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect-cause codes generated by the far-end switched network. The codes are passed across the packet network from the far-end MultiVoice gateway to the near-end MultiVoice gateway, and then delivered to the local telephone company.

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

- Yes enables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect-cause codes. The local telephone company switch plays the appropriate tone or disconnect message for the caller.
- No disables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect-cause codes generated by the far-end switched network. The near-end MultiVoice gateway plays the appropriate tones or messages for the caller, and does not deliver the Q.931 or Q.850 codes to the local telephone company switch.

Example: `set cause-code-transparency = yes`

Dependencies: For callers to hear both a busy signal and the call failure message, set Cause-Code-Transparency to Yes whenever voice-announcement reporting is enabled (H323-Voice-Ann-Enabled is set to Yes).

Location: Voip { *x y* } > PSTN-Attribute

See Also: H323-Voice-Ann-Enabled

CBCP-Enabled

Description: Specifies whether CBCP Callback is enabled.

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

- Yes enables CBCP Callback.
- No disables CBCP Callback.

Example: `set cbcP-enabled = yes`

Location: Connection *station* > PPP-Options

See Also: Mode-Callback-Control, Trunk-Group-Callback-Control

Cell-Level

Description: Specifies the modem cellular-communications transmit and receive level.

Usage: Specify one of the following values:

- -18-dB-Cell-Level (the default)
- -17-dB-Cell-Level
- -16-dB-Cell-Level
- -15-dB-Cell-Level
- -14-dB-Cell-Level
- -13-dB-Cell-Level
- -12-dB-Cell-Level
- -11-dB-Cell-Level
- -10-dB-Cell-Level

Example: `set cell-level = -18-db-cell-level`

Dependencies: If terminal services are disabled, Cell-Level does not apply.

Location: Terminal-Server > Modem-Configuration

See Also: Cell-Mode-First, Modem-Configuration

Cell-Mode-First

Description: Determines whether the TAOS unit attempts a cellular connection before a land-based connection.

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

- Yes specifies that the TAOS unit attempts a cellular connection first.
- No specifies that the TAOS unit attempts a land-based connection before attempting a cellular connection.

Example: `set cell-mode-first = no`

Dependencies: If terminal services are disabled, Cell-Mode-First does not apply.

Location: Terminal-Server > Modem-Configuration

See Also: Cell-Level, Modem-Configuration

Channel-Config

Description: A subprofile containing channel-configuration subprofiles, one for each channel.

Usage: With a T1 or E1 profile as the working profile, enter `list line-interface channel-config` to display the Channel-Config subprofile. To close the Channel-Config subprofile and return to a higher context in the profile, enter the List command, followed by a space and two periods.

Example: To list the Channel-Config subprofile:

```
admin> list line-interface channel-config
[in T1/{ shelf-1 slot-2 3 }:line-interface:channel-config]
channel-config[1] = {switched-channel 9 " " {any-shelf any-slot+
channel-config[2] = {switched-channel 9 " " {any-shelf any-slot+
channel-config[3] = {switched-channel 9 " " {any-shelf any-slot+
channel-config[4] = {switched-channel 9 " " {any-shelf any-slot+
...
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface, T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Channel-Config *N*, Channel-State, Channel-State *N*, Channel-Usage, Line-Interface

Channel-Config *N*

Description: A subprofile of the Channel-Config subprofile. Channel-Config *N* contains configuration options for an individual channel of an E1 or T1 line. The index for each subprofile is a channel number.

Usage: With a T1 or E1 profile as the working profile, use the List command to display the configuration for one of the channels. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To display the configuration for channel 1 in the T1 profile:

```
admin> list line-interface channel-config 1
[in T1/{ shelf-1 slot-2 3 }:line-interface:channel-config[1]]
channel-usage = switched-channel
trunk-group = 9
phone-number = ""
call-route-info = { any-shelf any-slot 0 }
nailed-group = 0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config,
T1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config

See Also: Call-Route-Info, Channel-Config, Channel-State, Channel-State *N*, Channel-Usage, Line-Interface, Nailed-Group, Phone-Number, Trunk-Group

Channel-State

Description: An array listing the state of each channel of a T1 line. The index to each array component is a channel number (1–24).

Usage: Use the List command to display the array. To close the array and return to a higher context in the profile, enter the List command, followed by a space and two periods.

Example: In the following example, T1-Stat is the working profile:

```
admin> list channel-state
[in T1-STAT/{ shelf-1 slot-1 1 }:channel-state]
channel-state[1] = idle
channel-state[2] = idle
channel-state[3] = dialing
...
```

Location: T1-Stat {shelf-*N* slot-*N* *N*}

See Also: Channel-Config, Channel-Config *N*, Channel-State *N*, Channel-Usage, Line-State

Channel-State *N*

Description: Specifies the individual state of a channel in a T1 line. The index to each component is a channel number (1–24).

Usage: The Channel-State *N* setting can be one of the following:

Setting	Description
Unavailable	The channel is not available.
Unused	The channel is not in use.
Out-Of-Service	The channel has been taken out of service.
Nailed-Up	The channel is nailed-up (rather than switched).
Held	The channel is on hold.
Idle	The channel is not being used for a call.
Clear-Pending	Call clearing is in process.
Dialing	A number is being dialed for the channel.
Ringing	The TAOS unit is attempting a connection on the channel.
Connected	The channel is being used for an established connection.
Signaling	The channel is a D channel.
Current-D	The channel is a current D channel in a Non-Facility Associated Signaling (NFAS) configuration.
Backup-D	The channel is the backup D channel in an NFAS configuration.
Maintenance	The channel is in a maintenance state.
Spc-Up	A semipermanent circuit is up (Australian installations only).

Location: T1-Stat {shelf-*N* slot-*N* *N*} > Channel-State

See Also: Channel-Config, Channel-Config *N*, Channel-State, Channel-Usage, Line-State

Channel-Usage

Description: Specifies the usage for a channel.

Usage: For a T1 or E1 channel, specify one of the following values:

- Unused-Channel specifies that the channel is unused. The TAOS unit sends the single idle code defined for the channel.
- Switched-Channel (the default) specifies a switched channel, which uses either robbed-bit or D-channel signaling.
- Nailed-64-Channel specifies a clear-channel 64K circuit. It does not require any setup information.

T1 and E1 channels also support the D-Channel setting, which specifies a channel used for ISDN D-channel signaling. For T1, the D channel is channel 24. For E1, it is channel 16.

Only T1 channels support the following additional usage values:

- NFAS-Primary-D-Channel specifies the primary D channel for a group of T1 lines with the same Non-Facility Associated Signaling (NFAS) ID. You must set all other channels on the NFAS line to Switched-Channel, Nailed-64-Channel, or Unused-Channel. Within an NFAS group, you should configure only one line to provide the primary ISDN D channel.
- NFAS-Secondary-D-Channel specifies the secondary D channel for a group of T1 lines with the same NFAS ID. You must set all other channels on the NFAS line to Switched-Channel, Nailed-64-Channel, or Unused-Channel. Within an NFAS group, you should configure only one line to provide the secondary (backup) D channel.

Example: `set channel-usage = switched-channel`

Dependencies: Consider the following:

- For Signaling System 7 (SS7) data trunks associated with a T1 line, the Channel-Usage setting for channel 24 must be Switched-Channel.
- For SS7 data trunks associated with an E1 line, the Channel-Usage setting for channel 17 must be Switched-Channel.
- Channel usage can be different from the usage specified for the line itself. For example, the line might specify switched usage, while individual channels within that line might specify nailed-up usage.

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*,

T1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*

See Also: Channel-Config, Channel-Config *N*, Channel-State, Line-Interface, NFAS-ID, Signaling-Mode

Circuit-Name

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

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

Example: `set circuit-name = circuit-1`

Dependencies: If FR-Direct-Enabled is set to Yes, Circuit-Name does not apply.

Location: Connection *station* > FR-Options

See Also: Encapsulation-Protocol, FR-Direct-Enabled, FR-Options

Circuit-Type

Description: Specifies the type of Virtual Circuit (VC) in use.

Usage: Specify one of the following values:

- PVC (the default) specifies a Permanent Virtual Circuit.
- SVC specifies a Switched Virtual Circuit. This value indicates that the circuit will be established by means of Frame Relay SVC call signaling, but only when data transfer is required.

Example: `set circuit-type = svc`

Location: Connection *station* > FR-Options

See Also: DLCI, Frame-Relay-Profile

CIR-Timer

Description: Specifies the Committed Information Rate (CIR) timer value, in milliseconds, that the unit uses to finetune the accuracy of the RX-Data-Rate-Limit and TX-Data-Rate-Limit values.

Usage: Specify a value from 10 to 5000. The default is 5000.

Example: `set cir-timer = 500`

Location: Connection *station* > Session-Options

See Also: RX-Data-Rate-Limit, TX-Data-Rate-Limit

CL1-Action

Description: Specifies the action taken when congestion level 1 (defined by the value of CL1-Level) is reached.

Usage: Specify one of the following values:

- Ignore specifies that no action is taken.
- Send-Info-To-Mgc (the default) specifies that the TAOS unit sends a congestion indicator to the media gateway controller.

Note: The media gateway controller is not required to respond to the congestion level 1 indicator.

Example: `set cl1-action = ignore`

Dependencies: If you set both CL1-Action and CL2-Action to Ignore and enable signaling heartbeat messages by setting Enabled to Yes in the Signaling-Heartbeat subprofile, the TAOS unit sends a Request Test Echo (RTE) message without a congestion indicator.

Location: SS7-Gateway > Congestion-Control

See Also: CL1-Level

CL1-Level

Description: the unit informs the signaling gateway that congestion level 1 has been exceeded.

Usage: Specify a number from 0 to 1000. The default is 60.

Example: `set cl1-level = 100`

Location: SS7-Gateway > Congestion-Control

See Also: CL1-Action

CL2-Action

Description: Specifies the action taken when congestion level 2 (defined by the value of CL2-Level) is reached.

Usage: Specify one of the following values:

- Ignore specifies that no action is taken.
- Send-Info-To-Mgc specifies that the TAOS unit sends a congestion indicator to the media gateway controller.
- Reject-New-Call (the default) specifies that the TAOS unit rejects new calls and sends a congestion indicator.

Example: `set cl2-action = ignore`

Dependencies: If you set both CL1-Action and CL2-Action to Ignore and enable signaling heartbeat messages by setting Enabled to Yes in the Signaling-Heartbeat subprofile, the TAOS unit sends a Request Test Echo (RTE) message without a congestion indicator.

Location: SS7-Gateway > Congestion-Control

See Also: CL2-Level

CL2-Level

Description: Specifies, in terms of the number of messages in the queue, the point at which the unit informs the signaling gateway that congestion level 2 has been exceeded.

Usage: Specify a number from 0 to 1000. The default is 120.

Example: `set cl2-level = 100`

Location: SS7-Gateway > Congestion-Control

See Also: CL2-Action

Clear-Call

Description: Specifies whether the TAOS unit clears a dial-in connection when an interactive Telnet, Rlogin, or TCP session terminates.

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

- Yes specifies that the TAOS unit clears a dial-in connection when an interactive Telnet, Rlogin, or TCP session terminates.
- No specifies that the TAOS unit does not clear a dial-in connection when an interactive session terminates. Instead, the TAOS unit returns the user to the terminal-server menu.

Example: `set clear-call = yes`

Dependencies: If terminal services are disabled, Clear-Call does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Terminal-Mode-Configuration

Clear-Screen

Description: Specifies whether the TAOS unit clears the screen when a terminal-server session begins.

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

- Yes specifies that the TAOS unit clears the screen of all status messages and echoed scripts when it establishes a terminal-server session.
- No specifies that the TAOS unit establishes the terminal-server session without clearing the screen.

Example: `set clear-screen = yes`

Dependencies: If terminal services are disabled, Clear-Screen does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Terminal-Mode-Configuration

CLID

Description: For an ISDN call, specifies the telephone number of the remote station. For a Frame Relay link, specifies the E.164 address of the local end of the Switched Virtual Circuit (SVC). In the Password-Profile subprofile, specifies the Calling-Line ID (CLID) specified as the password in a RADIUS profile.

Usage: Specify the calling party's telephone number, E.164 address of the local end of the SVC, or the CLID specified as the password in a RADIUS profile. For the calling party's telephone number, you can enter up to 24 characters. For the E.164 subaddress, you can enter up to 15 digits. For the CLID value specified as the password in a RADIUS profile, you can specify up to 21 characters. For the calling-party's telephone number and the E.164 address, the default is null. For the CLID used as a password in a RADIUS profile, the default is Ascend-CLID.

Example: `set clid = 510-555-1213`

Dependencies: Consider the following:

- For Calling-Line ID (CLID) Callback, you must specify a CLID value.
- If the CLID is present for an incoming call, the TAOS unit can perform CLID authentication before answering the call.
- There is no restriction on specifying the same CLID in multiple Connection profiles.
- The local E.164 address is typically specified by the FR-Address setting in a Frame-Relay profile. If an E.164 address is specified by the CLID setting, it overrides the value of FR-Address.

Location: Connection *station*, External-Auth > Password-Profile

See Also: CLID-Auth-Mode, FR-Address

CLID-Auth-Mode

Description: Specifies how the TAOS unit uses the telco-provided Calling-Line ID (CLID) and Dialed Number Information Service (DNIS) called number for authenticating incoming calls.

Usage: Specify one of the following values:

- Ignore (the default) specifies that the TAOS unit does not require a matching ID from incoming calls.
- CLID-First specifies that if the CLID is sent by the telco switch, the TAOS unit uses it to authenticate the call. If CLID authentication fails for any reason, or if the telco switch does not provide the CLID, the TAOS unit does not drop the call, but allows negotiations to proceed to password authentication.
- CLID-Prefer specifies that the TAOS unit uses the CLID, if available, to authenticate the call. If the CLID is not provided by the switch, the TAOS unit uses the type of authentication specified by the Send-Auth-Mode setting in the Connection profile. If the CLID is provided by the switch but does not match the calling number specified in a local Connection profile or Remote Authentication Dial-In User Service (RADIUS) user profile, or if the CLID succeeds but the encapsulation protocol's authentication fails, the TAOS unit drops the call.
- CLID-Require specifies that the TAOS unit must receive a CLID from the incoming call, and the CLID must match the calling number specified in a local Connection profile or RADIUS user profile. If the TAOS unit does not receive a CLID, or does not find a matching number in a profile, the TAOS unit does not answer the call. A matching RADIUS user profile can require name and password authentication after CLID authentication by setting Ascend-Require-Auth to Require-Auth.
- CLID-Fallback specifies that the TAOS unit must receive a CLID in the incoming call. Otherwise, the TAOS unit does not answer the call. If the CLID matches a calling number specified in a local Connection profile or RADIUS user profile, the TAOS unit authenticates the call with the CLID. If the TAOS unit does not receive a response from the RADIUS server, it uses the authentication configured in the Answer-Defaults profile.

- **DNIS-First** specifies that if the called number is sent by the telco switch, the TAOS unit uses it to authenticate the call. If called-number authentication fails for any reason, or if the telco switch does not provide the called number, the TAOS unit does not drop the call, but allows negotiations to proceed to password authentication.
- **DNIS-Require** specifies that the called number must match the number specified in a local Connection profile or RADIUS user profile. If the TAOS unit does not find a matching number in a profile, the TAOS unit does not answer the call. You can configure a matching RADIUS user profile to require name and password authentication after called-number authentication by setting Ascend-Require-Auth to Require-Auth.
- **DNIS-Pref** specifies that the TAOS unit uses the called number, if available, to authenticate the call. If the called number is not provided by the switch, the TAOS unit uses the type of authentication specified by the Answer-Defaults profile. If the called number is provided by the switch but does not match the called number specified in a local Connection profile or RADIUS user profile, the TAOS unit drops the call.

Example: `set clid-auth-mode = dnis-pref`

Dependencies: For CLID Callback, you must set CLID-Auth-Mode to CLID-Require. For DNIS Callback, you must set CLID-Auth-Mode to DNIS-Require.

Location: Answer-Defaults

See Also: CalledNumber, CLID

CLID-Selection

Description: Specifies which Calling-Line ID (CLID) to use for an incoming call. A CLID provided by the Public Switched Telephone Network (PSTN) is considered secure. A CLID provided by the end user is secure only if it has been validated by the PSTN. Other forms of user CLIDs are considered insecure.

Usage: Specify one of the following values:

- **First** (the default) specifies that the TAOS unit uses the first CLID provided by the PSTN. The CLID could be provided by either the user or the network.
- **Secure-Prefer** specifies that the TAOS unit uses a secure CLID if one is available. If no secure CLID is available, an insecure CLID will be used, if present.
- **Secure-Require** specifies that the TAOS unit uses a secure CLID if one is available. If no secure CLID is available, the unit behaves as though no CLID is present.
- **User-Prefer** specifies that the TAOS unit uses a user-provided CLID if one is available. If no user-provided CLID is available, the unit choose a network CLID, if present.
- **User-Require** specifies that the TAOS unit uses a user-provided CLID is one is available. If no user-provided CLID is available, the unit behaves as though no CLID is present.

Example: `set clid-selection = secure-prefer`

Location: Answer-Defaults

See Also: CLID

CLID-Suppress

Description: Specifies whether the local TAOS unit blocks transmission of the Calling-Line ID (CLID) received from the remote TAOS unit, excluding it from data passed to the local Public Switched Telephone Network (PSTN).

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

- Yes specifies that the local TAOS unit blocks transmission of the CLID received from the remote TAOS unit.
- No specifies that the local TAOS unit passes the CLID from the remote TAOS unit to the local PSTN.

Example: `clid-suppress = yes`

Dependencies: Changes to CLID-Suppress are effective with the next Voice over IP (VoIP) call.

Location: VoIP {x y}

See Also: CLID

Client-Auth-ID

Description: Specifies the name sent to the Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnel server for authenticating the tunnel.

Usage: Specify up to 31 characters. The default is null.

Example: `set client-auth-id = nyserver`

Dependencies: L2F does not support the Client-Auth-ID setting in a Tunnel-Server profile.

Location: Connection *station* > Tunnel-Options, Tunnel-Server *name*

See Also: Server-Auth-ID

Client-Default-Gateway

Description: Specifies the default gateway to use for traffic from this connection if no specific route appears in the IP routing table.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0, which causes the system to use the Default route.

Example: `set client-default-gateway = 10.207.23.13`

Location: Connection *station* > IP-Options

See Also: Ignore-Def-Route, IP-Options

Client-DNS-Addr-Assign

Description: Specifies whether the TAOS unit presents client Domain Name System (DNS) server addresses while the connection is being negotiated.

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

- Yes specifies that the TAOS unit makes the client DNS server addresses available to the connection.
- No specifies that TAOS unit makes the client DNS server addresses unavailable.

Example: `set client-dns-addr-assign = no`

Location: Connection *station* > IP-Options

See Also: Allow-As-Client-DNS-Info, Client-DNS-Primary-Addr, Client-DNS-Secondary-Addr, Client-Primary-DNS-Server, Client-Secondary-DNS-Server

Client-DNS-Primary-Addr

Description: Specifies a primary Domain Name System (DNS) server address to send to a client that is connecting to the TAOS unit.

A client configuration defines DNS servers that the TAOS unit presents to WAN connections during IP Control Protocol (IPCP) negotiation. These servers provide a way to protect your local DNS information from WAN users. Client DNS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration. The Client-DNS-Primary-Addr setting applies to the connection-specific level.

The TAOS unit uses the global client addresses only if the Connection profile specifies no DNS server addresses. You can also choose to present your local DNS servers to clients if no other servers are defined or available.

Usage: Specify the IP address of the primary DNS server for the connection. Separate the optional subnet mask from the address by using a forward slash. 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 = 10.1.2.3/24`

Dependencies: If Client-DNS-Addr-Assign is set to No, Client-DNS-Primary-Addr does not apply.

Location: Connection *station* > IP-Options

See Also: Allow-As-Client-DNS-Info, Client-DNS-Addr-Assign, Client-DNS-Secondary-Addr, Client-Primary-DNS-Server, Client-Secondary-DNS-Server

Client-DNS-Secondary-Addr

Description: Specifies a secondary Domain Name System (DNS) server address to send to a client that is connecting to the TAOS unit. The unit presents this server address 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. Separate the optional subnet mask from the address by entering a forward slash. 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 = 10.5.6.7/24`

Dependencies: If Client-DNS-Addr-Assign is set to No, Client-DNS-Secondary-Addr does not apply.

Location: Connection *station* > IP-Options

See Also: Allow-As-Client-DNS-Info, Client-DNS-Addr-Assign, Client-DNS-Primary-Addr, Client-Primary-DNS-Server, Client-Secondary-DNS-Server

Client-Primary-DNS-Server

Description: Specifies a primary Domain Name System (DNS) server address to send to a client that is connecting to the TAOS unit or the Virtual Router (VRouter).

Client DNS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration. The Client-Primary-DNS-Server setting defines the global level. The TAOS unit or VRouter uses the global client addresses only if the Connection profile specifies no DNS server addresses. You can also choose to present your local DNS servers to clients if no other servers are defined or available.

Usage: Specify the IP address of a DNS server to use for all connections that do not have a defined DNS server. Separate the optional subnet mask from the address by entering a forward slash. The default is 0.0.0.0/0, which specifies that no primary DNS server is available on a global level.

Example: `set client-primary-dns-server = 10.9.8.7/24`

Location: IP-Global, VRouter *name*

See Also: Allow-As-Client-DNS-Info, Client-DNS-Addr-Assign, Client-DNS-Primary-Addr, Client-DNS-Secondary-Addr, Client-Secondary-DNS-Server

Client-Secondary-DNS-Server

Description: Specifies a secondary Domain Name System (DNS) server address to send to any client connecting to the TAOS unit or the Virtual Router (VRouter).

Client DNS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration. The Client-Primary-DNS-Server setting defines the global level. The TAOS unit or VRouter uses the global client addresses only if the Connection profile specifies no DNS server addresses. You can also choose to present your local DNS servers to clients if no other servers are defined or available.

Usage: Specify the IP address of a secondary DNS server to use for all connections that do not have a DNS server defined. Separate the optional subnet mask from the address by entering a forward slash. The default is 0.0.0.0/0, which specifies that no secondary DNS server is available on a global level.

Example: `set client-secondary-dns-server = 10.9.8.3/24`

Location: IP-Global, VRouter *name*

See Also: Allow-As-Client-DNS-Info, Client-DNS-Addr-Assign, Client-DNS-Primary-Addr, Client-DNS-Secondary-Addr, Client-Primary-DNS-Server

Client-WINS-Addr-Assign

Description: Specifies whether the TAOS unit presents client WINS server addresses to the dial-in client while negotiating the session.

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

- Yes specifies that the TAOS unit presents client WINS server addresses to the dial-in client while negotiating the session.
- No specifies that the TAOS unit does not present client WINS server addresses to the dial-in client while negotiating the session. A No setting still enables the PC to access WINS name resolution if NetBIOS servers have been configured in the IP-Global profile.

Example: `set client-wins-addr-assign = no`

Dependencies: For the client WINS feature to work, the PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings. In addition, a WINS server must be specified by the Client-WINS-Primary-Addr setting. You can specify a backup WINS server by setting the Client-WINS-Secondary-Addr value.

Location: Connection *station* > IP-Options

See Also: Client-WINS-Primary-Addr, Client-WINS-Secondary-Addr, NetBIOS-Primary-NS, NetBIOS-Secondary-NS

Client-WINS-Primary-Addr

Description: Specifies the IP address of the primary WINS server. The primary server is used for WINS name resolution. The secondary server, if specified, is used only if the primary server is unavailable.

Usage: Specify the IP address of a WINS server.

Example: `set client-wins-primary-addr = 10.1.1.1`

Dependencies: For the client WINS feature to work, the PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings. In addition, Client-WINS-Addr-Assign must be set to Yes for the server address to be passed to the dial-in client during session negotiation.

Location: Connection *station* > IP-Options

See Also: Client-WINS-Addr-Assign, Client-WINS-Secondary-Addr, NetBIOS-Primary-NS, NetBIOS-Secondary-NS

Client-WINS-Secondary-Addr

Description: Specifies the IP address of the secondary WINS server. The secondary server is used for WINS name resolution only if the primary server is unavailable.

Usage: Specify the IP address of a WINS server.

Example: `set client-wins-secondary-addr = 20.1.1.1`

Dependencies: For the client WINS feature to work, the PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings. In addition, Client-WINS-Addr-Assign must be set to Yes for the server address to be passed to the dial-in client during session negotiation.

Location: Connection *station* > IP-Options

See Also: Client-WINS-Addr-Assign, Client-WINS-Primary-Addr, NetBIOS-Primary-NS, NetBIOS-Secondary-NS

Clocking

Description: A subprofile containing settings for an internal clock on the Serial WAN (SWAN) line.

Usage: With the Line-Config subprofile as the working profile, list the Clocking settings. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Clocking subprofile:

```
admin> list clocking
[in SWAN {shelf-1 slot-13 2}:line config:clocking]
clock-mode = external-clock
divider = 1
exp = 2
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: SWAN {shelf-*N* slot-*N* *N*} > Line-Config

See Also: Clock-Mode, Divider, Exp

Clock-Mode

Description: Specifies whether the Serial WAN (SWAN) card generates an internal clock.

Usage: Specify one of the following values:

- External-Clock (the default) specifies that the SWAN line receives a clock from an external source.
- Internal-Clock specifies that the SWAN line generates its own clock.

Example: `set clock-mode = internal-clock`

Location: SWAN {shelf-*N* slot-*N* *N*} > Line-Config > Clocking

See Also: Divider, Exp

Clock-Priority

Description: Assigns a clock priority to a T1 or E1 line. When multiple lines are eligible to be the clock source for synchronous transmissions, the TAOS unit uses the value you specify to select a line as the master clock source. If multiple lines are eligible to be the clock source, and each line has an equal Clock-Priority value, the TAOS unit chooses a source at random.

Usage: Specify one of the following values:

- High-Priority specifies the highest priority. The TAOS unit chooses a line with this priority setting as the clock source over other lines with a lower priority. If more than one line has the highest priority, the first available line becomes the clock source.
- Middle-Priority specifies the second priority. The TAOS unit chooses a line with this priority setting if every line with a High-Priority setting is unavailable. If more than one line has a Middle-Priority setting, the first available Middle-Priority line becomes the clock source.
- Low-Priority specifies the lowest priority. The TAOS unit chooses a line with this priority only if every line with a higher priority setting is unavailable. If more than one line has a Low-Priority setting, the first available Low-Priority line becomes the clock source.

Once the TAOS unit chooses a line as the clock source, it uses that line until the line becomes unavailable, or a until a higher-priority source becomes available.

Example: `set clock-priority = middle-priority`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface, T1 {shelf-*N* slot-*N* *N*} > Line-Interface, OC3-ATM {shelf-*N* slot-*N* *N*} > Line Config

See Also: Clock-Source, Line-Interface

Clock-Source

Description: Specifies whether the TAOS unit can use the T1 or E1 line as the master clock source for synchronous connections.

Usage: Specify one of the following values:

- Eligible (the default) specifies that the TAOS unit can use the line as the master clock source.
- Not-Eligible specifies that the TAOS unit cannot use the line as the master clock source.

Example: `set clock-source = eligible`

Location: E1 {shelf-*N* slot-*N N*} > Line-Interface, T1 {shelf-*N* slot-*N N*} > Line-Interface, OC3-ATM {shelf-*N* slot-*N N*} > Line Config

See Also: Clock-Priority, Line-Interface

Coldstart-Enabled

Description: Specifies whether the system generates a trap when the TAOS unit reinitializes itself in such a way that the configuration of the Simple Network Management Protocol (SNMP) manager or of the system itself might be altered.

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

- Yes specifies that the system generates a trap when a reinitialization might alter the configuration of the SNMP manager or of the system itself.
- No specifies that when a reinitialization might alter the configuration of the SNMP manager or of the system itself, no trap is generated.

Example: `set coldstart-enabled = no`

Location: Trap *host-name*

See Also: Warmstart-Enabled

Collect-Incoming-Digits

Description: Specifies whether the Digital Signal Processor (DSP) decodes the calling and called Dual Tone Multifrequency (DTMF) digits on a T1 line that uses inband signaling, making Dialed Number Information Service (DNIS) and Calling-Line ID (CLID) information presented by the switch available for authentication and accounting.

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

- Yes specifies that the DSP decodes the DTMF digits.
- No specifies that the DSP does not decode the DTMF digits.

Example: `set collect-incoming-digits = yes`

Dependencies: You must set Signaling-Mode to Inband for Collect-Incoming-Digits to have any effect.

Location: T1 {shelf-*N* slot-*N N*} > Line-Interface

See Also: DSP-DTMF-Input-Sample-Count, Signaling-Mode

Command-Spoof

Description: Enables or disables spoofing of certain fax commands. Command spoofing is a method of improving performance and reducing fax errors on low-latency networks.

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

Example: `set command-spoof = no`

Dependencies: For Command-Spoof to apply, you must set RT-Fax-Enable to Yes.

Location: VoIP {x y} > RT-Fax-Options

See Also: ECM-Enable, Local-Retransmit-LSF, Low-Latency-Mode, RT-Fax-Enable

Community-Name

Description: Specifies the Simple Network Management Protocol (SNMP) community name associated with SNMP Protocol Data Units (PDUs). The string you specify becomes a password that the TAOS unit sends to the SNMP manager when an SNMP trap event occurs. The password authenticates the sender identified by Host-Address.

Usage: Specify the community name. You can enter up to 31 characters. The default is `public`.

Example: `set community-name = unit0`

Location: Trap *host-name*

See Also: Alarm-Enabled, Host-Address, Host-Name, Port-Enabled, Security-Mode

Comp-Neq

Description: Specifies the type of comparison to make between a packet's contents and the filter's Value setting.

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

- Yes specifies that the comparison succeeds when the values are not equal.
- No specifies that the comparison succeeds when the values are equal.

Example: `set comp-neq = no`

Dependencies: Comp-Neq applies only when Type is set to Generic-Filter.

Location: Filter *filter-name* > Input-Filters > Gen-Filter,
Filter *filter-name* > Output-Filters > Gen-Filter

See Also: Gen-Filter, Input-Filters, Output-Filters, Type

Config-Change-Enabled

Description: Specifies whether the unit generates a trap whenever the system configuration is modified or a new software version is loaded. The trap has an integer value of 30. The accompanying string contains the date and time the change occurred, and information about the user that changed the configuration or software version. The trap has the following format:

Date, Time, "Configuration changed by user profile (YYY)."

YYY indicates the name of the User profile.

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

- Yes specifies that the unit generates a trap whenever the system configuration is modified or a new software version is loaded.
- No specifies that the unit does not generate a trap whenever the system configuration is modified or a new software version is loaded.

Example: `set config-change-enabled = no`

Location: Trap *name*

See Also: Coldstart-Enabled

Congested-Metric

Description: Specifies a number from 0 to 255 to use as a transaction server's current metric the server sends a Quick Transaction Protocol (QTP) status message with a Flow Control attribute set to Congested.

Usage: Specify a number from 0 to 255. The default is 10.

Example: `set congested-metric = 15`

Location: Transaction-Server

See Also: Available-Metric, Partly-Congested-Metric, Shutdown-Metric

Congestion-Control

Description: A subprofile that enables you to configure congestion-control for an SS7 configuration.

Usage: With SS7-Gateway as the working profile, list the Congestion-Control subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Congestion-Control subprofile:

```
admin> list congestion-control
[In SS7-GATEWAY:congestion-control]
congestion-control-type = l3-queue-depth
cl1-level = 60
cl1-action = send-info-to-mgc
cl2-level = 120
cl2-action = reject-new-call
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: SS7-Gateway

See Also: CL1-Action, CL1-Level, CL2-Action, CL2-Level

Congestion-Control-Type

Description: Specifies the congestion-control algorithm to use.

Usage: Specify one of the following settings:

- None specifies that congestion control is disabled.
- L3-Queue-Depth (the default) specifies that the unit measures the depth of the Layer-3 queue as the criterion for congestion.

Example: `set congestion-control-type = none`

Location: SS7-Gateway > Congestion-Control

See Also: CL1-Action, CL1-Level, CL2-Action, CL2-Level

Connection

Description: A profile containing connection-specific information, including authentication settings, compression values, filter specifications, and telco options.

The TAOS unit uses the settings in the Answer-Defaults profile to answer a call and determine whether to attempt to build a connection. It then looks for a Connection profile or Remote Authentication Dial-In User Service (RADIUS) user profile.

Usage: Use the Read and List commands to read a Connection profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Connection profile `newyork` the working profile and list its contents:

```
admin> read connection newyork
CONNECTION/newyork read
```

```

admin> list
[in CONNECTION/newyork]
station* = newyork
active = no
encapsulation-protocol = mpp
called-number-type = national
dial-number = ""
sub-address = ""
clid = ""
ip-options = { yes yes 0.0.0.0/0 0.0.0.0/0 1 60 120 no no 0 +
ipx-options = { no router-peer both both no 00:00:00:00 +
bridging-options = { 0 no }
session-options = { "" "" no no 120 no-idle 120 "" 0 disabled +
telco-options = { ans-and-orig no off 1 no no 56k-clear 0 "" "" +
ppp-options = { no-ppp-auth none "" "" "" "" stac 1524 no 600+
mp-options = { 1 1 2 no no }
mpp-options = { "" quadratic transmit 1 1 15 5 10 70 }
fr-options = { "" pvc 16 "" transparent-link no "" 16 "" }
tcp-clear-options = { "" 0 "" 0 "" 0 "" 0 no "" 256 20 }
ara-options = { "" 0 }
vl20-options = { 7 3 1500 30000 256 }
x75-options = { 7 10 1000 1024 }
appletalk-options = { no "" 0 0 router-peer }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
dhcp-options = { no 1 4 }
shared-prof = no
framed-only = no
tunnel-options = { disabled atmp-protocol 0 rip-off "" "" 5150 +
vrouter = ""
atm-options = { aal5-llc 0 32 no "" none 1 { no { undefined "" +
hdlc-nrm-options = { 2000 2 60000 5000 2 yes yes 255 }
visa2-options = { 10000 04 06 15 05 03 00:03:00:00 }
sdtm-packets-server = no
AT-string = ""
port-redirect-options = { none 0 0.0.0.0 }

```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```

admin> write
CONNECTION/newyork written

```

See Also: Active, ATM-Options, AT-String, CalledNumber, Called-Number-Type, CLID, DHCP-Options, Dial-Number, Encapsulation-Protocol, IP-Options, PPP-Options, SDTN-Packets-Server, Session-Options, Station, Subaddress, Telco-Options, UsrRad-Options, VRouter

Console-Enabled

Description: Specifies whether the system generates a trap when the console has changed state. The console entry can be read to see what its current state is.

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

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

Example: `set console-enabled = no`

Location: Trap *host-name*

See Also: Ascend-Enabled

Contact

Description: Specifies the person or department to contact for reporting error conditions. The Contact value is Simple Network Management Protocol (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

See Also: Location

Context-Stats

Description: A read-only subprofile containing controller-statistics subprofiles, one for each controller.

Usage: With Redundancy-Stats as the working profile, use the List command to display the Context-Stats subprofiles. To close the Context-Stats subprofile and return to a higher context in the profile, enter the List command, followed by a space and two periods.

Example: `admin> list context-stats`
[in REDUNDANCY-STATS]
context-stats[1]={ monitoring secondary defer-to-running +
context-stats[2]={ monitoring secondary defer-to-running +

Location: Redundancy-Stats

See Also: Context-Stats N

Context-Stats *N*

Description: A read-only subprofile of the Context-Stats subprofile. Context-Stats *N* contains configuration options for an individual controller. The index for each subprofile is a controller number.

Usage: With a Redundancy-Stats profile as the working profile, use the List command to display the statistics for one of the controllers. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: The following example shows statistics for the primary controller:

```
admin> list context-stats 1
[in REDUNDANCY-STATS:context-stats[1]]
state = monitoring
function = secondary
select-reason = defer-to-running-primary
prior-function = no-function
last-reboot = crash
fan = { 317873482 }
```

Location: Redundancy-Stats > Context-Stats

See Also: Fan, Function, Last-Reboot, Prior-Function, Select-Reason, State

Control-Connect-Establish-Timer

Description: Specifies the maximum number of seconds during which the TAOS unit can establish an Layer 2 Tunneling Protocol (L2TP) tunnel with another unit. Any change you make to this value takes effect when the previous timer expires.

Usage: Enter a decimal number from 0 to 600. The default is 60.

Example: `set control-connect-establish-timer = 60`

Dependencies: Control-Connect-Establish-Timer applies only if you have set L2TP-Mode to LAC.

Location: L2-Tunnel-Global > L2TP-Config

See Also: First-Retry-Timer, Hello-Timer, LAC-Incoming-Call-Timer, Retry-Count

Control-Protocol

Description: Specifies the signaling protocol that controls the Signaling System 7 (SS7) gateway.

Usage: Specify one of the following settings:

- ASGCP sets the signaling gateway control to the proprietary protocol ASGCP. This setting enables the unit to communicate with an ICD for Softswitch using ASGCP-Q.931+.
- IPDC-0.x sets the signaling gateway control to IPDC support for SS7 gateways. It specifies XCOM/Level 3 Internet Protocol Device Control (IPDC) 0.12, which enables the unit to communicate with a Lucent Technologies Softswitch using IPDC.
- Q931-Plus sets the signaling gateway control to IMT support over IP Q.931. This setting enables the unit to communicate with a PacketStar Connection Gateway.

Example: `set control-protocol = ipdc-0.x`

Dependencies: Consider the following:

- If only one control protocol is licensed, the setting defaults to the licensed protocol and cannot be modified. However, if multiple protocols are licensed, the Control-Protocol setting defaults to ASGCP. Because of this default and because the TAOS unit does not store unmodified profile items in NVRAM, the setting can be modified unintentionally when you upgrade to new software or enable a new license to support another SS7 control protocol. For this reason, Lucent recommends that you verify the setting after upgrading. If the proper protocol is not specified, change the setting and then reset the unit.
- Although the control protocol is configurable in real time, you must reset the TAOS unit to begin using the new protocol. After the unit is reset, it establishes a new TCP link to the signaling gateway and begins using the specified control protocol to communicate with the signaling gateway.

Location: SS7-Gateway

See Also: System-Type

Cost

Description: Specifies the cost of an Open Shortest Path First (OSPF) link. The lower the cost, the more likely OSPF will use the interface to forward data traffic.

Usage: Specify a number greater than 0 and less than 16777215. 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 0xFFFFFFFF (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 TAOS 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 AS.

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* } *N* } > OSPF, IP-Route *name*

See Also: ASE-Type, IP-Options, OSPF, OSPF-Options

Countries-Enabled

Description: Contains a bit set identifying the enabled countries.

Usage: The Countries-Enabled setting is read only.

Example: `countries-enabled = 0`

Location: Base

See Also: AIM-Enabled, Data-Call-Enabled, Frame-Relay-Enabled, MAXLink-Client-Enabled, Modem-Dialout-Enabled, Multi-Rate-Enabled, R2-Signaling-Enabled, Switched-Enabled

Country

Description: Enables the TAOS unit to generate country-specific local call-progress tones (such as a dial tone and busy signals) on the basis of the ITU-T specification TSB Circular 18: *Update of Supplement No. 2, ITU-T (former CCITT) Blue Book, Fascicle II.2 - Various tones used in national networks.*

Usage: Specify one of the following values for MultiVoice:

Argentina
Australia
Belgium
China
Costa-Rica
Finland
France
Germany
Hong-Kong
Italy
Japan
Korea
Mexico
Netherlands
New-Zealand
Singapore
Spain
Sweden
Switzerland
UK
US (the default)

Example: `set country = france`

Dependencies: Consider the following:

- If Cut-Thru-Enable-Nearend is set to Yes, the Country value applies only to dial tone, busy, fast-busy, and number-unobtainable tones. Ringback is typically carried by means of Real-Time Transport Protocol (RTP) from the remote end in this case.
- If announcements are enabled (H323-Voice-Ann-Enabled is set to Yes), the Country value applies only to busy and number-unobtainable tones. Announcements are played in all other cases with this configuration.

Location: System

See Also: Cut-Thru-Enable-Nearend, H323-Voice-Ann-Enabled, Idle-Timer, Max-Dialout-Time, Parallel-Dialing

CSU-Build-Out

Description: Specifies the line buildout value for a T1 line connected to an internal Channel Service Unit (CSU). The buildout value is the amount of attenuation the TAOS unit should apply to the line's network interface to compensate for the interface being too close to a repeater.

Usage: After checking with your carrier to determine the correct value, specify one of the following decibel values:

0-dB (the default)

7.5-dB

15-dB

22.5-dB

Example: `set csu-build-out = 0-db`

Dependencies: CSU-Build-Out applies only if the T1 line has an internal CSU.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Front-End-Type, Line-Interface

Current-State

Description: Indicates the current operational state of the slot.

Usage: The Current-State value is read only. It can have one of the following values:

State	Description
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	Although the slot is no longer down, it 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.

State	Description
Oper-State-Post indicates	The slot is running a self-test.
Oper-State-None	The slot is empty.

Location: Slot-State {shelf-*N* slot-*N* *N*}

See Also: Channel-State, Line-State

Cut-Thru-Enable-Nearend

Description: Specifies whether call-progress tones from the distant Public Switched Telephone Network (PSTN) are passed across the IP network to the local TAOS unit. This feature allows callers at either end of a MultiVoice call to hear the call-progress tones from the distant PSTN, and provides answer supervision for MultiVoice networks using non-PRI trunks.

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

- Yes specifies that the local TAOS unit plays call-progress tones from the remote device. PSTN-generated call-progress tones are passed across the IP network between MultiVoice gateways. These audio signals from the distant PSTN are compressed by the remote gateway for transmission across the IP network, and then decompressed by the local gateway and played for the caller.
- No specifies that callers hear silence until the local TAOS unit generates call-progress tones in response to Q.931 messages.

Example: `set cut-thru-enable-nearend = no`

Dependencies: Consider the following:

- When call volumes increase, setting Cut-Thru-Enable-Nearend to No can improve call performance.
- Changes to the value of Cut-Thru-Enable-Nearend become effective with the next call.

Location: VoIP {*x y*}

D

Data

Note: The TAOS unit does not support firewalls at this time.

Description: Contains information about the firewall definition.

Usage: If you list the Data setting separately, it appears as a sparse array:

```
admin> list data
[in FIREWALL/berkeley]
data[0] = ACAfiwgAAAAAAADE2RmZDTiz0zOLeDkBAAFTVl4DAAA
data[33] = AA
data[66] =
```

Location: Firewall *name*

See Also: Version

Data-Ack-Timeout

Description: Specifies the number of milliseconds that the TAOS unit waits for a transaction server to send a Quick Transaction Protocol (QTP) Acknowledge in response to a QTP data message.

Usage: Specify a number from 500 to 30000. The default is 10000.

Example: `set data-ack-timeout = 5000`

Location: Transaction-Server

See Also: Keep-Alive-Timeout

Data-Call-Enabled

Description: Indicates whether the TAOS unit supports data calls over ISDN lines.

Usage: The Data-Call-Enabled setting is read only. Yes indicates that the TAOS unit supports data calls over ISDN lines. No indicates that the TAOS unit does not support data calls over ISDN lines.

Example: `data-call-enabled = yes`

Location: Base

See Also: AIM-Enabled, Countries-Enabled, D-Channel-Enabled, Firewalls-Enabled, Frame-Relay-Enabled, MAXLink-Client-Enabled, Modem-Dialout-Enabled, Multi-Rate-Enabled, Network-Management-Enabled, R2-Signaling-Enabled, Selectools-Enabled, Switched-Enabled, Toggle-Screen

Data-Filter

Description: Specifies the name of a filter the TAOS unit uses to determine whether it should forward or drop a packet. If the TAOS unit 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 can reach the call filter.

Usage: Specify the filter name. The default is null, which specifies that the TAOS unit does not apply a data filter.

Example: `set data-filter = ip-spoof`

Dependencies: Data-Filter applies only when the Filter-Name setting specifies a data filter.

Location: Answer-Defaults > Session-Info, Connection *station* > Session-Options

See Also: Call-Filter, Filter, Filter-Name, Filter-Persistence, Session-Info, 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 is advertised instead.

Example: `set data-ip-address = 1.1.1.1`

Dependencies: The TAOS unit supports a soft IP interface, which is an internal interface that never goes down. Routing protocols always advertise the soft interface address as reachable on all interfaces that are up 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 TAOS 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 in order 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 *name*

See Also: Multicast-Address, Multicast-Interface-IP-Address

Data-Sense

Description: Specifies whether the D channel uses normal or inverted data. Inverted data has 1s changed into 0s, and 0s into 1s. In some connections, you need to invert the data to avoid transmitting a pattern that the connection cannot handle. If you use inverted data, you should do so on both sides of the connection.

Usage: Specify one of the following values:

- Normal (the default) specifies noninverted data.
- Inv specifies inverted data.

Example: `set data-sense = normal`

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface

Data-Service

Description: For a switched connection, specifies the type of service requested of the switch. For a nailed-up connection, specifies the bandwidth to use per channel.

Usage: Specify one of the following settings:

Setting	Specifies
Voice (switched calls only)	The call should be set up as a voice call, even if the TAOS unit transmits data over the channel.
56K	The data rate to use with a switched-services line that uses Alternate Mark Inversion (AMI) and/or robbed-bit signaling.
56K-Restricted (the default)	Data is transmitted to meet the density requirements for AMI-encoded T1 lines.
56K-Clear	The call should be set up as a data call that uses 56 Kbps of the bandwidth of the data channel.
64K-Restricted	The call should be set up as a data call at a rate of 64 Kbps on an AMI-encoded line on which the sender transmits only non-zero data. Use this setting with LAPD and AMI signaling.
64K-Clear	The call should be set up as a data call that uses the full 64-Kbps bandwidth of the data channel. Use this setting with B8ZS, LAPD, and Signaling System 7 (SS7) signaling.
384K-Clear (switched calls only)	The call should be set up as a data call that connects to the Switched-384 data service. This AT&T data service does not require Multi-Rate or GlobanD.
384K-Restricted (switched calls only)	The call should be set up as a data call that connects to Multi-Rate or GlobanD data services at 384 Kbps.
DWS-384-clear (switched calls only)	A 384-Kbps call coded as Multi-Rate, not H0.

Setting	Specifies
1536K-Clear (switched calls only)	The call should be set up as a data call that connects to the Switched-1536 data service at 1536 Kbps. Non-Facility Associated Signaling (NFAS) 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 (switched calls only)	The same as 1536K-Clear, but with a request for restricted data transfer. A binary 1 is inserted with each transmission in the least significant bit.
128K-Clear to 1472K-Clear, in multiples of 64 (switched calls only)	Available on a T1 PRI line with Multi-Rate or GlobanD data services. You can specify the following values: 128K-Clear, 192K-Clear, 256K-Clear, 320K-Clear, 448K-Clear, 512K-Clear, 576K-Clear, 640K-Clear, 704K-Clear, 768K-Clear, 832K-Clear, 896K-Clear, 960K-Clear, 1024K-Clear, 1088K-Clear, 1152K-Clear, 1216K-Clear, 1280K-Clear, 1344K-Clear, 1408K-Clear, 1472K-Clear
Modem (switched calls only)	When the call is up, it goes to a digital modem.
Frame-Relay-SVC	Frame Relay Switched Virtual Circuit (SVC).
144-56k-v110	56Kbps unrestricted data transfer and a V.110 bit rate of 14,400bps.
288-56k-v110	56Kbps unrestricted data transfer and a V.110 bit rate of 28,800bps.
144-56kr-v110	56Kbps restricted data transfer and a V.110 bit rate of 14,400bps.
288-56kr-v110	56Kbps restricted data transfer and a V.110 bit rate of 28,800bps.
144-64k-v110	64Kbps unrestricted data transfer and a V.110 bit rate of 14,400bps.
288-64k-v110	64Kbps unrestricted data transfer and a V.110 bit rate of 28,800bps.
144-64kr-v110	64Kbps restricted data transfer and a V.110 bit rate of 14,400bps.
288-64kr-v110	64Kbps restricted data transfer and a V.110 bit rate of 28,800bps.

Example: `set data-service = voice`

Dependencies: To ensure data integrity when Data-Service is set to Voice:

- Use only digital end-to-end connectivity. No analog signals should be present 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. Analog lines can echo, and the technology that takes out the echoes can also scramble data in the link.
- Do not make any modifications that can change the data in the link.
- If a V.110 device makes a call at 14,400bps or 28,800bps to a TAOS unit with a MultiDSP or MultiDSP2 card, the call automatically connects at 14,400bps or 28,800bps, regardless of the setting of Data-Service.
- Data-Service is automatically set to Frame-Relay-SVC when you set Circuit-Type to SVC.

Location: Connection *station* > Telco-Options

See Also: Call-Type, Circuit-Type, Telco-Options

Date

Description: A subprofile that shows the day of the week and the current system date.

Usage: With the Timedate profile as the working profile, list the Date subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Date subprofile:

```
admin> list date
[in TIMEDATE]
weekday = Friday
month = June
day = 2
year = 2000
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Timedate

See Also: Time

DCEN392-Val

Description: Specifies the total number of errors, during DCE-N392-monitored events, that causes 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 DCEN393-Val. 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 *fr-name*

See Also: DCEN393-Val, Link-Type

DCEN393-Val

Description: Specifies the DCE-monitored event count.

Usage: Specify a value from 1 to 10. The value you specify must be greater than 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 *fr-name*

See Also: DCEN392-Val, Link-Type

D-Channel-Enabled

Description: Indicates whether the unit enables D-channel (ISDN) signaling.

Usage: The D-Channel-Enabled setting is read only. Yes indicates that the unit supports D-channel signaling. No indicates that the unit does not support D-channel signaling.

Location: Base

See Also: Data-Call-Enabled, Multi-Rate-Enabled, R2-Signaling-Enabled, Switched-Enabled

Dead-Interval

Description: Specifies the number of seconds the Open Shortest Path First (OSPF) router waits for Hello packets before deciding that its neighbor is down.

Usage: Specify a number from 0 to 65535. The default is 40 for a connected route, and 120 for a WAN connection.

Example: `set dead-interval = 40`

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* } *N* } > OSPF

See Also: Hello-Interval, IP-Options, OSPF, OSPF-Options

Decrement-Channel-Count

Description: Specifies the number of channels the TAOS unit removes as a bundle when bandwidth changes, either manually or automatically, during a call.

Usage: Specify an integer from 1 to 32. The default is 1.

Example: `set decrement-channel-count = 1`

Dependencies: You cannot clear a call by decrementing channels.

Location: Answer-Defaults > MPP-Answer, Connection *station* > MPP-Options

See Also: Add-Persistence, Bandwidth-Monitor-Direction, Base-Channel-Count, Dynamic-Algorithm, Increment-Channel-Count, Maximum-Channels, Minimum-Channels, MPP-Answer, MPP-Options, Seconds-History, Sub-Persistence, Target-Utilization

Default-Call-Type

Description: Specifies a default call type for calls on non-ISDN E1 or T1 lines. The TAOS unit uses the default type for call routing if no explicit routes are found.

Usage: Specify one of the following values:

- Digital (the default) specifies that the TAOS unit treats incoming calls as digital.
- Voice specifies that the TAOS unit treats incoming calls as voice calls from a modem. You must specify Voice for IP-Fax over inband signaling.
- VoIP specifies that the TAOS 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.

Dependencies: The VoIP setting is supported only when VoIP-Enabled is set to Yes. You must specify VoIP for T1 or E1 trunks with incoming Voice over IP (VoIP) calls that require true connect. Specifying VoIP causes *all* calls received on the trunk to be mapped to VoIP.

Example: `set default-call-type = voice`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface, T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface

Default-Filter-Cache-Time

Description: Specifies the default time (in minutes) during which the Remote Authentication Dial-In User Service (RADIUS) filter profile remains locally cached on the TAOS unit.

Usage: Specify an integer. The default is 1440 minutes (24 hours). If you specify 0 (zero), the system does not cache the profile.

Example: `set default-filter-cache-time = 720`

Location: IP-Global

See Also: Filter-Required

Default-Lease-Duration

Description: Specifies the valid lease period (in seconds) for assignments from the pool specified by Default-Pool.

Usage: Specify an integer. The default is 0 (zero), which places no time limit on assigned leases from the pool specified by Default-Pool.

Example: `set default-lease-duration = 1440`

Location: IP-Global > DHCP-Server

See Also: Active, Boot-File-Path, Default-Max-Lease, Default-Pool, Lease-Duration, Server-Address, Static-Address, TFTP-Host-Name

Default-Max-Lease

Description: Specifies the maximum number of lease renewals authorized for assignments from the pool specified by Default-Pool.

Usage: Specify an integer. The default is 0 (zero), which specifies no limit on the number of lease renewals.

Example: `set default-max-lease = 5`

Location: IP-Global > DHCP-Server

See Also: Active, Boot-File-Path, Default-Lease-Duration, Default-Pool, Lease-Duration, Server-Address, Static-Address, TFTP-Host-Name

Default-Pool

Description: Specifies an address pool number to be used for all assignments that require no Connection profile (such as a host connected to a local Ethernet segment).

Usage: Specify a pool number. The default is 0 (zero).

Example: `set default-pool = 5`

Location: IP-Global > DHCP-Server

See Also: Active, Boot-File-Path, Default-Lease-Duration, Default-Max-Lease, Lease-Duration, Server-Address, Static-Address, TFTP-Host-Name

Default-Prt-Cache-Time

Description: Specifies the default cache time for private-route profiles configured in Remote Authentication Dial-In User Service (RADIUS).

Usage: Specify an integer in minutes. The default is 1440 minutes. If you set Default-Prt-Cache-Time to 0 (zero), RADIUS private-route profiles are not cached.

Example: `set default-prt-cache-time = 1200`

Dependencies: The system uses the Default-Prt-Cache-Time value only if no cache time is specified in the RADIUS private-route profile.

Location: IP-Global

See Also: Private-Route-Profile-Required, Private-Route-Table

Default-Status

Description: Specifies whether or not the TAOS unit displays the status screen by default when the user logs in.

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

- Yes (the default) specifies that the TAOS unit displays the status screen when it authenticates the profile.
- No specifies that the TAOS unit does not display the status screen when it authenticates the profile.

Example: `set default-status = yes`

Dependencies: Default-Status applies to Telnet and console logins. It does not apply to use of the Auth command.

Location: User *name*

See Also: Bottom-Status, Left-Status, Top-Status

Delay

Description: On an incoming modem or V.120 call, specifies the number of seconds the TAOS unit waits for PPP packets before it changes to terminal-server mode. If it detects PPP, the TAOS unit routes the packets to its router. Otherwise, it displays the Telnet or terminal-server login prompt. If the caller's Connection profile specifies Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) authentication, and the first data received at the Telnet or terminal-server login prompt is PPP-encapsulated, the TAOS unit transitions to packet-mode processing immediately.

Usage: Specify an integer from 1 to 60. The default is 5.

Example: `set delay = 15`

Dependencies: If terminal services are disabled, Delay does not apply.

Location: Terminal-Server > PPP-Mode-Configuration

See Also: PPP-Mode-Configuration

Delay-Callback

Description: Specifies the number of seconds the TAOS unit waits before calling back a remote user.

Usage: Specify an integer from 0 to 60. The unit treats values of 0–3 as 3 seconds. The default is 0 (zero).

Example: `set delay-callback = 5`

Dependencies: If Callback is set to No, Delay-Callback does not apply.

Location: Connection > Telco-Options

See Also: Answer-Originate, Billing-Number, Callback, Call-By-Call, Call-Type, Data-Service, Dialout-Allowed, Expect-Callback, Force-56Kbps, FT1-Caller, Nailed-Groups, Transit-Number

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 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 indicates that the TAOS unit should change the device state in a graceful manner.

Usage: Specify one of the following values:

- Admin-State-Down specifies that the addressed device should terminate all operations and enter the down state.
- Admin-State-Up 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 Simple Network Management Protocol (SNMP) Set commands, or the TAOS unit Slot-d and Slot -u commands.

Example: `set desired-state = admin-state-up`

Location: Admin-State {shelf-*N* slot-*N* *N*}, Admin-State-Perm-If *station*, Admin-State-Phys-If {shelf-*N* slot-*N* *N*}

See Also: Desired-Trap-State, Device-Address, Inet-Profile-Type, Modem-Table-Index, Slot-Type, SNMP-Interface

Desired-Trap-State

Description: Indicates the desired up/down enable state of the interface.

Usage: The Desired-Trap-State setting is read only. The system can set it to one of the following values:

- Trap-State-Enabled indicates that an operator has specified that linkUp/linkDown traps should be generated for the interface.
- Trap-State-Disabled indicates that an operator has specified that linkUp/linkDown traps should not be generated for the interface.

Example: `desired-trap-state = trap-state-enabled`

Location: Admin-State-Perm-If *station*, Admin-State-Phys-If {shelf-*N* slot-*N* *N*}

See Also: Desired-State, Device-Address, Modem-Table-Index, Slot-Type, SNMP-Interface

Dest-Address

Description: Specifies a destination IP address.

Usage: Specify an IP address. The default is 0.0.0.0. In an IP-Route profile or a Route-Description-List *N* subprofile, the null address represents a default route. Packets whose destinations do not match an entry in the routing table are forwarded to the default route. In a Filter profile, the TAOS unit compares Dest-Address to a packet's destination address after applying the Dest-Address-Mask value.

Example: `set dest-address = 10.2.3.4`

Dependencies: In a Filter profile, Dest-Address applies only if Type is set to IP-Filter or TOS-Filter.

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter,
Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter, IP-Route *name*,
Private-Route-Table *name* > Route-Description-List > Route-Description-List *N*

See Also: Input-Filters, IP-Filter, Output-Filters, Type

Dest-Address-Mask

Description: Specifies a mask to apply to a filter's Dest-Address value before comparing the value to the destination address in a packet. You can use the Dest-Address-Mask value to hide either the host portion of an address, or both the host and subnet portion.

After the mask and address are both translated into binary format, the TAOS unit performs a logical AND to apply the mask to the address. The mask hides the address bits that are behind its binary 0s (zeroes).

Usage: Specify a mask of ones and zeros in dotted 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, and specifies the full destination address of a single host.

Example: `set dest-address-mask = 255.255.255.0`

Dependencies: Dest-Address-Mask applies only if Type is set to IP-Filter or TOS-Filter.

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter,
Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter

See Also: Input-Filters, IP-Filter, Output-Filters, Type

Dest-Net-Address

Description: Specifies an IPX network address that the TAOS unit compares to a packet's destination IPX network address.

Usage: Specify an IPX network address in hexadecimal format. The default is 00:00:00:00, which matches all packets.

Example: `set dest-net-address = 01:01:01:01`

Dependencies: Dest-Net-Address applies only if Type is set to IPX-Filter.

Location: Filter *filter-name* > Input-Filters > IPX-Filter,
Filter *filter-name* > Output-Filters > IPX-Filter

See Also: Input-Filters, IPX-Filter, Output-Filters, Type

Dest-Network

Description: Specifies the unique internal network number for the NetWare server.

Usage: Specify a hexadecimal number of up to eight characters. The default is 00000000. NetWare servers are assigned an internal IPX network number by the network administrator.

Example: `set dest-network = 00000001`

Location: IPX-Route *name*

See Also: Active-Route, Hops, Name, Profile-Name, Server-Node, Server-Socket, Server-Type, Ticks

Dest-Node-Address

Description: Specifies an IPX node number that the TAOS unit compares to a packet's destination IPX node number.

Usage: Specify an IPX node number in hexadecimal format. The default is 00:00:00:00, which matches all packets.

Example: `set dest-node-address = 01:01:01:01`

Dependencies: Dest-Node-Address applies only if Type is set to IPX-Filter.

Location: Filter *filter-name* > Input-Filters > IPX-Filter,
Filter *filter-name* > Output-Filters > IPX-Filter

See Also: Input-Filters, IPX-Filter, Output-Filters, Type

Dest-Port

Description: Specifies a value to compare with a packet's destination-port field.

Usage: Specify a number from 0 to 65535. The default is 0 (zero), which matches any port. Port 25 is reserved for SMTP, and is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, port 21 for FTP control sessions, and port 23 for Telnet.

Example: `set dest-port = 25`

Dependencies: Consider the following:

- Dest-Port applies only if Type is set to IP-Filter or TOS-Filter.
- Only TCP and UDP packets contain destination-port fields.
- The Dst-Port-Cmp setting specifies the type of comparison the TAOS unit makes.

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter,
Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter

See Also: Dst-Port-Cmp, Input-Filters, IP-Filter, Output-Filters, Type

Dest-Socket

Description: Specifies an IPX socket number that the TAOS unit compares to a packet's destination IPX socket number.

Usage: Specify an IPX socket number. The default is 00:00, which matches all packets.

Example: `set dest-socket = 01:01`

Dependencies: Dest-Socket applies only if Type is set to IPX-Filter.

Location: Filter *filter-name* > Input-Filters > IPX-Filter,
Filter *filter-name* > Output-Filters > IPX-Filter

See Also: Input-Filters, IPX-Filter, Output-Filters, Type

Detect-End-Of-Packet

Description: Specifies whether the TAOS unit buffers incoming data from TCP-Clear dial-in sessions that do not require V.120 processing.

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

- Yes specifies that after authenticating the session, the TAOS unit begins buffering incoming WAN data. The unit continues buffering data until it receives the specified End-Of-Packet-Pattern, until it reaches the timeout specified by Flush Time, or until the data reaches the maximum packet length specified by Flush-Length, whichever occurs first.
- No specifies that the TAOS unit does not buffer incoming data from a TCP-Clear dial-in session.

Example: `set detect-end-of-packet = yes`

Location: Answer-Defaults > TCP-Clear-Answer, Connection *station* > TCP-Clear-Options

See Also: Enabled, End-Of-Packet-Pattern, Flush-Length, Flush-Time

Device-Address

Description: Specifies the address of any of the following devices:

- High-Level Data Link Control (HDLC) processor
- Channel on an E1, T1, or T3 card
- Modem on a digital modem card
- V.35 interface on a Serial WAN (SWAN) card
- Ethernet interface on an Ethernet card

Usage: The device address has the format {*shelf slot item*}, where:

Syntax element	Description
<i>shelf</i>	Specifies the shelf in which the item resides (always 1).
<i>slot</i>	Specifies the number of the item's expansion slot.
<i>item</i>	Specifies an item, such as a digital modem or T1 line, on the slot card.

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. Use the List and Set commands to modify the Device-Address value.

Example: `admin> list device-address`
[in ADMIN-STATE { shelf-1 slot-9 37 }]
shelf = shelf-1
slot = slot-9
item-number = 37

`admin> set shelf = shelf-2`

As an alternative, you can just use the Set command. For example:

```
admin> set device-address shelf = shelf-2
```

Location: Admin-State {shelf-*N* slot-*N* *N*}, Admin-State-Phys-If {shelf-*N* slot-*N* *N*}, Device-State {{shelf-*N* slot-*N* *N*} *N*}

See Also: Item-Number, Physical-Address, Shelf, Slot

Device-Class

Description: Specifies the class of a device described by the Device-Summary profile.

Usage: The Device-Class setting is read only. It can specify Modem, HDLC, or Unknown.

Example: device-class = modem

Location: Device-Summary

See Also: Disabled-Count, Operational-Count, Total-Count

Device-ID

Description: Specifies the logical Signaling System 7 (SS7) command control device to which the Transport-Options settings apply.

Usage: Specify an integer. The default is 0 (zero).

Example: set device-id = 356

Location: SS7-Gateway > Transport-Options

See Also: ACK-Threshold, Heart-Beat, T1-Duration, T2-Duration, T3-Duration, Window-Size

Device-State

Description: Specifies the current operational state of a device.

Usage: Device-State is read only. It can have one of the following values:

- 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.

Example: device-state = up-dev-state

Location: Device-State {{shelf-*N* slot-*N* *N*} *N*}

See Also: Reqd-State

Device-State (profile)

Description: A profile that stores the current state of a device. The TAOS unit creates a Device-State profile for each DS0 and each SCA when the card enters the Up state. The unit does not store the Device-State profile in NVRAM, so the profile's settings do not persist across system resets or power cycles. The Device-State setting might differ from the Req-State setting during state changes, such as when a device is being brought down. State changes are complete when the Device-State and the Req-State match.

Usage: To make Device-State the working profile, use the Read command, specifying a shelf value of 1, and a slot, item, and logical item number. To list the contents of the Device-State profile, enter the List command.

Example: To make the Device-State profile with the index {{shelf-1 slot-4 2}15} the working profile and list its contents:

```
admin> read device-state {{1 4 2}15}
DEVICE-STATE/{ { shelf-1 slot-4 2 } 15 } read
admin> list
[in DEVICE-STATE/{ { shelf-1 slot-4 2 } 15 }]
device-address* = { { shelf-1 slot-4 2 } 15 }
device-state = down-dev-state
up-status = idle-up-status
reqd-state = up-reqd-state
```

Dependencies: A Simple Network Management Protocol (SNMP) manager can read the Device-State profile. The Device-State values are read only.

See Also: Device-Address, Device-State, Req-State, Up-Status

Device-Summary

Description: A read-only profile that supplies information about different classes of host devices available in the system.

Usage: Use the Read and List commands to make Device-Summary the working profile and list its contents.

```
Example: admin> read device-summary modem
DEVICE-SUMMARY/modem read
admin> list
[in DEVICE-SUMMARY/modem]
device-class* = modem
total-count = 48
operational-count = 48
disabled-count = 48
```

Dependencies: The Device-Summary profile is available in RAM only. It is not stored in NVRAM or by the Save command.

See Also: Device-Class, Disabled-Count, Operational-Count, Total-Count

DHCP-Options

Description: A subprofile that enables you to configure a connection to obtain its IP address by means of Dynamic Host Configuration Protocol (DHCP).

Usage: With a Connection profile as the working profile, list the DHCP-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the DHCP-Options subprofile:

```
admin> list dhcp-options
[in CONNECTION/robin:dhcp-options]
reply-enabled = no
pool-number = 1
maximum-leases = 4
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: Maximum-Leases, Pool-Number, Reply-Enabled

DHCP-Server

Description: A subprofile that enables you to configure the TAOS unit as a Dynamic Host Configuration Protocol (DHCP) server.

Usage: With the IP-Global profile as the working profile, list the DHCP-Server subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the DHCP-Server subprofile:

```
admin> list dhcp-server
[in IP-GLOBAL:dhcp-server]
active = no
lease-duration = 0
default-pool = 0
default-max-lease = 0
default-lease-duration = 0
tftp-host-name = " "
boot-file-path = " "
server-address = 0.0.0.0
static-address = [ { 0.0.0.0 00:00:00:00:00:00 } { 0.0.0.0 + }
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IP-Global

See Also: Active, Boot-File-Path, Default-Lease-Duration, Default-Max-Lease, Default-Pool, Lease-Duration, Server-Address, Static-Address, TFTP-Host-Name

Dialer-Type

Description: Specifies the type of redialer that the TAOS unit uses for incoming fax calls.

Usage: Specify one of the following settings:

- Mitel (the default) specifies the MITEL redialer.
- Atlas specifies the Atlas redialer.

Example: `set dialer-type = atlas`

Location: IP-Fax

See Also: IP-Fax-Enabled

Dial-Number

Description: Specifies the telephone number used to dial the connection.

Usage: Specify the telephone number or E.164 address of the remote station. You can enter up to 24 characters for a telephone number, and up to 15 digits of an E.164 address. The default is null.

Example: `set dial-number = 510-555-1212`

Dependencies: For a Frame Relay Switched Virtual Circuit (SVC), the combination of the Dial-Number and Subaddress values should be a unique value.

Location: Connection *station*

See Also: CalledNumber, Subaddress

Dialout-Allowed

Description: Specifies whether the connection can use the TAOS unit's digital modems to dial out.

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

- Yes specifies that the user can dial out on digital modems.
- No specifies that the user cannot dial out on digital modems.

Example: `set dialout-allowed = yes`

Location: Connection *station* > Telco-Options

See Also: Dialout-Configuration, LAN-Modem, Telco-Options

Dialout-Configuration

Description: A subprofile that contains configuration options for modem dial-out. If modem dial-out is enabled, local users can dial connections with the TAOS unit's digital modems. Each user can issue AT commands to the modem as if connected locally to the modem's asynchronous port.

Usage: With Terminal-Server as the working profile, list the Dialout-Configuration subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Dialout-Configuration subprofile:

```
admin> list dialout-configuration
[in TERMINAL-SERVER:dialout-configuration]
enabled = no
direct-access = yes
port-for-direct-access = 5000
security-for-direct-access = none
password-for-direct-access = mypassword
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server

See Also: Direct-Access, Enabled, Password-For-Direct-Access, Port-For-Direct-Access, Security-For-Direct-Access

Dialout-Poison

Description: Specifies whether the TAOS unit should stop advertising its IP dial-out routes (poison the routes) when no trunks are available.

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

- Yes specifies that the TAOS unit stops advertising its IP dial-out routes if no trunks are available.
- No specifies that the TAOS unit continues to advertise its dial-out routes, even if no trunks are currently available. No is the appropriate setting unless you have redundant TAOS units or don't use dial-out routes.

Example: `set dialout-poison = no`

Location: IP-Global

See Also: RIP-Policy

Dial-Query

Description: Specifies whether or not the TAOS unit brings up a connection when it receives a Service Advertising Protocol (SAP) query for service type 0x04 (File Server), and that service type is not present in the unit's SAP table.

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

- Yes specifies that the TAOS unit brings up a connection.
- No specifies that the TAOS unit does not bring up a connection.

Example: `set dial-query = yes`

Dependencies: Consider the following:

- If the TAOS unit has no SAP table entry for service type 0x04, it brings up every connection that has Dial-Query set to Yes. For example, if 20 Connection profiles specify that Dial-Query is set to Yes, the unit brings up all 20 connections in response to the query. However, if the TAOS unit has a static IPX route for even one remote server, it brings up that connection instead.
- If the TAOS unit does not route IPX for the connection, or if IPX routing is globally disabled, Dial-Query does not apply.

Location: Connection *station* > IPX-Options

See Also: IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Alias, Net-Number, Peer-Mode, RIP, SAP, SAP-Filter

Digital-Call-Routing-Sort-Method

Description: Specifies whether to use the old slot-first call-routing sort method or the new item-first sort method for digital calls.

The old sort-order processed the components of device addresses in the following order:

shelf slot item logical-item

The new sort-order processes device-address components in the following manner:

item shelf slot logical-item

For both types of sort methods, the shelf number is always 1.

Usage: Specify one of the following values:

- Slot-First (the default) specifies that the TAOS unit sorts by shelf and slot number, and then by item number. This setting improves system performance for Multilink Protocol (MP) and Multilink Protocol Plus (MP+) calls.
- Item-First specifies that the TAOS unit sorts by item number, then shelf, and then slot number. This setting distributes incoming calls evenly across multiple cards. Distributing calls across cards for bundled channels creates extra processing overhead.

Example: `set digital-call-routing-sort-method = item-first`

Location: System

See Also: Call-Route, Call-Route-Info, Call-Route-Type, Call-Routing-Sort-Method

Dirdo-Enabled

Description: Specifies whether the system generates a trap when a T-Online call comes in and no answer/subaddress has been received.

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

- Yes specifies that the system generates a trap.
- No specifies that the system does not generate a trap.

Example: `set dirdo-enabled = no`

Location: Trap *host-name*

See Also: T-Online

Direct

Description: Specifies whether PPP negotiation is initiated immediately after an interactive user enters the PPP command in the terminal-server interface.

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

- Yes enables direct PPP negotiation.
- No specifies that the terminal server waits to receive a PPP packet before beginning PPP negotiation.

Example: `set direct = no`

Dependencies: If terminal services are disabled, Direct does not apply.

Location: Terminal-Server > PPP-Mode-Configuration

See Also: PPP, PPP-Mode-Configuration

Direct-Access

Description: Enables or disables the direct-access dial-out feature.

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

- Yes specifies that a user can access a modem for direct-access dial-out service by initiating a Telnet session on the port specified by Port-For-Direct-Access.
- No disables the direct-access dial-out feature.

Example: `set direct-access = yes`

Dependencies: If terminal services are disabled, Direct-Access does not apply.

Location: Terminal-Server > Dialout-Configuration

See Also: Dialout-Configuration, Password-For-Direct-Access, Port-For-Direct-Access, Security-For-Direct-Access

Directed-Broadcast-Allowed

Description: Specifies whether the TAOS unit forwards directed broadcast traffic onto the interface and its network.

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

- Yes specifies that the TAOS unit forwards directed broadcast traffic onto the interface and its network.
- No specifies that the TAOS unit drops directed broadcast traffic that is not generated locally, preventing it from propagating onto intermediary networks.

Example: `set directed-broadcast-allowed = no`

Dependencies: To protect all of the LAN interfaces against Denial of Services (DoS) attacks that use directed broadcast traffic, you must set Directed-Broadcast-Allowed to No in all IP-Interface profiles.

Location: IP-Interface { {shelf-*N* slot-*N* *N*} *N*}

See Also: ICMP-Reply-Directed-Bcast

Disabled-Count

Description: Indicates the number of devices that are in the down state.

Usage: The Disabled-Count setting is read only.

Example: `disabled-count = 0`

Location: Device-Summary

See Also: Device-Class, Operational-Count, Total-Count

Disconnect-On-Auth-Timeout

Description: Instructs the TAOS unit to disconnect a PPP connection if it times out while waiting for Remote Authentication Dial-In User Service (RADIUS) authentication.

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

- Yes causes the TAOS unit to hang up a PPP connection upon a RADIUS timeout.
- No causes the TAOS unit to shut down cleanly after a RADIUS timeout.

Example: `set disconnect-on-auth-timeout = yes`

Location: Answer-Defaults > PPP-Answer

See Also: PPP, PPP-Answer

Divider

Description: Specifies the number by which the SCA internal clock speed (16.667 MHz) is divided in order to arrive at the internal clock speed on a Serial WAN (SWAN) line.

Usage: Specify a value from 1 to 256. The default is 1.

Example: `set divider = 5`

Dependencies: If Clock-Mode is set to External-Clock, Divider does not apply.

Location: SWAN {shelf-*N* slot-*N* *N*} > Line-Config > Clocking

See Also: Clock-Mode, Exp

DLCI

Description: Specifies 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: Specify an integer from 16 to 991. The default is 16. Ask your Frame Relay network administrator for the value you should enter.

Example: `set dlci = 17`

Dependencies: Consider the following:

- If FR-Direct-Enabled is set to Yes, DLCI does not apply.
- The T1 Frameline card supports a maximum of 240 active DLCIs.
- The Serial WAN (SWAN) card supports a maximum of 120 active DLCIs.
- The DLCI setting is ignored for a Connection profile that has Circuit-Type set to SVC. For an SVC, the DLCI value is assigned to the circuit by the network. The range of DLCI values for circuits is shared between PVCs and SVCs, and is managed between the network and user entities.

Location: Connection *station* > FR-Options

See Also: Circuit-Type, Encapsulation-Protocol, FR-Direct-Enabled, FR-Options

DNIS

Description: Specifies the Dialed Number Information Service (DNIS) value specified as the password in a RADIUS profile.

Usage: Specify up to 21 characters. The default is Ascend-DNIS.

Example: `set dnis = my_dnis`

Location: External-Auth > Password-Profile

See Also: CLID

DNS-List-Attempt

Description: Specifies whether the TAOS unit returns multiple addresses for a host when Domain Name System (DNS) responds with more than one address.

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

- Yes specifies that the TAOS unit returns the number of addresses it finds for the host, up to the limit specified by DNS-List-Size. The new addresses are stored in the DNS table in RAM, overwriting the configured addresses or the addresses received from earlier DNS queries. To prevent stale entries in the table in RAM, the system clears the number of addresses over the amount specified by DNS-List-Size.
- No specifies that the TAOS unit returns only one address from any successful DNS query. In the local DNS table in RAM, the returned address is stored and the remaining 34 addresses are cleared and set to null.

Example: An administrator configures 8 hostnames with null addresses and then sets Auto-Update to Yes. The DNS-Local-Table changes are propagated to RAM, and successful DNS queries to the specified hostnames will build the table with up to 14 addresses for each of the hosts.

```
admin> read ip-global
IP-GLOBAL read

admin> set dns-list-attempt = yes

admin> set dns-list-size = 14

admin> list dns-local-table
[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 } { " " +

admin> set enabled = yes

admin> set auto-update = yes

admin> list table-config
[in IP-GLOBAL:dns-local-table:table-config]
table-config[1] = { " " 0.0.0.0 }
table-config[2] = { " " 0.0.0.0 }
table-config[3] = { " " 0.0.0.0 }
table-config[4] = { " " 0.0.0.0 }
table-config[5] = { " " 0.0.0.0 }
table-config[6] = { " " 0.0.0.0 }
table-config[7] = { " " 0.0.0.0 }
table-config[8] = { " " 0.0.0.0 }

admin> set 1 host = mercury
admin> set 2 host = venus
admin> set 3 host = earth
admin> set 4 host = mars
admin> set 5 host = jupiter
admin> set 6 host = saturn
admin> set 7 host = uranus
```

```
admin> set 8 host = neptune
admin> write
IP-GLOBAL written
```

Dependencies: Consider the following:

- If Telnet and immediate Telnet are both disabled, DNS-List-Attempt does not apply.
- A TAOS unit operating as an L2TP Network Server (LNS) can use the Domain Name System (DNS) List feature to attempt to connect to a series of tunnel server endpoints if the first attempt fails. For the TAOS unit to use DNS List when attempting to bring up a tunnel, the client's Connection or Remote Authentication Dial-In User Service (RADIUS) profile must specify a DNS-resolvable hostname as the tunnel server endpoint.

Location: IP-Global

See Also: Auto-Update, DNS-List-Size, Host, Immediate-Mode-Options, TCP-Timeout

DNS-List-Size

Description: Specifies the maximum number of hosts listed in response to a Domain Name System (DNS) query. Users logging in through Telnet or immediate Telnet see a list containing up to the specified number of hosts. The DNS list can come from either a DNS server or a local DNS table.

Usage: Enter a number from 0 to 35. The default is 6.

Example: `set dns-list-size = 10`

Dependencies: A TAOS unit operating as an L2TP Network Server (LNS) can use the DNS List feature to attempt to connect to a series of server endpoints if the first attempt fails. For the TAOS unit to use DNS List when attempting to bring up a tunnel, the client's Connection or Remote Authentication Dial-In User Service (RADIUS) profile must specify a DNS-resolvable hostname as the tunnel endpoint.

Location: IP-Global

See Also: Auto-Update, DNS-List-Attempt

DNS-Local-Table

Description: A subprofile that enables you to configure a local Domain Name System (DNS) table of up to eight hostnames and their IP addresses. At system startup, the unit copies the values from the subprofile to the table in RAM. If you subsequently modify the DNS-Local-Table subprofile, the changes are propagated to the table in RAM when you Write the subprofile.

Note: The local DNS table has space for the number of addresses per hostname specified by the DNS-List-Size setting. However, the DNS-Local-Table subprofile allows only a single IP address per hostname.

Usage: With IP-Global as the working profile, list the DNS-Local-Table subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the DNS-Local-Table subprofile:

```
admin> list dns-local-table
[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 } +
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: Consider the following

- The local DNS table applies to all slot cards that support DNS.
- If you modify the DNS-Local-Table subprofile, assigning a single address to a host, the newly configured address is propagated to the table in RAM. The first address of the hostname entry is overwritten with the configured address, and all remaining addresses are cleared. If Auto-Update is set to Yes, the next successful DNS query overwrites the configured address and restores the multiple addresses (up to DNS-List-Size).

Location: IP-Global

See Also: Auto-Update, DNS-List-Size, Enabled, Table-Config N

DNS-Primary-Server

Description: Specifies the IP address of the primary Domain Name System (DNS) server for use on connected interfaces or for the Virtual Router (VRouter). If you do not configure client DNS, you can allow the TAOS unit to make your primary and secondary DNS servers available to both WAN users and users on connected networks.

Usage: Specify the IP address of a DNS server. The default is 0.0.0.0, which specifies that no local primary DNS server is available.

Example: `set dns-primary-server = 10.1.2.3/24`

Location: IP-Global, VRouter *name*

See Also: Allow-As-Client-DNS-Info, Client-DNS-Addr-Assign, Client-DNS-Primary-Addr, Client-DNS-Secondary-Addr, Client-Primary-DNS-Server, Client-Secondary-DNS-Server, DNS-Secondary-Server

DNS-Secondary-Server

Description: Specifies the IP address of the secondary Domain Name System (DNS) server for use on connected interfaces or for the Virtual Router (VRouter). The TAOS unit accesses the secondary server if the primary server is not available. If you do not configure client DNS, you can allow the unit to make your primary and secondary DNS servers available to both WAN users and users on connected networks.

Usage: Specify the IP address of the secondary DNS server. The default is 0.0.0.0, which indicates no secondary server.

Example: `set dns-secondary-server = 10.57.23.11/24`

Location: IP-Global, VRouter *name*

See Also: Allow-As-Client-DNS-Info, Client-DNS-Addr-Assign, Client-DNS-Primary-Addr, Client-DNS-Secondary-Addr, Client-Primary-DNS-Server, Client-Secondary-DNS-Server, DNS-Primary-Server

Domain-Name

Description: Specifies the domain name for Domain Name System (DNS) lookups.

Usage: Specify the local domain name. The default is null.

Example: `set domain-name = abc.com`

Location: IP-Global, VRouter *name*

See Also: DNS-Primary-Server, DNS-Secondary-Server

Down-Preference

Description: Specifies the preference for an inactive IP route. The TAOS unit uses this value to determine when to bring a route online.

When choosing which route to use, the router first compares the preference values, preferring the lower number. If the preference values are equal, the router compares the metric values, using the route with the lower metric.

Usage: Enter a number from 0 to 214748364. The lower the preference, the more likely the TAOS unit will bring the route online.

Example: `set down-preference = 255`

Location: Connection *station* > IP-Options

See Also: IP-Options, OSPF-ASE-Pref, OSPF-Pref, Preference, RIP-Pref, Static-Pref

DR-Capable

Description: Specifies whether the neighboring router can be the Designated Router (DR).

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

- Yes specifies that the neighboring router can be the DR.
- No specifies that the neighboring router cannot be the DR.

Example: `set dr-capable = yes`

Location: OSPF-NBMA-Neighbor *name*

See Also: Host-Name, IP-Address

Drop-Source-Routed-IP-Packets

Description: Specifies whether the TAOS unit forwards IP packets with the source-route option set.

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

- Yes specifies that the TAOS unit drops all packets that have a Loose or a Strict source route among their IP options.
- No specifies that the TAOS unit forwards all source-routed packets, as described in RFC 1812.

Example: `set drop-source-routed-ip-packets = no`

Location: IP-Global

See Also: IP-Global

DS2-State

Description: An array listing the state of each DS2 line in a DS3 line. The index to each array component is an integer from 1 to 7. Following are the possible values for DS2-State:

- Does-Not-Exist specifies that the line is not installed.
- Disabled specifies that the line is disabled.
- Loss-Of-Sync specifies that the line is in a red-alarm state.
- Yellow-Alarm specifies that a device on the DS2 stream is detecting certain framing errors in the signal.
- AIS-Receive specifies that the line is receiving a keepalive signal.
- Active specifies that multipoint service is established on the line.

Usage: Use the List command to display the array. You can then use the Set command to modify the settings. To close the array and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: `admin> list ds2-state`
`[in T3-STAT:ds2-state]`
`ds2-state[1] = idle`
`ds2-state[2] = idle`
`ds2-state[3] = dialing`
`...`

Location: T3-Stat {shelf-*N* slot-*N N*}

See Also: Line-State, Physical-Address

DS3-ATM

Description: Specifies the action to take when the code image for a DS3-ATM card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, Enet2, HDLC2, SWAN, T3, UDS3, UE1, Unknown-Cards, UT1

DS3-ATM (profile)

Description: A profile containing configuration settings for a DS3-ATM card.

Usage: To make DS3-ATM the working profile and list its contents, use the Read and List commands. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the DS3-ATM profile with the index { shelf-1 slot-1 0 } the working profile and list its contents:

```
admin> read ds3-atm { 1 1 0 }
DS3-ATM/{ shelf-1 slot-1 0 } read
admin> list
[in DS3-ATM/{ shelf-1 slot-1 0 }]
name = " "
physical-address* = { shelf-1 slot-1 0 }
enabled = no
line-config = { 9 0 static { shelf-1 slot-1 0 } no-loopback no +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
DS3-ATM/{ shelf-1 slot-1 0 } written
```

See Also: Enabled, Line-Config, Name, Physical-Address

DSP-DTMF-Input-Sample-Count

Description: Specifies the number of Goertzel input samples to compute in order to decode a Dual Tone Multifrequency (DTMF) digit.

Usage: Specify One-Sample or Two-Samples. The default is One-Sample. A setting of Two-Samples creates a more accurate result.

Example: `set dsp-dtmf-input-sample-count = two-samples`

Dependencies: You must set Signaling-Mode to Inband for DSP-DTMF-Input-Sample-Count to have any effect.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Collect-Incoming-Digits, Signaling-Mode

DSP-Portion

Description: A subprofile containing settings for the Domain-Specific Part (DSP) of an ATM End System Address (AESA). The DSP portion specifies the High-Order Domain-Specific Part (HO-DSP), End System Identifier (ESI), and Selector (SEL) subfields.

Usage: With ATM-Interface as the working profile, enter `list svc-options atm-address aesa-address dsp-portion`. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the DSP-Portion subprofile:

```
admin> list svc-options atm-address aesa-address dsp-portion
[ in ATM-INTERFACE/{ {any-shelf any-slot 0} 0 } :svc-options:atm+
ho-dsp = " "
esi = " "
sel = "
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: ATM-Interface {{shelf-*N* slot-*N* *N*} *N*} > SVC-Options > ATM-Address > AESA-Address,
Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr > AESA-Address,
Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr > AESA-Address

See Also: ESI, HO-DSP, IDP-Portion, SEL

Dst-Port-Cmp

Description: Specifies the type of comparison to use when comparing the Dest-Port value to the destination port in a packet.

Usage: Specify one of the following values:

- None (the default) specifies that the TAOS unit does not compare the packet's destination port number to the Dest-Port value.
- Less specifies that port numbers with a value less than the value specified by Dest-Port match the filter.
- Eql specifies that port numbers equal to the value specified by Dest-Port match the filter.
- Gtr specifies that port numbers with a value greater than the value specified by Dest-Port match the filter.
- Neq specifies that port numbers not equal to the Dest-Port value match the filter.

Example: `set dst-port-cmp = less`

Dependencies: For Dst-Port-Cmp to apply, you must set Type to IP-Filter or TOS-Filter. In addition, only TCP and UDP packets contain destination ports.

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter, Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter

See Also: Input-Filters, IP-Filter, Output-Filters, Type

Dst-Socket-Cmp

Description: Specifies the type of comparison to use when comparing the Dest-Socket value to the destination socket in a packet.

Usage: Specify one of the following values:

- None (the default) specifies that the TAOS unit does not compare the packet's destination socket number to the Dest-Socket value.
- Less specifies that socket numbers with a value less than the Dest-Socket value match the filter.
- Eql specifies that socket numbers equal to the Dest-Socket value match the filter.
- Gtr specifies that socket numbers with a value greater than the value specified by Dest-Socket match the filter.
- Neq specifies that socket numbers not equal to the value specified by Dest-Socket match the filter.

Example: `set dst-socket-cmp = less`

Dependencies: For Dst-Socket-Cmp to apply, you must set Type to IPX-Filter.

Location: Filter *filter-name* > Input-Filters > IPX-Filter,
Filter *filter-name* > Output-Filters > IPX-Filter

See Also: Input-Filters, IPX-Filter, Output-Filters, Type

DSX-Line-Length

Description: Specifies the length (in feet) of the physical T1 (DSX) line.

Usage: The value you specify should reflect the longest line length you expect to encounter in your installation. Specify one of the following values:

- 1-133 (the default)
- 134-266
- 267-399
- 400-533
- 534-655

Example: `set dsx-line-length = 133`

Dependencies: If the TAOS unit has an internal Channel Service Unit (CSU) at the interface to the line, DSX-Line-Length does not apply.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Front-End-Type, Line-Interface

DTMF-Tone-Passing

Description: Specifies whether the TAOS unit filters Dual Tone Multifrequency (DTMF) tones from the voice path and passes the corresponding digits to the remote gateway by means of a path that does not use Real-Time Transport Protocol (RTP).

Usage: Specify one of the following values:

- DTMF-Tone-Passed-Inband (the default) specifies that the local TAOS unit passes Public Switched Telephone Network (PSTN)-generated DTMF digits and tones as part of the voice processing stream. These tones are compressed by the selected audio codec and transported across the IP network by means of UDP packets.
- DTMF-Tone-Passed-Outofband specifies that the local TAOS unit passes PSTN-generated DTMF digits and tones across the network by means of non-UDP packets. Once received at the remote end, the digits are played out to the local PSTN.

Example: `set dtmf-tone-passing = outofband`

Dependencies: Changes to DTMF-Tone-Passing are effective with the next Voice over IP (VoIP) call.

Location: VoIP {*x* *y*}

See Also: True-Connect-Enable

Duplex-Mode

Description: Specifies whether the physical Ethernet interface of the 100BaseT port on the Ethernet-2 card uses full-duplex or half-duplex mode.

Usage: Specify one of the following settings:

- Full-Duplex (the default) provides increased throughput.
- Half-Duplex enables operation with older equipment that does not support full-duplex mode.

Example: `set duplex-mode=half`

Dependencies: When the unit uses the Ethernet-2 card to support Voice over IP (VoIP) call processing, the card must operate in full-duplex mode.

Location: Ethernet {shelf-*N* slot-*N* *N*}

See Also: Ether-IF-Type, Enabled, Filter-Name, Interface-Address, Link-State-Enabled

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 TAOS 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: Specify one of the following values:

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

Example: `set dynamic-algorithm = quadratic`

Location: Answer-Defaults > MPP-Answer, Connection *station* > MPP-Options

See Also: Add-Persistence, Bandwidth-Monitor-Direction, Base-Channel-Count, Decrement-Channel-Count, Increment-Channel-Count, Maximum-Channels, Minimum-Channels, MPP-Answer, MPP-Options, Seconds-History, Sub-Persistence, Target-Utilization

E

E1

Description: A profile that contains configuration settings for an E1 line and its channels.

Usage: Use the Read and List commands to make E1 the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the List command, followed by a space and two periods.

Example: To make the E1 profile with the index { shelf-1 slot-8 2 } the working profile and list its contents:

```
admin> read e1 {1 8 2}
E1/{ shelf-1 slot-8 2 } read

admin> list
[in E1/{ shelf-1 slot-8 2 }]
name = trunk-1
physical-address* = { shelf-1 slot-8 2 }
line-interface = { no g703 eligible middle-priority isdn +
back-to-back = false
t302-timer = 6000
t-online-type = te
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
E1/{ shelf-1 slot-8 2 } written
```

See Also: Back-To-Back, Line-Interface, Name, Physical-Address, T302-Timer, T-Online

E3-ATM

Description: A profile containing configuration settings for an E3-ATM card.

Usage: To make E3-ATM the working profile and list its contents, use the Read and List commands. For example:

```
admin> read e3-atm { 1 1 0 }
E3-ATM/{ shelf-1 slot-1 0 } read

admin> list
[in E3-ATM/{ shelf-1 slot-1 0 }]
name = ""
physical-address* = { shelf-1 slot-1 0 }
enabled = no
line-config = { 9 1 { any-shelf any-slot 0 } no-loopback no g751-adm +
```

You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command. For example:

```
admin> write
E3-ATM/{ shelf-1 slot-1 0 } written
```

See Also: Enabled, Line-Config, Name, Physical-Address

E164-Native-Address

Description: Specifies the Switched Virtual Circuit (SVC) address.

Usage: Specify an E.164 address. You can specify up to 30 characters. The default is null.

Example: `set e164-native-address = 5085552600`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options > ATM-Address,
Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr,
Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr

See Also: Numbering-Plan, SVC-Address-Info

E1-Inter-Digit-Timeout

Description: Specifies the number of milliseconds the E1 Digital Signal Processor (DSP) waits between digits before considering Dialed Number Information Service/Automatic Number Identification (DNIS/ANI) collection complete.

Usage: Specify a number from 100 to 6000 milliseconds. For backward compatibility, the default is 3 seconds. The setting takes effect with the next incoming call. Specifying a lower value improves call setup times, which are especially important for Voice over IP (VoIP) calls with single-stage-dial.

Example: `set e1-inter-digit-timeout = 2000`

Dependencies: E1-Inter-Digit-Timeout does not apply unless Collect-Incoming-Digits is set to Yes.

Location: E1 {shelf-*N* slot-*N* *N* } > Line-Interface

See Also: Collect-Incoming-Digits

Early-Ringback-Enable

Description: Enables or disables generation of an early ringback tone on networks experiencing long call setup times.

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

- Yes specifies that the local gateway plays a ringback tone to the caller as soon as a connection is established with the remote gateway.
- No disables generation of an early ringback tone.

Example: `set early-ringback-enable = yes`

Dependencies: For certain Voice over IP (VoIP) network configurations, such as satellite IP networks, wireless networks, or networks using channel-associated signaling (CAS) trunks, call setup times can be quite long. Callers might hang up before the call completes because they hear no call progress tones until Real-Time Transport Protocol (RTP) carries ringback from the remote Public Switched Telephone Network (PSTN). Early ringback allows the TAOS unit to generate a ringback tone locally, as soon as the call is started on the remote gateway. Early ringback is intended for use only on networks that experience long call setup times. Its use for other network configurations is not recommended, and might result in erroneous ring-to-busy and ring-to-failure announcements.

Location: VoIP {x y}

See Also: Voice-Ann-Dir

ECM-Enable

Description: Enables or disables Error Correction Mode (ECM) for real-time fax calls. ECM frames are relayed end to end between terminals.

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

- Yes specifies that fax frames can be retransmitted in the event that a frame is not received correctly.
- No disables ECM. Fax frames containing errors are not corrected.

Example: `set ecm-enable = no`

Dependencies: For ECM-Enable to apply, you must set RT-Fax-Enable to Yes.

Location: VoIP {x y} > RT-Fax-Options

See Also: Command-Spoof, Local-Retransmit-LSF, Low-Latency-Mode, RT-Fax-Enable

Ena-Adap-Jitter-Buffer

Description: Specifies whether the jitter buffer mode is adaptive for Voice over IP (VoIP) calls.

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

- Yes specifies that the jitter buffer can range in size between the values set for Max-Jitter-Buffer-Size and one packet, depending on the number of late or out-of-sequence packets received during the call.
- No specifies that static jitter buffers will be used for processing VoIP calls.

Example: `set ena-adap-jitter-buffer = no`

Dependencies: Consider the following:

- Changes to the Ena-Adap-Jitter-Buffer value become effective with the next VoIP call.
- When Silence-Det-Cng is set to Yes, MultiVoice uses the value assigned to Initial-Jitter-Buffer-Size to open static call jitter buffers.
- When Ena-Adap-Jitter-Buffer is set to No, MultiVoice uses the value assigned to Initial-Jitter-Buffer-Size to open static call jitter buffers.
- When a G.723 codec is selected for Packet-Audio-Mode, Max-Jitter-Buffer-Size cannot exceed nine packets.

Location: VoIP {x y}

See Also: Initial-Jitter-Buffer-Size, Max-Jitter-Buffer-Size, Silence-Det-Cng

Enable

Description: Starts or stops Open Shortest Path First (OSPF) operation.

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

- Yes globally enables OSPF.
- No globally disables OSPF.

Example: `set enable = no`

Dependencies: 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.

Location: IP-Global > OSPF-Global

See Also: OSPF, OSPF-Enabled

Enabled

Description: Enables or disables a feature, interface, or line.

Usage: Specify Yes or No. The default for the Ethernet profile is Yes. The default for other profiles is No.

- Yes enables a feature, interface, or line.
- No disables a feature, interface, or line. If Enabled is set to No in the Ethernet profile, packets routed to and received by the interface are discarded.

Example: `set enabled = yes`

Dependencies: Consider the following:

- 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 if 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 TAOS unit attempts to resolve the query by using the host-to-address mappings 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.
- In the SS7-Gateway profile, if you set Enabled=Yes, the interface is enabled only if the Primary-IP-Address and Primary-TCP-Port values are valid. Changing the setting from Yes to No closes the signaling links but does not disconnect active Signaling System 7 (SS7) calls.
- In the Transaction-Server profile, the Enabled setting is read only and specifies whether the SDTN license is enabled.

Location: Answer-Defaults, ATM-Interface { {shelf-*N* slot-*N* *N*}*N* }, Call-Switching, Connection *station*, DS3-ATM {shelf-*N* slot-*N* *N*}, E1 {shelf-*N* slot-*N* *N*}, E3-ATM {shelf-*N* slot-*N* *N*}, Ethernet {shelf-*N* slot-*N* *N*}, Frame-Relay *fr-name*, IP-Global, OC3-ATM {shelf-*N* slot-*N* *N*}, Private-Route-Table *name*, SNMP, SS7-Gateway, Stacking *name*, SWAN {shelf-*N* slot-*N* *N*}, T1 {shelf-*N* slot-*N* *N*}, T3 {shelf-*N* slot-*N* *N*}, Terminal-Server, Transaction-Server, Tunnel-Server *name*

See Also: Answer-Defaults, Connection, DNS-Local-Table, E1, Ethernet, IP-Global, SNMP, SWAN (profile), T1, T3 (profile), Terminal-Server, Transaction-Server

Enable-Permit

Description: Enables or disables control over Telnet access to the unit on the basis of the Permit-List settings in the TACL profile.

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

- Yes specifies that the IP addresses specified in one or more Permit-Lists are allowed to use Telnet to gain access to the unit.
- No specifies that no devices are permitted Telnet access to the unit.

Example: `enable-permit = yes`

Location: TACL

See Also: Permit-List

Encap-Mode

Description: Specifies the encapsulation mode in which IP Security (IPSec) operates.

Usage: Specify one of the following values:

- Transport specifies transport mode (the default). Transport mode is the more efficient encapsulation mode.
- Tunnel specifies that the data stream is tunneled using IP-in-IP encapsulation. Tunnel mode is required if the IPSec endpoint addresses differ from the TCP endpoint addresses for TCP-Clear sessions.
- Optimized specifies that the system uses transport mode if possible, and tunnel mode only when required for a particular connection.

Example: `set encap-mode = tunnel`

Location: IPSec *name*

See Also: Active, Name, Recv-AH, Recv-ESP, Send-AH, Send-ESP, Tunnel-Address

Encapsulation-Protocol

Description: Specifies the encapsulation method to use for the connection. Both sides of the connection must support the specified encapsulation method. Usually, encapsulation protocols have their own configuration options within the subprofile of a Connection profile.

Usage: Specify one of the following values:

- PPP for single-channel PPP connections.
- MP (Multilink Protocol, as specified in RFC 1990) for multichannel connections with MP-compliant devices from other vendors.
- MPP (Multilink Protocol Plus) for multichannel connections with other TAOS units. This value is the default.
- Frame-Relay for Frame Relay configurations.
- Frame-Relay-Circuit for Frame Relay switch configurations.
- TCP-Raw (unencapsulated TCP) for use with a proprietary encapsulation method.
- DTPT for T-Online.
- ARA (AppleTalk Remote Access) for AppleTalk connections.
- SLIP for an asynchronous Serial Line Internet Protocol (SLIP) connection.
- CSLIP for a Compressed SLIP connection that uses VJ header compression.
- ATM for an Asynchronous Transfer Mode (ATM) connection.
- ATM-Frame-Relay-Circuit for an ATM-to-Frame Relay link.
- HDLC-NRM for a High-Level Data Link Control-Normal Response Mode (HDLC-NRM) link.
- Visa2 for a Visa terminal connection.

Example: `set encapsulation-protocol = ppp`

Dependencies: You must set Encapsulation-Protocol to Frame-Relay for Frame Relay Switched Virtual Circuit (SVC) connections, and to ATM for ATM SVC connections. Setting Encapsulation-Protocol to ATM suggests that IP-over-ATM is used on the Virtual Circuit (VC).

Location: Connection *station*

See Also: FR-Options, HDLC-NRM-Options, MP-Options, MPP-Options, PPP-Options, TCP-Clear-Options, Visa2-Options

Encoding

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

Usage: Specify one of the following values:

- AMI (the default) specifies Alternate Mark Inversion encoding.
- B8ZS specifies Bipolar encoding with 8-Zero Substitution. B8ZS is often required for ISDN lines (for which Signaling-Mode is set to ISDN).
- None specifies encoding identical to AMI, but without density enforcement.

Example: `set encoding = ami`

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface, Signaling-Mode

End-Of-Packet-Pattern

Description: Defines a character pattern that signals the end of a packet. When the pattern matches the buffered data, the system immediately flushes the buffer by writing all data, up to and including the pattern, into TCP packets.

Usage: Specify up to 64 characters. The default is null. You can enter both ASCII characters and binary data, using the backslash (\) as an escape mechanism. Consider the following:

- To insert a literal backslash in the pattern, enter two backslash characters (\\).
- To insert a 1- to 3-digit octal number, use a single backslash. (To avoid confusion between the literal ASCII characters 1 through 7 and an octal value, you can pad the octal value with leading zeroes.)
- To insert a 1- or 2-digit hexadecimal number in the pattern, precede the number with the pattern \x.

Following are other special escape sequences:

Escape Sequence	Description	Value
\a	Alarm	7
\b	Backspace	8
\f	Form feed	12
\n	New line	10
\r	Carriage return	13
\t	Tab	9
\v	Vertical tab	11
\\	Backslash	92
\'	Apostrophe	44
\"	Double Quote	34
\?	Wildcard	Matches any single character

Example: The pattern \015 represents a carriage return (octal 15). The pattern \x0D also represents a carriage return (hex 0D).

Dependencies: If Detect-End-Of-Packet is set to No, End-Of-Packet-Pattern does not apply.

Location: Answer-Defaults > TCP-Clear-Answer, Connection *station* > TCP-Clear-Options

See Also: Detect-End-Of-Packet, Enabled, Flush-Length, Flush-Time

Enet2

Description: Specifies the action to take when the code image for an Ethernet-2 card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, HDLC2, SWAN, T3, UDS3, UE1, Unknown-Cards, UT1

Enforce-Address-Security

Description: Specifies whether the TAOS unit should validate the IP address of a Simple Network Management Protocol (SNMP) manager attempting to access the unit. If address security is not enforced, any SNMP manager who presents the appropriate community name is allowed in.

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

- Yes specifies that, before allowing access, the TAOS unit compares the source IP address of an SNMP manager to the host addresses specified by Read-Access-Hosts and Write-Access-Hosts.
- No specifies that the TAOS unit does not compare IP addresses, but uses only the community name to validate SNMP access.

Example: `set enforce-address-security = yes`

Dependencies: Read-Access-Hosts and Write-Access-Hosts do not restrict access unless Enforce-Address-Security is set to Yes.

Location: SNMP

See Also: Read-Access-Hosts, Write-Access-Hosts

Entry-Number

Description: Specifies an entry number in the call-routing database. The TAOS unit uses the entry number to discriminate among multiple entries for the same device.

Usage: Specify a number greater than 0 (zero). Entry numbers do not have to be sequential, as long as they are unique.

Example: `set index entry-number = 1`

Location: Call-Route { { {shelf-*N* slot-*N* *N*} *N*} *N*}

See Also: Index

Error

Description: A read-only profile that provides information about any errors that occur when the TAOS unit is running.

Usage: Use the Read and List commands to make Error the working profile and list its contents.

Example: `admin> read error 1`
ERROR/1 read

`admin> list`
[in ERROR/1]
is-post = no
type = 100
slot = 17
version = 2.1a0e0
user-profile = ""
ip-address = 0.0.0.0
stack-trace = [0 0 0 0 0 0]
loadname = tntsr
index* = 1
shelf = 1

See Also: Index, IP-Address, IS-Post, Loadname, Shelf, Slot, Stack-Trace, Type, User-Profile, Version

Error-Count

Description: Indicates the number of errors experienced, since the last reset, by a T1 line or a Serial WAN (SWAN) line. For a T1 line, the value is an array that indicates errors for each channel of the line.

Usage: For a T1 line, use the List command to display an array of values indicating the number of errors for each channel. For a SWAN line, use the List command to display the number of errors.

Example: To display an array of values indicating the number of errors for each channel of a T1 line:

```
admin> list error-count
[in T1-STAT/{ shelf-1 slot-1 1 }:error-count]
error-count[1] = 0
error-count[2] = 0
error-count[3] = 0
error-count[4] = 0
...
```

Location: SWAN-Stat {shelf-*N* slot-*N* *N*}, T1-Stat {shelf-*N* slot-*N* *N*}

See Also: SWAN-Stat, T1-Stat

ESI

Description: Specifies a hexadecimal number that uniquely identifies the End System Identifier (ESI) field of the Domain-Specific Part (DSP) of an ATM End System Address (AESA). ESI indicates the end system within the specified subnetwork, typically an IEEE Media Access Control (MAC) address.

Usage: Specify a value 6 bytes long (12 hexadecimal digits). The default is null.

Example: `set esi = 010203040506`

Location: ATM-Interface {{shelf-*N* slot-*N* *N*} *N*} > SVC-Options > ATM-Address > AESA-Address > DSP-Portion,
 Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr > AESA-Address > DSP-Portion,
 Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr > AESA-Address > DSP-Portion

See Also: HO-DSP, SEL

ESP-Type

Description: Specifies the type of Encapsulating Security Payload (ESP) transform to use to encrypt the data portion of IP packets.

Usage: Specify one of the following values:

- None (the default) specifies that encryption is not in use.
- DES-CBC specifies DES-CBC mode as described in RFC 1829 concerning the US Data Encryption Standard cipher block chaining algorithm.
- 3DES-CBC specifies 3DES-CBC mode as described in RFC 1851 concerning the Triple DES-CBC algorithm.
- 40DES-CBC specifies DES-CBC mode, restricted to 40 bits.

Example: `set esp-type = descbc`

Location: IPsec *name* > Recv-ESP, IPsec *name* > Send-ESP

See Also: Active, AH-Type, Auth-Key, Auth-Type, IV-Len, Key, Key2, Key3, Replay-Protection, SPI, Version

Ether-IF-Type

Description: Indicates the type of physical Ethernet interface in use.

Usage: The Ether-IF-Type setting is read only. It can have one of the following values:

- UTP indicates unshielded twisted pair (thin Ethernet) as specified in IEEE 802.3 (10BaseT) Ethernet.
- AUI (Auxiliary Unit Interface) indicates a thick Ethernet transceiver as specified in IEEE 802.3 (10Base5) Ethernet.
- Coax indicates coaxial cable.

Location: Ethernet {shelf-*N* slot-*N* *N*}

See Also: Enabled, Filter-Name, Interface-Address, Link-State, Link-State-Enabled, MAC-Address

Ether-Info

Description: A profile that specifies the Media Access Control (MAC) address and link state of an Ethernet interface. The Ether-Info profile is created when the installed Ethernet card enters an active state, and deleted when the slot is brought down. The contents of the profile are not written to NVRAM.

Usage: Use the Read and List commands to make Ether-Info the working profile and list its contents.

Example: To make the Ether-Info profile with the index { shelf-1 slot-2 1 } the working profile and list its contents:

```
admin> read ether-info { 1 2 1 }
ETHER-INFO/{ shelf-1 slot-2 1 } read
admin> list
[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
```

Dependencies: The Ether-Info profile is read only.

See Also: Interface-Address, Link-State, MAC-Address

Description: A profile that defines the physical components of a system Ethernet interface.

Usage: To make Ethernet the working profile and list its contents, enter the Read and List commands. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: On a MAX TNT unit:

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

admin> list
[in ETHERNET/{ shelf-1 controller 1 }]
interface-address* = { shelf-1 controller 1 }
ether-if-type = utp
filter-name = ""
enabled = yes
link-state-enabled = no
duplex-mode = full-duplex
media-speed-mbit = 100mb

admin> set filter-name = filter1

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

On an APX 8000 unit:

```
admin> read ethernet {1 first 1}
ETHERNET/{ shelf-1 left-controller 1 } read

admin> list
[in ETHERNET/{ shelf-1 left-controller 1 }]
interface-address* = { shelf-1 left-controller 1 }
ether-if-type = utp
filter-name = ""
enabled = yes
link-state-enabled = no
duplex-mode = full-duplex
media-speed-mbit = 100mb

admin> set filter-name = filter1

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

See Also: Duplex-Mode, Ether-IF-Type, Enabled, Filter-Name, Interface-Address, Link-State-Enabled, Media-Speed-Mbit

Ethernet-Address

Description: Specifies the Media Access Control (MAC) address of the host to which the associated IP address is assigned.

Usage: Specify a physical address. The default is 00:00:00:00:00:00.

Example: `set ethernet-address = 00009459A653`

Location: IP-Global > DHCP-Server > Static-Address

See Also: IP-Address

Event-Overwrite-Enabled

Description: Specifies whether the system generates a trap when a new event has overwritten an unread event. Once the trap has been sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events have occurred.

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

- Yes specifies that the system generates a trap when a new event has overwritten an unread event.
- 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 *host-name*

See Also: RADIUS-Change-Enabled

Exclusive-Port-Routing

Description: Enables or disables exclusive port routing. Exclusive port routing is a way to prevent the TAOS unit from accepting calls for which it has no explicit routing destination.

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

- Yes specifies that the TAOS unit drops calls for which it has no explicit call-routing information.
- No specifies that the TAOS unit uses service-based routing to route voice calls to a digital modem and data calls to its router software.

Example: `set exclusive-port-routing = yes`

Location: System

See Also: Parallel-Dialing

Exp

Description: Specifies the exponent used to calculate the internal clock speed on a Serial WAN (SWAN) line.

Usage: Specify a value from 0 to 9. The default is 2.

Example: `set exp = 5`

Dependencies: Exp does not apply if Clock-Mode is set to External-Clock.

Location: SWAN {shelf-*N* slot-*N* *N*} > Line-Config > Clocking

See Also: Clock-Mode, Divider

Expect-Callback

Description: Specifies whether the TAOS unit expects outgoing calls to result in a call back from the remote device.

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

- Yes specifies that the TAOS unit expects the remote device to hang up and call back. Use this setting if Ping or Telnet is in use and the TAOS unit cannot dial back to the calling device.
- No specifies that the TAOS unit does not expect callback.

Example: `set expect-callback = yes`

Location: Connection *station* > Telco-Options

See Also: Callback

External-Auth

Description: A profile containing configuration options for Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control (TACACS), and Terminal Access Controller Access Control Plus (TACACS+).

Usage: Use the Read and List commands to make External-Auth the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the External-Auth profile the working profile and list its contents:

```
admin> read external-auth
EXTERNAL-AUTH read
admin> list
[in EXTERNAL-AUTH]
auth-type = radius
acct-type = none
rad-serv-enable = no
rad-auth-client = { 200.168.6.153 0.0.0.0 0.0.0.0 1645 0 +
rad-acct-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 " 0 0 +
rad-auth-server = { 0 no rad-serv-attr-any [ 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 " " }
tacplus-acct-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 " " }
password-profile = {***** *****}
rad-id-space = unified
local-profiles-first = lpf=yes
noattr6-use-termsrv = yes

```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```

admin> write
EXTERNAL-AUTH written

```

See Also: Acct-Type, Auth-Type, Local-Profiles-First, NoAttr6-Use-Termsrv, Password-Profile, Rad-Acct-Client, Rad-Auth-Client, Rad-Auth-Server, Rad-Serv-Enable, Tac-Auth-Client, TacPlus-Acct-Client, TacPlus-Auth-Client

Ext-Tsrv

Description: A read-only profile that stores banner and hosts information loaded from Remote Authentication Dial-In User Service (RADIUS).

Usage: Use the Read and List commands to make Ext-Tsrv the working profile and list its contents. The Refresh -t command requests initial-banner and banner/hosts information from RADIUS as two separate requests, which independently update the Ext-Tsrv profile. If the information changes the profile contents, the system notifies the slot cards and they update their information.

Example: admin> **read ext-tsrv**

```
EXT-TSRV read
```

```

admin> list init-banner
[in EXT-TSRV:init-banner]
init-banner[1] = " "
init-banner[2] = " "
init-banner[3] = " "
init-banner[4] = " "
init-banner[5] = " "
init-banner[6] = " "
init-banner[7] = " "
init-banner[8] = " "
init-banner[9] = " "
init-banner[10] = " "
init-banner[11] = " "
init-banner[12] = " "
init-banner[13] = " "
init-banner[14] = " "
init-banner[15] = " "
init-banner[16] = " "

```

```
admin> list banner
[in EXT-TSRV:banner]
banner[1] = " "
banner[2] = " "
banner[3] = " "
banner[4] = " "
banner[5] = " "
banner[6] = " "
banner[7] = " "
banner[8] = " "
banner[9] = " "
banner[10] = " "
banner[11] = " "
banner[12] = " "
banner[13] = " "
banner[14] = " "
banner[15] = " "
banner[16] = " "

admin> list hosts-info
[in EXT-TSRV:hosts-info]
hosts-info[1] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[2] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[3] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[4] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[5] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[6] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[7] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[8] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[9] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[10] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[11] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[12] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[13] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[14] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[15] = { 0.0.0.0 " " 0 telnet " " }
hosts-info[16] = { 0.0.0.0 " " 0 telnet " " }
```

See Also: Banner, Hosts-Info N, Init-Banner N

F

Facility

Description: Specifies the Syslog daemon facility code for messages logged from the TAOS unit. For detailed information, see the `syslog.conf` manual page entry on the UNIX Syslog server.

Usage: Specify one of the following values:

- Local0 (the default)
- Local1
- Local2
- Local3
- Local4
- Local5
- Local6
- Local7

Example: `set facility = local0`

Dependencies: Consider the following:

- If Syslog is not enabled, Facility does not apply.
- In the Log profile, the Facility value applies to the first data stream.
- In the Auxiliary-Syslog [1] subprofile, the Facility value applies to the second data stream.
- In the Auxiliary-Syslog [2] subprofile, the Facility value applies to the third data stream.
- The settings in the Auxiliary-Syslog subprofile affect an individual Syslog stream, and override the values specified in the Log profile.

Location: Log, Log > Auxiliary-Syslog

See Also: Host, Syslog-Enabled

Fan

Description: Specifies the serial number associated with the redundant controller.

Usage: The Fan setting is read only.

Example: `fan = 317873482`

Location: Redundancy-Stats > Context-Stats > Context-Stats *N*

Fantray-Lownoise-RPM

Description: Specifies the RPM of the fantray when the low noise speed has been selected.

Usage: Specify a number from 2000 to 3000. The default is 2500.

Example: `set fantray-lownoise-rpm = 2000`

Location: Thermal

See Also: Operation-Mode

Far-End-Number

Description: Specifies the telephone number of the remote device.

Usage: Specify a text string of up to 40 characters. The default is 0 (zero), which indicates a default profile for either the system or a particular gateway.

Example: `set far-end-number = 15105551212`

Location: VoIP {x y} > VoIP-Index

See Also: Gateway-Access-Number

Fax-DID

Description: An array listing up to eight Direct Inward Dialing (DID) numbers. The TAOS unit compares the DID number supplied by the PRI setup message of an incoming call to the configured numbers. If the match is not exact, the unit does not start IP fax.

Usage: With IP-Fax as the working profile, use the List command to display the array. To close the array and return to a higher context in the profile, enter the List command, followed by a space and two periods.

Example: `admin> list fax-did`
[in IP-FAX]
fax-did[1] = 7470000
fax-did[2] = 7471111
fax-did[3] = " "
fax-did[4] = " "
fax-did[5] = " "
fax-did[6] = " "
fax-did[7] = " "
fax-did[8] = " "

Location: IP-Fax

See Also: Fax-DNIS

Fax-DNIS

Description: An array listing up to eight Dialed Number Information Service (DNIS) numbers. The TAOS unit compares the DNIS number supplied by the PRI setup message of an incoming call to the configured numbers. If the match is not exact, the unit does not start IP fax.

Usage: With IP-Fax as the working profile, use the List command to display the array. To close the array and return to a higher context in the profile, enter the List command, followed by a space and two periods.

Example: admin> **list fax-dnis**

```
[in IP-FAX]
fax-dnis[1] = 8057
fax-dnis[2] = 8054
fax-dnis[3] = " "
fax-dnis[4] = " "
fax-dnis[5] = " "
fax-dnis[6] = " "
fax-dnis[7] = " "
fax-dnis[8] = " "
```

Location: IP-Fax

See Also: Fax-DID

Fax-Incoming-Call-Type

Description: Specifies the type of fax calls that the unit accepts.

Usage: Specify one of the following values:

- Redialer (the default) specifies that all fax calls are redialer calls.
- DID specifies that the unit authenticates calls on the basis of Direct Inward Dialing (DID) numbers.

Example: **set fax-incoming-call-type = did**

Dependencies: A TAOS unit authenticates a call on the basis of the values specified by the All-Calls-Are-Fax and Fax-Incoming-Call-Type parameters as follows:

All-Calls-Are-Fax	Fax-Incoming-Call-Type	TAOS unit behavior
Yes	Redialer	Receives all incoming calls as redialer-type fax calls.
Yes	DID	Treats all incoming calls as DID-type fax calls.
No	DID	Authenticates the call against the DID numbers in the Fax-DID array.
No	Redialer	Authenticates the call against the DNIS numbers in the Fax-DNIS array.

Location: IP-Fax

See Also: All-Calls-Are-Fax

Fax-Servers

Description: An array listing the IP addresses of up to five fax servers.

Usage: With IP-Fax as the working profile, use the List command to display the array. To close the array and return to a higher context in the profile, enter the List command, followed by a space and two periods.

Example: admin> **list fax-servers**
[in IP-FAX]
fax-servers[1] = 1.2.3.4
fax-servers[2] = 5.6.7.8
fax-servers[3] = 0.0.0.0
fax-servers[4] = 0.0.0.0
fax-servers[5] = 0.0.0.0

Location: IP-Fax

See Also: Fax-DNIS

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 devices.

Usage: Specify one of the following values:

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

Example: **set fdl = at&t**

Dependencies: FDL does not apply to D4-framed T1 lines. However, even if you do not choose an FDL protocol, the TAOS unit accumulates D4 and ESF performance statistics in the FDL Stats windows.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Frame-Type, Line-Interface

Fgd-Signaling-Enabled

Description: Indicates whether Feature Group D (FGD) signaling is enabled on a MultiVoice gateway.

Usage: The Fgd-Signaling-Enabled parameter is read only. Yes indicates that FGD signaling is enabled. No indicates that FGD signaling is disabled.

Example: fgd-signaling-enabled = yes

Location: Base

Filter

Description: A profile that specifies filter rules for an interface.

When you apply a filter to an interface, the TAOS unit monitors the data stream and takes a specified action when packet contents match the filter rules. Depending on how you define the filter, it might apply to incoming packets, outgoing packets, or both. You can apply the specified action (forward or drop) to all packets that match the rules, or to all packets *except* those that match the rules.

Usage: Use the New and List commands to create a new filter and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To create a new filter called `test-name`:

```
admin> new filter test-name
FILTER/test-name read

admin> list
[in FILTER/test-name (new)]
filter-name* = test-name
input-filters = [ { no no generic-filter { 0 0 no no +
output-filters = [ { no no generic-filter { 0 0 no no +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
FILTER/test-name written
```

See Also: Call-Filter, Data-Filter, Filter-Name, Filter-Persistence, Input-Filters, Output-Filters

Filter-Name

Description: Specifies the name of a Filter profile. In a Filter profile, the name you assign becomes the Filter profile's index. In an Ethernet profile, the name specifies the data filter that the TAOS unit applies to the Ethernet interface.

Usage: Specify a filter name of up to 16 characters. The default is null.

Example: `set filter-name = ip-spoof`

Location: Ethernet {shelf-*N* slot-*NN*}, Filter *filter-name*

See Also: Call-Filter, Data-Filter, Filter-Persistence

Filter-Persistence

Description: Specifies whether filters persist across state changes. A state change occurs when a connection temporarily goes down because of inactivity on the line.

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

- Yes specifies that filters persist across state changes.
- No specifies that filters do not persist across state changes.

Example: `set filter-persistence = yes`

Location: Answer-Defaults > Session-Info, Connection *station* > Session-Options

See Also: Call-Filter, Data-Filter, Filter, Filter-Name, Session-Info, Session-Options

Filter-Required

Description: Specifies whether the TAOS unit establishes a call if the filter profile applied in the caller's Connection profile cannot be found locally or in Remote Authentication Dial-In User Service (RADIUS).

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

- Yes specifies that the TAOS unit does not establish a call if the filter profile applied in the caller's Connection profile cannot be found locally or in RADIUS.
- No specifies that the TAOS unit establishes a call if the filter profile applied in the caller's Connection profile cannot be found locally or in RADIUS.

Example: `set filter-required = yes`

Dependencies: Consider the following:

- If the call needs to be brought down, the cause code 425 results. If the call is allowed to come up, the system logs a notice-level message that the filter cannot be found.
- If the Ascend-Filter-Required attribute is missing in the RADIUS user profile, the TAOS unit uses the Filter-Required value in the Answer-Defaults profile.

Location: Answer-Defaults > Session-Info, Connection *station* > Session-Options

See Also: Default-Filter-Cache-Time

Finger

Description: Specifies whether the TAOS unit accepts Finger queries and returns active session details to a remote client.

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

- Yes enables the TAOS unit to accept Finger queries and return the requested active session details to a remote client. The client can ask for short or wide format. For example, a UNIX client can request the wide format by using the `-l` option. The following command:

```
# finger @tnt1
```

displays the narrow (80-character-wide) format. The following command:

```
# finger -l @tnt1
```

displays a wide (140-character-wide) format of session information. The client can also request the details of all sessions, or of a single session. For example, to request information about a single user named Gavin:

```
# finger gavin@tnt1
```

- No causes the TAOS unit to reject queries from Finger clients with the following message:
Finger online user list denied.

Example: `set finger = yes`

Dependencies: Finger 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 client sees the following message:

Finger forwarding service denied.

Location: IP-Global

See Also: Allow-As-Client-DNS-Info, Assign-Count, BOOTP-Enabled, Client-Primary-DNS-Server, Client-Secondary-DNS-Server, Dialout-Poison, DNS-List-Attempt, DNS-List-Size, DNS-Primary-Server, DNS-Secondary-Server, Domain-Name, Drop-Source-Routed-IP-Packets, Ignore-Def-Route, Ignore-ICMP-Redirects, IPRoute-Cache-Enable, IPRoute-Cache-Size, Must-Accept-Address-Assign, NetBIOS-Primary-NS, NetBIOS-Secondary-NS, OSPF-ASE-Pref, OSPF-Pref, Pool-Base-Address, Pool-Summary, RARP-Enabled, RIP-ASE-Type, RIP-Policy, RIP-Pref, RIP-Tag, Sec-Domain-Name, Shared-Prof, Static-Pref, Summarize-RIP-Routes, System-IP-Addr, Telnet-Password, UDP-Cksum, User-Profile

Firewall

Note: The TAOS unit does not support firewalls at this time.

Description: A profile created when you upload a firewall.

Usage: Use the Read and List commands to make Firewall the working profile and list its contents.

Example: To make the Firewall profile secure the working profile and list its contents:

```
admin> read firewall secure
Firewall/secure read
```

```
admin> list
[in FIREWALL/secure]
name* = secure
version = 2
data = [ ACAfiwgAAAAAAADE2RmZDTiz0zOLeDkBAAFTVl4DAAAAA== ]
link = " "
```

Dependencies: The Firewall profile is read only.

See Also: Data, Name, Version

Firewalls-Enabled

Note: The TAOS unit does not support firewalls at this time.

Description: Indicates whether firewalls are enabled.

Usage: The Firewalls-Enabled setting is read only. Yes indicates that firewalls are enabled. No indicates that firewalls are disabled.

Example: firewalls-enabled = yes

Location: Base

See Also: Advanced-Agent-Enabled, AIM-Enabled, Countries-Enabled, Data-Call-Enabled, D-Channel-Enabled, Frame-Relay-Enabled, MAXLink-Client-Enabled, Modem-Dialout-Enabled, Multi-Rate-Enabled, Network-Management-Enabled, PHS-Support, R2-Signaling-Enabled, Selectools-Enabled, Serial-Number, Shelf-Number, Software-Level, Software-Revision, Software-Version, Switched-Enabled, Toggle-Screen

First-Data-Forward-Character

Description: Specifies the hexadecimal value of the first character to be used as a trigger to forward data.

Usage: Specify a hexadecimal value. The default is 04.

Example: set first-data-forward-character = 05

Location: Connection *station* > Visa2-Options

See Also: Fourth-Data-Forward-Character, Second-Data-Forward-Character, Third-Data-Forward-Character

First-Retry-Timer

Description: Specifies, in milliseconds, the initial interval that the TAOS unit waits before making a second attempt to establish a Layer 2 Tunneling Protocol (L2TP) tunnel with another unit. Any change you make to this value takes effect when the previous timer expires.

Usage: Enter a decimal number from 100 to 5000. The default is 1000.

Example: set first-retry-timer = 1000

Dependencies: First-Retry-Timer applies only if you have set L2TP-Mode to LAC.

Location: L2-Tunnel-Global > L2TP-Config

See Also: Control-Connect-Establish-Timer, Hello-Timer, LAC-Incoming-Call-Timer, Retry-Count

Fixed-Packets

Description: Enables or disables the pre-9.0 fax packet scheme for real-time fax processing.

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

- Yes enables the pre-9.0 fax packet scheme. Variable-length, zero-terminated packets are used to process fax calls, allowing Class 1 modems to underrun gracefully.
- No disables the pre-9.0 fax packet scheme. Jitter buffering and packet redundancy for real-time fax processing are enabled.

Example: `fixed-packets = no`

Dependencies: When you set Fixed-Packets to Yes, the Packet-Redundancy setting does not apply.

Location: VoIP {x y} > RT-Fax-Options

See Also: Packet-Redundancy

Flow-Control

Description: Specifies the flow control method used on the serial port.

Usage: Specify one of the following values:

- None (the default)
- Xon-Xoff
- Hardware-Handshake

Example: `set flow-control = xon-xoff`

Location: Serial {shelf-N slot-N N}

See Also: Serial

Flush-Length

Description: Specifies the maximum number of bytes to buffer when handling incoming TCP-Clear data that does not require V.120 processing. If the system buffers the specified number of bytes without matching the End-Of-Packet-Pattern value, the TAOS unit flushes the buffer by writing the data into TCP packets.

Usage: Specify an integer from 1 to 8192. The default is 256. Note that buffering large packets consumes a larger amount of system resources than buffering small packets.

Example: `set flush-length = 300`

Dependencies: If Detect-End-Of-Packet is set to No, Flush-Length does not apply.

Location: Answer-Defaults > TCP-Clear-Answer, Connection *station* > TCP-Clear-Options

See Also: Detect-End-Of-Packet, Enabled, End-Of-Packet-Pattern, Flush-Time

Flush-Time

Description: Specifies the amount of time (in milliseconds) to buffer TCP-Clear data that does not require V.120 processing. The timer begins counting down upon receiving the first byte of buffered data. If the specified number of milliseconds elapses before the buffered data matches the End-Of-Packet-Pattern value, the TAOS unit flushes the buffer by writing the data into TCP packets.

Usage: Specify an integer from 1 to 1000. The default is 20.

Example: `set flush-time = 300`

Dependencies: If Detect-End-Of-Packet is set to No, Flush-Time does not apply.

Location: Answer-Defaults > TCP-Clear-Answer, Connection *station* > TCP-Clear-Options

See Also: Detect-End-Of-Packet, Enabled, End-Of-Packet-Pattern, Flush-Length

Force-56Kbps

Description: Specifies whether the TAOS unit uses only the 56-Kbps portion of a channel, even when all 64 Kbps appear to be available.

The default bandwidth for data calls coming in over E1 channels using R2 signaling is now 64K. To configure a connection to use 56K instead, set Force-56Kbps to Yes. In addition, you should specify this setting when you place calls to European or Pacific Rim countries from within North America, if the complete path cannot distinguish between the Switched-56 and Switched-64 data services. You need not set this value for calls within North America.

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

- Yes causes the TAOS unit to use only the 56-Kbps portion of a channel.
- No specifies that the TAOS unit uses the full 64-Kbps bandwidth, if it is available.

Example: `set force-56kbps = no`

Location: Answer-Defaults, Connection *station* > Telco-Options

See Also: Data-Service, Telco-Options

Force-Fragmentation

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

Usage: Specify Yes or No.

- Yes specifies that when the MTU-Limit setting is a nonzero value, the TAOS unit ignores the DF bit and performs the fragmentation that normally should be performed by the client. It prefragments those packets at the specified MTU-Limit size, and then adds the GRE and IP headers.

Setting the Force-Fragmentation setting to Yes causes the TAOS unit to bypass the standard MTU discovery mechanism and fragment larger packets before encapsulating them in GRE. Because this scenario changes expected behavior, it is not recommended except for Ascend Tunnel Management Protocol (ATMP) interoperoperation with outdated client software that does not handle fragmentation properly.

- No (the default) specifies that the TAOS unit does not fragment an incoming packet that has the DF bit set.

Dependencies: You must set MTU-Limit to a nonzero value when you set Force-Fragmentation to Yes.

Location: ATMP

See Also: Agent-Mode, Agent-Type, MTU-Limit, Password, Retry-Limit, Retry-Timeout, UDP-Port

Format

Description: Specifies the ATM End System Address (AESA) format for the interface.

Usage: Specify one of the following settings:

- Undefined (the default) specifies that an address has not been configured.
- DCC-AESA specifies that Data Country Code (DCC) is indicated in the address, identifying the country in which the address is registered. Country codes are standardized and defined in ISO Reference 3166.
- ICD-AESA specifies that International Country Designator (ICD) is indicated in the address, identifying an international organization. The British Standards Organization administers these values.
- E164-AESA specifies an E.164 address that uses the international format.
- Custom-AESA specifies the custom Authority and Format Identifier (AFI) and byte order.

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > ATM-Address > AESA-Address,
Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr > AESA-Address
Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr > AESA-Address

See Also: DSP-Portion, IDP-Portion

Forward

Description: Specifies the forwarding action for a filter. For a data filter, the Forward value specifies whether the TAOS unit forwards or drops packets that match the filter rules. For a call filter, the Forward value specifies whether matching packets reset the session timer or bring up a connection.

Usage: Specify Yes or No. When no filters are in use, the TAOS unit forwards all packets by default. When a filter is in use, the TAOS unit discards all packets by default.

- Yes specifies that the TAOS unit forwards packets that match the filter rules.
- No specifies that the TAOS unit drops packets that match the filter rules.

Example: `set forward = yes`

Location: Filter *filter-name* > Input-Filters, Filter *filter-name* > Output-Filters

See Also: Input-Filters, Input-Filters N, Output-Filters, Output-Filters N

Fourth-Data-Forward-Character

Description: Specifies the hexadecimal value of the fourth character to be used as a trigger to forward data.

Usage: Specify a hexadecimal value. The default is 05.

Example: `set fourth-data-forward-character = 06`

Location: Connection *station* > Visa2-Options

See Also: First-Data-Forward-Character, Second-Data-Forward-Character, Third-Data-Forward-Character

FR-08-Mode

Description: Specifies whether Frame Relay traffic can be switched across a DS3-ATM card without translating the data to Asynchronous Transfer Mode (ATM) format.

Usage: Specify one of the following settings:

- Translation (the default) specifies that the Frame Relay traffic is translated before it is switched.
- Transparent enables FRF.8 Transparent mode support, specifying that the Frame Relay traffic is passed to the ATM switch without being translated.

Example: `set fr-08-mode = transparent`

Dependencies: You must set Encapsulation-Protocol to ATM-Frame-Relay-Circuit for the FR-08-Mode setting to have any effect.

Location: Connection *station* > ATM-Options

See Also: Encapsulation-Protocol

FR-Address

Description: Specifies the E.164 address for this data link.

Usage: Specify an E.164 address. E.164 addresses are ISDN numbers, including telephone numbers. An E.164 address can contain up to 15 ASCII digits. For example, standard 10-digit United States telephone numbers, such as 508-555-1234, are native E.164 addresses.

Example: `set fr-address = 508-555-1234`

Dependencies: The value of FR-Address is the Calling-Line ID (CLID) for dial-out Switched Virtual Connections (SVCs) on this interface.

Location: Frame-Relay *fr-name* > SVC-Options

See Also: Enabled

Framed-Only

Description: Specifies whether an incoming call must use a framed protocol.

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

- Yes specifies that an incoming call must use a framed protocol.
- No specifies that an incoming call need not use a framed protocol.

Example: `set framed-only = yes`

Location: Answer-Defaults, Connection *station*

See Also: Encapsulation-Protocol, Frame-Length, Frame-Type, Protocol

Frame-Length

Description: For incoming V.120 calls, specifies the frame length. For packets sent by X.75 TAs, specifies the number of bytes in the information field.

Usage: For V.120 calls, specify an integer from 30 to 260, or accept the default of 256, which enables the TAOS unit to operate with an AT&T ISDN telephone without reconfiguration. For X.75 calls, specify an integer from 128 to 2048. For X.75 calls, the default is 1024.

Example: `set frame-length = 260`

Location: Answer-Defaults > V120-Answer
Answer-Defaults > X75-Answer
Connection > X75-Options

See Also: Encapsulation-Protocol, Framed-Only, Frame-Type, V120-Answer

Frame-Relay

Description: A profile that specifies the datalink to a Frame Relay switch or Customer Premises Equipment (CPE).

Usage: Use the New and List commands to create a Frame-Relay profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Frame-Relay profile `pacbell` the working profile and list its contents:

```
admin> new frame-relay pacbell
FRAME-RELAY/pacbell read

admin> list
[ in FRAME-RELAY/pacbell (new) ]
fr-name* = pacbell
active = no
nailed-up-group = 1024
nailed-mode = ft1
called-number-type = national
switched-call-type = 56k-restricted
phone-number = " "
billing-number = " "
transit-number = " "
link-mgmt = none
call-by-call-id = 0
n391-val = 6
n392-val = 3
n393-val = 4
t391-val = 10
t392-val = 15
mru = 1532
link-type = dte
dcen392-val = 3
dcen393-val = 4
mfr-bundle-name = " "
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
FRAME-RELAY/pacbell written
```

See Also: Active, Billing-Number, Call-By-Call-ID, Called-Number-Type, DCEN392-Val, DCEN393-Val, FR-Name, Link-Mgmt, Link-Type, MFR-Bundle-Name, MRU, N391-Val, N392-Val, N393-Val, Nailed-Mode, Nailed-Up-Group, Phone-Number, Switched-Call-Type, T391-Val, T392-Val, Transit-Number

Frame-Relay-Enabled

Description: Indicates whether Frame Relay is enabled on the TAOS unit.

Usage: The Frame-Relay-Enabled setting is read only. Yes indicates that Frame Relay is enabled. No indicates that Frame Relay is not enabled.

Example: `frame-relay-enabled = no`

Location: Base

See Also: Frame-Relay

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: If FR-Direct-Enabled is set to Yes, Frame-Relay-Profile does not apply.

Location: Connection *station* > FR-Options

See Also: Encapsulation-Protocol, FR-Direct-Enabled, FR-Name, FR-Options

Framer-Mode

Description: Specifies the DS3-ATM, E3 ATM, or Sonet framer mode.

Usage: In a DS3-ATM profile, specify one of the following values:

- C-Bit-ADM specifies free-running and fixed-stuffing C-Bit-ADM mode.
- C-Bit-PLCP (the default) specifies free-running and fixed-stuffing C-Bit-PLCP mode.
- C-Bit-ADM-Loop-Timed specifies loop-timed C-Bit-ADM mode.
- C-Bit-PLCP-Loop-Timed specifies loop-timed C-Bit-PLCP mode.
- C-Bit-ADM-Frame-Locked specifies frame-locked C-Bit-ADM mode.
- C-Bit-PLCP-Frame-Locked specifies frame-locked C-Bit-PLCP mode.

In an E3-ATM profile, specify one of the following values:

- G751-ADM (the default) specifies G751 framing with ATM Direct cells.
- G751-PLCP specifies G751 framing with PLCP cells.
- G832-ADM specifies G832 framing with ATM Direct cells

In an OC3-ATM profile, specify Sonet or SDH (the default).

Example: `set framer-mode = c-bit-plcp-frame-locked`

Location: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line Config

See Also: Framer-Rate

Framer-Rate

Description: Specifies the framing to use on the link.

Usage: Currently, the only supported value is STS-3C, which is used for a 155.52-Mbps interface in the U.S. as well as the equivalent European 155 Mbps interface (STM-1).

Location: OC3-ATM {shelf-*N* slot-*N* *N*} > Line-Config

See Also: Framer-Mode

Frames-Per-Packet

Description: Specifies the number of compressed audio frames assigned to each Real-Time Transport Protocol (RTP) packet used to transport voice across the IP network.

Usage: Specify a number from 1 to 10. The default is 4.

Example: `set frames-per-packet = 10`

Dependencies: Consider the following:

- Lowering the value of Frames-Per-Packet reduces the delay and distortion introduced into any given voice call. But a lower value can also degrade performance, because it results in more IP packets per voice call.
- When a different audio codec is dynamically selected during call setup, the TAOS unit uses the default value of four frames per RTP packet to process that call.

Location: VoIP {*x y*}

See Also: Packet-Audio-Mode

Frame-Type

Description: Specifies the framing mode in use on the physical links of a T1, E1, or DS3 line. Your carrier can tell you which framing mode to choose.

Usage: For a T1 or E1 line, specify one of the following values:

- D4 specifies the superframe format, which consists of 12 consecutive frames, separated by framing bits. Do not use this setting with ISDN D-channel signaling (when Signaling-Mode is set to ISDN).
- ESF specifies the Extended Superframe Format, which consists of 24 consecutive frames, separated by framing bits. The ISDN specification advises that you use ESF with ISDN D-channel signaling (when Signaling-Mode is set to ISDN).

An E1 line supports the following additional Frame-Type values:

- G703 specifies that the trunk interface uses CRC-4.
- 2DS specifies that the trunk interface does not use CRC-4.

A DS3 line supports only the following values:

- M13 specifies an M23 application.
- C-Bit-Parity specifies a C-bit parity application.

Example: `set frame-type = esf`

Location: E1 {shelf-*N* slot-*N N*} > Line-Interface,
T1 {shelf-*N* slot-*N N*} > Line-Interface, T3 {shelf-*N* slot-*N N*}

See Also: Framed-Only, Line-Interface, Signaling-Mode

FR-Answer

Description: A subprofile in the Answer-Defaults profile. The FR-Answer subprofile can enable the TAOS unit to answer incoming connections that use Frame Relay encapsulation.

Usage: With Answer-Defaults as the working profile, list the FR-Answer subprofile. You can then use the Set command to modify the setting in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the FR-Answer subprofile:

```
admin> list fr-answer
[in ANSWER-DEFAULTS:fr-answer]
enabled = yes
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Enabled

FR-Direct-DLCI

Description: Specifies the Data Link Connection Identifier (DLCI) in a Frame Relay Direct configuration.

Usage: Specify an integer from 16 to 991. The default value is 16.

Example: `set fr-direct-dlci = 25`

Dependencies: FR-Direct-DLCI applies only if FR-Direct-Enabled is set to Yes.

Location: Connection *station* > FR-Options

See Also: FR-Direct-Enabled

FR-Direct-Enabled

Description: Specifies that the TAOS unit uses the connection for Frame Relay Direct.

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

- Yes specifies that the TAOS unit uses the connection for Frame Relay Direct.
- No specifies that the TAOS unit does not use the connection for Frame Relay Direct.

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 *station* > FR-Options

See Also: Encapsulation-Protocol, FR-DLCI, FR-Options, FR-Profile

FR-Direct-Profile

Description: Specifies the name of the Frame Relay profile for a Frame Relay Direct configuration.

Usage: Specify the name of a Frame Relay profile. This profile connects to the Frame Relay switch handling the Data Link Connection Identifier (DLCI) specified by FR-Direct-DLCI. You can specify up to 15 lowercase, alphanumeric characters. The default value is null.

Example: `set fr-direct-profile = myprofile`

Dependencies: FR-Direct-Profile applies only if FR-Direct-Enabled is set to Yes.

Location: Connection *station* > FR-Options

See Also: FR-Direct-Enabled

FR-DLCI

Description: Specifies a Frame Relay 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: Consider the following:

- If FR-Direct-Enabled is set to No, FR-DLCI does not apply.
- The T1 Frameline card supports a maximum of 240 active DLCIs.
- The Serial WAN (SWAN) card supports a maximum of 120 active DLCIs.

Location: Connection *station* > FR-Options

See Also: Encapsulation-Protocol, FR-Direct-Enabled, FR-Options, FR-Profile

FR-LinkDown-Enabled

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

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

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

Example: `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 *host-name*

See Also: Alarm-Enabled, FR-LinkUp-Enabled

FR-Link-Type

Description: Specifies the type of link for the circuit endpoint.

Usage: Specify one of the following settings:

- Transparent-Link (the default) specifies a 1:1 circuit. It requires two endpoints that specify the same circuit name and the Transparent-Link type. If only one endpoint is specified, data received on the specified DLCI is dropped. If more than two Transparent-Link endpoints are specified with the same circuit name, only two of the profiles will be used to form a circuit.
- Host-Link specifies virtual channel trunking with multiple endpoints on the host side.
- Trunk-Link specifies virtual channel trunking with a single endpoint on the trunk side.

Example: `set fr-link-type = host-link`

Location: Connection *station* > FR-Options

See Also: FR-08-Mode

FR-LinkUp-Enabled

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

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

- Yes specifies that a trap is sent whenever a DLCI is brought up.
- 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 *host-name*

See Also: Alarm-Enabled, FR-LinkDown-Enabled

FR-Name

Description: Specifies the name of a Frame-Relay profile.

Usage: Specify a name for the profile. The name must be unique and cannot exceed 15 characters. The default is null.

Example: `set fr-name = att-dce`

Location: Frame-Relay *fr-name*

See Also: Frame-Relay-Profile

Front-End-Type

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

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

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

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

- Long-Haul (120-ohm termination only) is equivalent to the CSU setting for a T1 line. The transmitter sends a standard bipolar pulse. The receiver amplifies the signal level, and has to correct for the distortion caused by the transmission line. This correction is done by a equalizer that is part of the receiver.
- Short-Haul is equivalent to the DSX setting for a T1 line. The transmitter sends a pulse shaped so that the receiver gets a “perfect” nominal bipolar pulse shape. On the basis of the standardized line type and the line length configured by the user, the transmitter determines what kind of pulse should be transmitted. The receiver gets a “perfect” pulse shape and only needs to compensate for the signal amplitude.

Example: `set front-end-type = csu`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface, T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: CSU-Build-Out, DSX-Line-Length, Line-Interface

FR-Options

Description: A subprofile containing settings for Frame Relay connections.

Usage: With a Connection profile as the working profile, list the FR-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the FR-Options subprofile:

```
admin> list fr-options
[In CONNECTION/tim:fr-options]
frame-relay-profile = " "
circuit-type = pvc
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
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: Frame Relay calls must be enabled in the Answer-Defaults profile.

Location: Connection *station*

See Also: Circuit-Name, Circuit-Type, DLCI, Frame-Relay-Profile, FR-Direct-DLCI, FR-Direct-Enabled, FR-Direct-Profile, FR-DLCI, FR-Link-Type, FR-Profile

FR-Profile

Description: Specifies the name of the Frame-Relay profile to use for a Frame Relay Direct connection.

Usage: Specify the name of a configured Frame-Relay profile, exactly as specified by the FR-Name setting, including case changes.

Example: `set fr-profile = att-dce`

Dependencies: For FR-Profile to apply, you must set FR-Direct-Enabled to Yes.

Location: Connection *station* > FR-Options

See Also: Encapsulation-Protocol, FR-Direct-Enabled, FR-DLCI, FR-Options

FT1-Caller

Description: Specifies whether the TAOS unit initiates fractional T1 calls.

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

- Yes enables the TAOS unit to initiate the FT1 call. The unit dials to bring online any switched circuits that are part of the call.
- No specifies that the TAOS unit cannot originate the FT1 call.

Example: `set ft1-caller = yes`

Dependencies: The FT1-Caller value applies when both nailed-up and switched channels are in use for the connection (that is, when Call-Type is set to FT1-MPP). Only one side of the connection should have FT1-Caller set to Yes.

Location: Connection *station* > Telco-Options

See Also: Call-Type, Telco-Options

Function

Description: Specifies whether the controller is functional and, if so, whether it is a primary controller or a secondary controller.

Usage: The Function setting is read only. Its possible values are No-Function, Primary, or Secondary.

Example: `function = primary`

Location: Redundancy-Stats > Context-Stats > Context-Stats *N*

See Also: Prior-Function

G

G711-Transparent-Data

Description: Enables or disables transparent modem mode for a Voice over IP (VoIP) configuration.

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

- Yes specifies that when a MultiVoice gateway detects a fax or modem Answer tone in a VoIP channel, the unit transparently requests end-to-end G.711 encoding and bandwidth for the call, in a process similar to that used by real-time fax. The echo cancelers are disabled when the unit enters this mode. The data is encoded transparently as an audio-mode type, either G.711 U-Law (64Kbps) or G.711 A-Law (64Kbps).
- No specifies that a MultiVoice gateway continues with VoIP call processing, even when a fax or modem Answer tone is detected.

Example: `set g711-transparent-data = yes`

Dependencies: Consider the following:

- The G711-Transparent-Data setting does not apply when G.711 U-Law or G.711 A-Law encoding is selected for the Packet-Audio-Mode setting.
- Settings take effect with the next incoming Public Switched Telephone Network (PSTN) call.
- A separate license is not required for this feature.
- In a Signaling System 7 (SS7) environment, values in IPDC messages override corresponding call management settings in the default VoIP profile.

Location: VoIP {x y}

See Also: Allow-Coder-Fallback, Allow-G711-Fallback

Gatekeeper-IP

Description: Specifies the primary device that performs all H.323 gatekeeper functions for the TAOS unit when MultiVoice is configured to perform H.323 processing.

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

Example: `set gatekeeper-ip = 10.1.2.3`

Dependencies: Consider the following:

- Changes to Gatekeeper-IP take effect after the TAOS unit is reinitialized.
- In order for a TAOS unit to start processing Voice over IP (VoIP) calls in an H.323 network, you must specify a value for Gatekeeper-IP.

Location: VoIP {x y}

See Also: Gatekeeper-IP-Sec, Gatekeeper-Keepalive

Gatekeeper-IP-Sec

Description: Specifies the secondary device that performs all H.323 gatekeeper functions for the TAOS unit when MultiVoice is configured to perform H.323 processing.

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

Example: `set gatekeeper-ip-sec = 10.1.2.4`

Dependencies: When you do not specify a value for Gatekeeper-IP-Sec, the TAOS unit goes into slow poll mode with the MultiVoice™ Access Manager (MVAM) device at the address specified by the Gatekeeper-IP parameter. The TAOS unit attempts registration with the MVAM at 30-second intervals. During the time the gateway is unregistered, the TAOS unit rejects any new calls.

Location: VoIP {x y}

See Also: Gatekeeper-IP, Gatekeeper-Keepalive

Gatekeeper-Keepalive

Description: Specifies the time interval (in seconds) between attempts to reregister with a system running the MultiVoice Access Manager (MVAM).

Usage: Specify a number from 1 to 65535. The default is 120.

Example: `set gatekeeper-keepalive = 180`

Dependencies: If you change the value of Gatekeeper-Keepalive, you should also change the registrationDuration value on the MVAM.

Location: VoIP {x y}

See Also: Gatekeeper-IP, Gatekeeper-IP-Sec, Registration-Retries

Gateway-Access-Number

Description: Specifies the Dialed Number Information Service (DNIS) number passed from the Public Switched Telephone Network (PSTN) associated with the inbound telephone number used to access the TAOS unit.

Usage: Specify a telephone number. The default is null. If you have configured the unit to perform two-stage dialing of Voice over IP (VoIP) calls, specify the telephone number dialed to gain access to the unit from the PSTN.

Example: `set gateway-access-number = 8903190`

Location: VoIP {x y} > VoIP-Index

See Also: Far-End-Number

Gateway-Address

Description: Specifies the address of the next-hop router the TAOS unit uses to reach the destination address specified by a static or private route. A next-hop router is directly connected to the TAOS unit on the Ethernet, or is one hop away on a WAN link.

Usage: Specify the IP address of the router the TAOS unit uses to reach the target host for the route. The default is 0.0.0.0.

Example: `set gateway-address = 10.207.23.1`

Dependencies: You must make sure that Voice over IP (VoIP) calls can always find a route to the next-hop gateway on the path to the destination VoIP gateway. The route can be learned dynamically or configured as a static route. Many sites choose to configure default routes for VoIP traffic, so that Real-Time Transport Protocol (RTP) packets are never dropped due to lack of routing information.

Location: IP-Route *name*,
Private-Route-Table *name* > Route-Description-List > Route-Description-List *N*

See Also: Dest-Address

Gen-Filter

Description: A subprofile containing a generic filter specification.

Usage: With a Filter profile as the working profile, list the Gen-Filter subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Gen-Filter subprofile:

```
admin> list input-filters 1 gen-filter
[in FILTER/test:input-filters[1]:gen-filter]
offset = 2
len = 8
more = no
comp-neq = no
mask = 0f:ff:ff:ff:00:00:00:f0:00:00:00:00
value = 07:fe:45:70:00:00:00:90:00:00:00:00
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name* > Input-Filters, Filter *filter-name* > Output-Filters

See Also: Comp-Neq, Input-Filters, Input-Filters N, Len, Mask, More, Offset, Output-Filters, Output-Filters N, Value

Gk-Mlg-Control

Description: Specifies whether a MultiVoice gateway can accept and process call-specific administration instructions from a device running version 3.0 of MultiVoice Access Manager (MVAM).

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

- Yes enables processing of call-specific administration instructions. The gateway can apply call-specific processing instructions for PIN authentication, single- or two-stage dialing, voice-announcement playback, and call timers for prepaid billing. Values received from an MVAM device or from a third-party billing system override parameter settings in the VoIP profile for processing the current VoIP call.
- No disables processing of call-specific administration instructions. When you specify this value, the unit uses the values in the VoIP profile to perform global administration of Voice over IP (VoIP) calls.

Example: `set gk-mlg-control = yes`

Dependencies: If Gk-Mlg-Control is set to Yes, the VPN-Mode and Single-Dial-Enable values do not apply.

Location: VoIP { x y }

See Also: Single-Dial-Enable, VPN-Mode

Global-Call-ID

Description: Indicates the global call ID for Signaling System 7 (SS7) data or Voice over IP (VoIP) calls.

Usage: The Global-Call-ID value is read only.

Example: `global-call-id = 03040506-0102-0900-0807-010203040506`

Location: Call-Info

Global-VRouter

Description: Specifies a name for the global Virtual Router (VRouter).

Usage: Specify up to 23 characters. The default is `main`.

Example: `set global-vrouter = global-1`

Location: IP-Global, IPX-Global

See Also: System-IP-Addr

GMT-Offset

Description: Specifies your time zone as an offset from Coordinated Universal Time (UTC). The GMT-Offset setting enables the TAOS unit to update its system time from an SNTP server.

UTC is in the same time zone as Greenwich Mean Time (GMT), and the offset is specified in hours, using a 24-hour clock. Because some time zones, such as Newfoundland, cannot use an even-hour boundary, the offset includes 4 digits and is specified in half-hour increments. For example, in Newfoundland the time is 1.5 hours ahead of UTC, so GMT-Offset is represented as follows:

UTC+0130

For San Francisco, which is 8 hours ahead of UTC:

UTC+0800

For Frankfurt, which is 1 hour behind UTC:

UTC-0100

Usage: Specify one of the following values to represent your time zone:

UTC-1130
UTC-1100
UTC-1030
UTC-1000
UTC-0930
UTC-0900
UTC-0830
UTC-0800
UTC-0730
UTC-0700
UTC-0630
UTC-0600
UTC-0530
UTC-0500
UTC-0430
UTC-0400
UTC-0330
UTC-0300
UTC-0230
UTC-0200
UTC-0130
UTC-0100
UTC-0030
UTC+0000
UTC+0030
UTC+0100
UTC+0130
UTC+0200
UTC+0230
UTC+0300
UTC+0330
UTC+0400

UTC+0430
UTC+0500
UTC+0530
UTC+0600
UTC+0630
UTC+0700
UTC+0730
UTC+0800
UTC+0830
UTC+0900
UTC+0930
UTC+1000
UTC+1030
UTC+1100
UTC+1130
UTC+1200

Example: `set gmt-offset = utc+0800`

Location: IP-Global > SNTP-Info

See Also: Enabled, Host, SNTP-Info

Group-II-Signal

Description: Specifies the group-II signal, which the TAOS unit sends on an outgoing call immediately after the called end acknowledges that it has received all the necessary address digits.

Usage: Specify Signal-II-1, Signal-II-2, and so on, up to Signal-II-15. The default is Signal-II-2. Systems in Mexico and Korea should use the default. Systems in Argentina should set Group-II-Signal to Signal-II-1. For information about the proper settings for other countries, please contact your carrier.

Example: `set group-ii-signal = signal-ii-2`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Group-B-Answer-Signal, Group-B-Busy-Signal, Line-Interface

Group-B-Answer-Signal

Description: Specifies the group-B signal that the TAOS unit sends immediately before answering an incoming call.

Usage: Specify Signal-B-1, Signal-B-2, and so on, up to Signal-B-15. The default is Signal-B-6, which is the recommended setting for E1-R2 Israeli signaling. The relevant specifications for E1-R2 Israeli signaling are in ITU-T recommendations Q.400 to Q.490 and Israeli MFC-R2 Register Signaling documentation.

Systems in Mexico and Korea should set Group-B-Answer-Signal to Signal-B-1. Systems in Argentina should use Signal-B-6 (the default). For information about the proper settings for other countries, please contact your carrier.

Example: `set group-b-answer-signal = signal-b-6`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Group-II-Signal, Group-B-Busy-Signal, Group-B-Collect-Signal

Group-B-Busy-Signal

Description: Specifies the group-B signal that the TAOS unit sends as a busy signal.

Usage: Specify Signal-B-1, Signal-B-2, and so on, up to Signal-B-15. The default is Signal-B-3, which is the recommended setting for E1-R2 Israeli signaling. The relevant specifications for E1-R2 Israeli signaling are in ITU-T recommendations Q.400 to Q.490 and Israeli MFC-R2 Register Signaling documentation.

Example: `set group-b-busy-signal = signal-b-3`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Group-B-Answer-Signal, Group-B-Collect-Signal

Group-B-Collect-Signal

Description: For Brazilian R2 signaling lines, specifies the group-B signal that the TAOS unit sends in response to a collect call.

Usage: Specify one of the following signal values:

- Signal-B-2 specifies a busy line.
- Signal-B-5 specifies a line for which there is no fee.
- Signal-B-7 specifies that the line does not accept collect calls, that the number is not accessible, or that the call is forwarded to an answering machine.

Dependencies: If Signaling-Mode is set to any value other than E1-Brazil-Signaling, the Group-B-Collect-Signal setting does not apply.

Example: `set group-b-collect-signal = signal-b-7`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Group-II-Signal, Group-B-Answer-Signal, Group-B-Busy-Signal

H

H323-Voice-Ann-Enabled

Description: Specifies whether the TAOS unit plays voice announcements for callers to indicate call progress.

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

- Yes specifies that the TAOS unit plays voice announcements.
- No specifies that the TAOS unit plays Dual Tone Multifrequency (DTMF)-based call-progress tones. These tones can include traditional Public Switched Telephone Network (PSTN) call-progress tones, such as ringback and busy signals, which are easily recognized by the caller. They can also include MultiVoice call-progress tones, such as PIN prompt and PIN error tone, which are not as easily recognized.

Example: `set h323-voice-ann-enabled = yes`

Dependencies: Even when voice announcements are enabled, users still hear call-progress tones under the following conditions:

- A traditional call progress tone is available.
- The gateway cannot play any more simultaneous announcements.

Changes to H323-Voice-Ann-Enabled are effective with the next Voice over IP (VoIP) call.

Location: VoIP {x y}

See Also: Voice-Ann-Dir

Hardware-Level

Description: Indicates a one- or two-character string representing the hardware revision level of the card.

Usage: The Hardware-Level setting is read only. A value of 0 (zero) means that the revision level is unknown.

Location: Base, Slot-Info {shelf-N slot-N N}

See Also: Software-Level

Hardware-Rework-Count

Description: Indicates the number of times the card has been reworked.

Usage: The Hardware-Rework-Count setting is read only.

Location: Slot-Info {shelf-N slot-N N}

See Also: Hardware-Level

HDLC2

Description: Specifies the action to take when the code image for a Hybrid Access II card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, SWAN, T3, UDS3, UE1, Unknown-Cards, UT1

HDLC-NRM-Answer

Description: A subprofile that lets you specify whether the system rejects incoming High-Level Data Link Control-Normal Response Mode (HDLC-NRM) calls.

Usage: With the Answer-Defaults profile as the working profile, list the HDLC-NRM-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the HDLC-NRM-Answer subprofile:

```
admin> list hdlc-nrm-answer
[ in ANSWER-DEFAULTS:hdlc-nrm-answer ]
enabled = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Enabled

HDLC-NRM-Options

Description: A subprofile containing settings for High-Level Data Link Control-Normal Response Mode (HDLC-NRM) connections.

Usage: With a Connection profile as the working profile, list the HDLC-NRM-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the HDLC-NRM-Options subprofile:

```
admin> list hdlc-nrm-options
[in CONNECTION/newyork:hdlc-nrm-options]
enabled = no
snrm-response-timeout = 20000
snrm-retry-counter = 2
poll-timeout = 60000
poll-rate = 5000
poll-retry-counter = 2
primary = yes
async-drop = yes
station-poll-address = 255
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: Async-Drop, Enabled, Poll-Rate, Poll-Retry-Counter, Poll-Timeout, Primary, SNRM-Response-Timeout, SNRM-Retry-Counter, Station-Poll-Address

Heart-Beat

Description: Enables or disables detection of a physical link failure, such as the disconnection of a cable or the failure of the signaling gateway.

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

- Yes specifies enables detection of a physical link failure. When you specify Yes, the TAOS unit periodically sends out heartbeat frames to the signaling gateway and waits for an acknowledgment. If it does not receive an acknowledgment within the number of milliseconds specified by T2-Duration, the unit resets the signaling link.
- No disables detection of a physical link failure.

Example: `set heart-beat = yes`

Location: SS7-Gateway > Transport-Options

See Also: ACK-Threshold, Device-ID, T1-Duration, T2-Duration, T3-Duration, Window-Size

Hello-Interval

Description: Specifies the number of seconds between the Hello packets that the Open Shortest Path First (OSPF) router sends on the interface.

Usage: Specify an integer. The defaults are 10 seconds for connected routes and 30 seconds for WAN connections.

Example: `set hello-interval = 30`

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF

See Also: Dead-Interval, IP-Options, OSPF, OSPF-Options

Hello-Timer

Description: Specifies the interval, in seconds, between Hello messages that the TAOS unit sends to another unit. Any change you make to this value takes effect when the previous timer expires.

Usage: Specify a decimal number from 0 to 600. The default is 60. 0 specifies that the TAOS unit sends no Hello messages.

Example: `set hello-timer = 60`

Dependencies: Hello-Timer applies only if you have set L2TP-Mode to LAC.

Location: L2-Tunnel-Global > L2TP-Config

See Also: Control-Connect-Establish-Timer, First-Retry-Timer, LAC-Incoming-Call-Timer, Retry-Count

High-Temperature-Trigger

Description: Specifies the high-temperature threshold setting for the fantray.

Usage: Specify a number from 0 to 60 degrees Celsius. The default is 40.

Example: `set high-temperature-trigger = 45`

Dependencies: If the fantray is in auto-regulation mode (Operation-Mode is set to Auto-Regulation) and the High-Temperature-Trigger threshold is crossed, the system switches the fans to full speed and logs a message. If you specify a lower value than the Low-Temperature-Trigger setting, the system displays an error message when you attempt to write the profile.

Location: Thermal

See Also: Low-Temperature-Trigger, Operation-Mode

High-Tx-Output

Description: Specifies whether the DS3 or E3 cable length is more than 255 feet.

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

- Yes specifies that the cable length is more than 255 feet.
- No specifies that the cable length less than 255 feet.

Example: `set high-tx-output = yes`

Location: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config

See Also: Loopback

Hint-Net-Hi

Description: Specifies the end of the network range for an AppleTalk network. If the TAOS unit is the first router up and is in nonseed mode, it uses the Hint settings to try to find another router. To optimize the process by which a nonseed router acquires a configuration across the network after a system reset or power cycle, you set Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, and Hint-Zone with known good information. A seed router must be available at startup time, or the TAOS unit cannot come up in AppleTalk routing mode.

Usage: Specify an integer from 1 to 65,199. The default is 0 (zero).

Example: `set hint-net-hi = 300`

Dependencies: If Atalk-Routing-Enabled is set to No, Atalk-Router is set to Atlk-Router-Off, or Atalk-Router is set to Atlk-Router-Seed, Hint-Net-Hi does not apply.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}

See Also: Atalk-Default-Zone, Atalk-Net-End, Atalk-Net-Start, Atalk-Router, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Lo, Hint-Net-Node, Hint-Zone, Interface-Address

Hint-Net-Lo

Description: Specifies the beginning of the network range for an AppleTalk network. If the TAOS unit is the first router up and is in nonseed mode, it uses the Hint settings to try to find another router. To optimize the process by which a nonseed router acquires a configuration across the network after a system reset or power cycle, you set Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node, and Hint-Zone with known good information. A seed router must be available at startup time, or the TAOS unit cannot come up in AppleTalk routing mode.

Usage: Specify an integer from 1 to 65,199. The default is 0 (zero).

Example: `set hint-net-lo = 200`

Dependencies: If Atalk-Routing-Enabled is set to No, Atalk-Router is set to Atlk-Router-Off, or Atalk-Router is set to Atlk-Router-Seed, Hint-Net-Lo does not apply.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}

See Also: Atalk-Default-Zone, Atalk-Net-End, Atalk-Net-Start, Atalk-Router, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Node, Hint-Zone

Hint-Net-Node

Description: Specifies an AppleTalk node number that the TAOS unit can use when it comes up as a nonseed router.

Usage: Specify a node number. The default is 0 (zero).

Example: `set hint-net-node = 5`

Dependencies: If Atalk-Routing-Enabled is set to No, Atalk-Router is set to Atlk-Router-Off, or Atalk-Router is set to Atlk-Router-Seed, Hint-Net-Node does not apply.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}

See Also: Atalk-Default-Zone, Atalk-Net-End, Atalk-Net-Start, Atalk-Router, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Lo, Hint-Zone

Hint-Zone

Description: Specifies the AppleTalk zone in which the TAOS unit resides. The unit can include the zone name in the ZipGetNetInfo request packet it sends out to get its configuration from a seed router, and the router can return a valid network range for the zone.

Usage: Specify a zone name of up to 32 characters. The default is null.

Example: `set hint-zone = Alameda`

Dependencies: If Atalk-Routing-Enabled is set to No, Atalk-Router is set to Atlk-Router-Off, or Atalk-Router is set to Atlk-Router-Seed, Hint-Zone does not apply.

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}

See Also: Atalk-Default-Zone, Atalk-Net-End, Atalk-Net-Start, Atalk-Router, Atalk-Routing-Enabled, Atalk-Zone-List, Hint-Net-Hi, Hint-Net-Lo, Hint-Net-Node

HO-DSP

Description: Specifies the hexadecimal number for the High-Order Domain-Specific Part (HO-DSP) field of an ATM End System Address (AESA). This field specifies a segment of address space assigned to a particular device or network.

Usage: For the DCC-AESA and ICD-AESA formats, the HO-DSP field is 10 bytes long, containing 20 hexadecimal digits. For the E164-AESA format, it is 4 bytes long (8 hexadecimal digits), and for the Custom-AESA format it is 12 bytes long (24 hexadecimal digits). The default is null.

Example: `set ho-dsp = 01020304050607080900`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > ATM-Address > AESA-Address > DSP-Portion,
Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr > AESA-Address > DSP-Portion,
Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr > AESA-Address > DSP-Portion

See Also: ESI, SEL

Home-Agent-Password

Description: Specifies the password that the Foreign Agent sends to the Home Agent during Ascend Tunnel Management Protocol (ATMP) operation.

Usage: Specify a text string of up to 20 characters.

Example: `set home-agent-password = mypw`

Dependencies: Under ATMP operation, all Mobile Clients accessing a single Home Agent must specify the same password.

Location: ATMP

See Also: Password

Home-Network-Name

Description: Specifies the name of the home network connection in an Ascend Tunnel Management Protocol (ATMP) configuration or in a Layer 2 Tunneling Protocol (L2TP) configuration for an L2TP Access Server (LAC).

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, accept the default of null.

Example: `set home-network-name = myhome`

Location: Connection *station* > Tunnel-Options

See Also: Agent-Mode, Agent-Type, Max-Tunnels, Password, Primary-Tunnel-Server, Profile-Type, Retry-Limit, Retry-Timeout, Secondary-Tunnel-Server, UDP-Port

Hops

Description: Specifies the distance to the destination network, in hops.

Usage: Specify a value from 1 to 8. The default is 8.

Location: IPX-Route *name*

See Also: Active-Route, Dest-Network, Name, Profile-Name, Server-Node, Server-Socket, Server-Type, Ticks

Host

Description: Specifies the Domain Name System (DNS) hostname or address of a host on the network, as follows:

- In the Auxiliary-Syslog [1] subprofile, the Host value specifies the host to which the unit sends Syslog messages for the second data stream. In the Auxiliary-Syslog [2] subprofile, the Host value specifies the host to which the unit sends Syslog messages for the third data stream.
- In a Connection profile, the Host value specifies the first host that the TAOS 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 SNTP servers.
- In the Log profile, the Host value specifies the host to which the unit sends Syslog messages for the first data stream.
- In the Terminal-Server profile, the Host value specifies the name, IP address, or X.121 address of the host to use for immediate service. When the TAOS unit authenticates a connection, it immediately directs the data stream to the specified host.

Usage: Your usage depends on the profile:

- In 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 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. The default is 0.0.0.0.
- For the Log profile, specify the IP address of a UNIX Syslog server. The default is 0.0.0.0.
- For the Terminal-Server profile, specify the name, IP address, or X.121 address of the host to use for immediate service. The default is a null string or null address.

Example: The following example specifies two login hosts:

```
admin> read connection fred
CONNECTION/fred read

admin> set tcp-clear-options host = mercury
admin> set tcp-clear-options host2 = venus
admin> write
CONNECTION/fred written
```

Dependencies: Consider the following:

- 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. If the connection to the next host fails, the system attempts to connect to the third host, and so forth. If all connection attempts fail, the session terminates and the TAOS unit returns a TCP connection error to the dial-in client.
- The settings in the Auxiliary-Syslog subprofile affect an individual Syslog stream, and override the values specified in the Log profile.

Location: Connection *station* > TCP-Clear-Options, Log, Log > Auxiliary-Syslog, IP-Global > SNTP-Info, Terminal-Server > Immediate-Mode-Options

See Also: Facility, Host2, Host3, Host4, Immediate-Mode-Options, Port, Port2, Port3, Port4, Save-Level, Save-Number, Service, Syslog-Enabled, TCP-Clear-Options

Host2

Description: Specifies the name of the second login host the TAOS unit attempts to use for TCP-Clear connections.

Usage: Specify the name of the second login host the TAOS unit attempts to use for TCP-Clear connections. You can enter up to 32 characters. The default is null.

Example: The following example specifies two login hosts:

```
admin> read connection fred
CONNECTION/fred read
admin> set tcp-clear-options host = mercury
admin> set tcp-clear-options host2 = venus
admin> write
CONNECTION/fred written
```

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. If the connection to the next host fails, the system attempts to connect to the third host, and so forth. If all connection attempts fail, the session terminates and the TAOS unit returns a TCP connection error to the dial-in client.

Location: Connection *station* > TCP-Clear-Options

See Also: Facility, Host, Host3, Host4, Immediate-Mode-Options, Port, Port2, Port3, Port4, Save-Level, Save-Number, Service, Syslog-Enabled, TCP-Clear-Options

Host3

Description: Specifies the name of the third login host the TAOS unit attempts to use for TCP-Clear connections.

Usage: Specify the name of the third login host the TAOS unit attempts to use for TCP-Clear connections. You can enter up to 32 characters. The default is null.

Example: The following example specifies three login hosts:

```
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 host3 = neptune
admin> write
CONNECTION/fred written
```


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. If the connection to the next host fails, the system attempts to connect to the third host, and so forth. If all connection attempts fail, the session terminates and the TAOS unit returns a TCP connection error to the dial-in client.

Location: Connection *station* > TCP-Clear-Options

See Also: Facility, Host, Host2, Host4, Immediate-Mode-Options, Port, Port2, Port3, Port4, Save-Level, Save-Number, Service, Syslog-Enabled, TCP-Clear-Options

Host4

Description: Specifies the name of the fourth login host the TAOS unit attempts to use for TCP-Clear connections.

Usage: Specify the name of the fourth login host the TAOS unit attempts to use for TCP-Clear connections. You can enter up to 32 characters. The default is null.

Example: The following example specifies four login hosts:

```
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 host3 = neptune
admin> set tcp-clear-options host4 = pluto
admin> write
CONNECTION/fred written
```

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. If the connection to the next host fails, the system attempts to connect to the third host, and so forth. If all connection attempts fail, the session terminates and the TAOS unit returns a TCP connection error to the dial-in client.

Location: Connection *station* > TCP-Clear-Options

See Also: Facility, Host, Host2, Host3, Immediate-Mode-Options, Port, Port2, Port3, Port4, Save-Level, Save-Number, Service, Syslog-Enabled, TCP-Clear-Options

Host-N

Description: Specifies the IP addresses of the Telnet hosts the TAOS unit displays in the terminal-server menu. You can specify up to four host addresses. If the user cannot use the terminal-server command-line interface, the hosts you specify are the only ones to which the user has access.

Usage: Specify an IP address in dotted decimal notation. Separate the optional subnet mask from the address by entering a forward slash. The default is 0.0.0.0.

Example: `set host-1 = 10.1.2.3/29`

Dependencies: If terminal services are disabled, Host-N does not apply. In addition, the TAOS unit ignores the host addresses if Remote-Configuration is set to Yes. If you want to specify more than four addresses, you must do so in Remote Authentication Dial-In User Service (RADIUS).

Location: Terminal-Server > Menu-Mode-Options

See Also: Menu-Mode-Options, Port-N, Remote-Configuration, Service-N, User-N

Host-Address

Description: Specifies the address to which the TAOS unit sends trap-PDUs.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0. If Host-Address is set to 0.0.0.0 and DNS (or YP/NIS) is supported, the TAOS 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.

Example: `set host-address = 10.2.3.4/24`

Location: Trap *host-name*

See Also: Alarm-Enabled, Community-Name, Host-Name, Port-Enabled, Security-Mode

Host-Name

Description: In an OSPF-NBMA-Neighbor profile, specifies the station name of a local Connection profile that defines the connection to the neighboring router. In a Table-Config subprofile, specifies a hostname for a local Domain Name System (DNS) table entry. In the Trap profile, specifies the hostname of a station running Simple Network Management Protocol (SNMP) manager utilities.

Usage: Enter a text string:

- In the OSPF-NBMA-Neighbor profile, specify the name of a local Connection profile.
- In the Table-Config subprofile, specify a hostname that begins with an alphabetic character and consists of fewer than 256 characters.
- In the Trap profile, specify a hostname of up to 16 characters.

For all profiles, the default is null.

Example: `set host-name = sparky`

Dependencies: For the Host-Name setting in the Table-Config subprofile, consider the following:

- You can specify either a local hostname or a hostname that contains the domain name. If your setting does not specify a domain name, the system appends the value specified by Domain-Name or Sec-Domain-Name.
- Trailing periods are ignored.

For the Host-Name setting in the Trap profile, consider the following:

- If Host-Address is set, the TAOS unit does not use the Host-Name value.
- The TAOS unit sends SNMP traps to the host you specify.
- When DNS or YP/NIS is supported, but Host-Address is not specified, the TAOS unit uses the hostname to look up the LAN address of the SNMP manager.

Location: IP-Global > DNS-Local-Table > Table-Config *N*, OSPF-NBMA-Neighbor *name*, Trap *host-name*

See Also: Alarm-Enabled, Community-Name, Domain-Name, Host-Address, IP-Address, Port-Enabled, Sec-Domain-Name, Security-Mode

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 *name*

See Also: Active-Enabled, Msg-Proc-Model, Notify-Tag-List, Security-Level, Security-Model, Security-Name, Tag, Target-Params-Name

Hosts-Info *N*

Description: Provides information about the menu displayed in Terminal-Server menu mode.

Usage: The Hosts-Info setting is read only.

Example: `hosts-info[1] = { 0.0.0.0 "" 0 telnet "" }`

Location: Ext-Tsrv

See Also: IP-Address, Port, Service, User

Hunt-Grp-Phone-Number-N

Description: Specifies a hunt-group telephone number associated with the line.

Usage: Specify a telephone number of up to 24 characters. The default is null.

Example: `set hunt-grp-phone-number-1 = 555-1212`

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface

Hunting-Mechanism

Description: Specifies the method by which the TAOS unit searches the primary (or secondary) list of transaction servers.

Usage: At present, the TAOS unit supports only the Cyclic setting, which specifies that the list is searched in cyclic order.

Location: Transaction-Server

See Also: Metric-Max, Selection-Timeout

/

ICMP-Reply-Directed-Bcast

Description: Specifies whether the TAOS unit responds to directed-broadcast Internet Control Message Protocol (ICMP) echo requests.

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

- Yes specifies that the TAOS unit responds to directed-broadcast ICMP echo requests.
- No specifies that the TAOS unit does not respond to directed-broadcast ICMP echo requests.

Example: `set icmp-reply-directed-bcast = no`

Location: IP-Global

See Also: Directed-Broadcast-Allowed

ID-Auth-Prefix

Description: Specifies the string inserted as a prefix to the telephone number presented to the Remote Authentication Dial-In User Service (RADIUS) server in Calling-Line ID (CLID) or Dialed Number Information Service (DNIS) authentication requests.

Usage: Specify up to 16 characters. The default is null.

Example: `set id-auth-prefix = test`

Location: External-Auth > Rad-Auth-Client

See Also: Auth-ID-Fail-Return-Busy, Auth-ID-Timeout-Return-Busy

IDI

Description: Specifies a hexadecimal code that identifies the subauthority that has allocated the address.

Usage: For DCC-AESA and ICD-AESA, the IDI is 2 bytes long (4 digits). For E164-AESA, the IDI is 8 bytes long, containing 16 digits that specify the E.164 address. The E.164 address can be up to 15 digits, so the system pads the number with leading zeros as required. The default is null.

Example: `set idi = abcd`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > ATM-Address > AESA-Address > IDP-Portion,
Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr > AESA-Address > IDP-Portion,
Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr > AESA-Address > IDP-Portion

See Also: AFI

Idle-Character-Delay

Description: Specifies the number of milliseconds of idle time to wait before forwarding data after receiving a character.

Usage: Specify a number from 0 to 30000. The default is 10000.

Example: `set idle-character-delay = 20000`

Location: Connection *station* > Visa2-Options

See Also: 1-Char-Sequence, 2-Char-Sequence

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 *name*

See Also: Auto-Logout, Idle-Mode, Idle-Timer

Idle-Mode

Description: Specifies whether the D channel looks for a flag pattern (01111110) or a mark pattern (11111111) as the idle indicator.

Usage: Specify one of the following values:

- Flag-Idle (the default) specifies that the D channel looks for a flag pattern.
- Mark-Idle specifies that the D channel looks for a mark pattern.

Example: `set idle-mode = flag-idle`

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Idle-Logout, Idle-Timer, Line-Interface

Idle-Timer

Description: In the Answer-Defaults and Connection profiles, specifies the number of seconds the TAOS unit waits before clearing a call when a session is inactive. 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. In the Answer-Defaults and Connection profiles, the default setting is 120 seconds. In the ATMP profile, the default is 0 (zero) minutes. In any of the three profiles, setting a value of 0 (zero) disables the idle timer, so that an idle call or tunnel is maintained indefinitely.

Example: `set idle-timer = 30`

Dependencies: Consider the following:

- In the Answer-Defaults and Connection profiles, the Idle-Timer value applies only to sessions in which the TAOS unit transmits data in packets through the router to the WAN connection.
- Idle-Timer does not apply to nailed-up or terminal-server connections. For a terminal-server connection, use TS-Idle-Timer.
- For H.323 Voice over IP (VoIP), the value of Idle-Timer can prevent fax/modem calls from timing out prematurely. By default, once a fax/modem call is initiated at the local unit, it will only wait 120 seconds (2 minutes) for a response to the call request from the distant unit. When the local unit doesn't receive a response within that time, the call is dropped. For real-time fax or transparent modem calls, set Idle-Timer to 0 (zero) to disable the idle timer and prevent the fax or modem calls from timing out.

Location: Answer-Defaults > Session-Info, ATMP, Connection *station* > Session-Options

See Also: Agent-Mode, Agent-Type, Call-Filter, Data-Filter, Filter-Persistence, Force-Fragmentation, MTU-Limit, Password, Retry-Limit, Retry-Timeout, Session-Info, Session-Options, TS-Idle-Timer, UDP-Port

IDP-Portion

Description: A subprofile containing settings for the IDP portion of an ATM End System Address (AESA).

Usage: With ATM-Interface as the working profile, enter `list svc-options atm-address aesa-address idp-portion`. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the IDP-Portion subprofile:

```
admin> list svc-options atm-address aesa-address idp-portion
[ in ATM-INTERFACE/ { { any-shelf any-slot 0 } 0 } :svc-options+
afi = " "
idi = " "
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > ATM-Address > AESA-Address,
Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr > AESA-Address,
Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr > AESA-Address

See Also: AFI, DSP-Portion, Format, IDI

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.

Dependencies: For IF-Remote-Address to apply, you must enable IP for the Connection profile.

Location: Connection *station* > IP-Options

See Also: IP-Options

Ignore-Def-Route

Description: Specifies whether the TAOS unit ignores the default route when applying Routing Information Protocol (RIP) updates to its routing table. The default route specifies a static route to another IP router, which is often a local router. When you configure the TAOS unit to ignore the default route, RIP updates do not modify the default route in the routing table.

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

- Yes specifies that the TAOS unit ignores advertised default routes. Lucent Technologies recommends that you specify Yes.
- No specifies that the TAOS unit can modify its default route on the basis of RIP updates.

Example: `set ignore-def-route = yes`

Location: IP-Global

See Also: Client-Default-Gateway, RIP

Ignore-ICMP-Redirects

Description: Specifies whether the TAOS unit processes incoming Internet Control Message Protocol (ICMP) redirect packets.

ICMP redirects are one of the oldest route-discovery mechanisms on the Internet, and one of the least secure, because they can be used to redirect packets dynamically. Most secure sites configure the TAOS unit to ignore redirect packets.

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

- Yes causes the TAOS unit to ignore ICMP redirect packets.
- No causes the TAOS unit to process ICMP redirect packets.

Example: `set ignore-icmp-redirects = yes`

Location: IP-Global

See Also: OSPF-ASE-Pref, OSPF-Pref, Preference, RIP-Pref, Static-Pref

Immediate-Mode-Options

Description: A subprofile containing terminal-server configuration options for immediate mode. In immediate mode, the TAOS unit makes a connection to an IP host immediately upon login.

Usage: With Terminal-Server as the working profile, list the Immediate-Mode-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Immediate-Mode-Options subprofile:

```
admin> list immediate-mode-options
[in TERMINAL-SERVER:immediate-mode-options]
service = none
telnet-host-auth = no
host = " "
port = 0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server

See Also: Host, Port, Service, Telnet-Host-Auth

Incoming-Caller-Addr

Description: A subprofile that enables you to specify the Asynchronous Transfer Mode (ATM) address of the remote end of the dial-in Switched Virtual Circuit (SVC) connection. This address is used to authenticate the incoming call.

Usage: With a Connection profile as the working profile, enter `list atm-options svc-options incoming-caller-addr`. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Incoming-Caller-Addr subprofile:

```
admin> list atm-options svc-options incoming-caller-addr
[in CONNECTION/robin:atm-options:svc-options:incoming-caller-addr]
numbering-plan = undefined
e164-native-address = " "
aesa-address = { undefined { " " " " } { " " " " " " } }
svc-address-info = " "
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: To configure an SVC that can be initiated by either a dial-in or dial-out call, specify the same ATM address in both the Incoming-Caller-Addr and Outgoing-Called-Addr subprofiles.

Location: Connection *station* > ATM-Options > SVC-Options

See Also: AESA-Address, E164-Native-Address, Numbering-Plan, SVC-Address-Info

Incoming-Call-Handling

Description: Specifies how the TAOS unit processes incoming calls on this line.

Usage: Specify one of the following values:

- Internal-Processing (the default) specifies that the unit itself processes incoming calls.
- SS7-Gateway-Processing specifies that the unit passes incoming call requests to an external signaling gateway. This setting is not currently supported.

Example: `set incoming-call-handling = internal-processing`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface, T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Signaling-Mode

Incoming-Fax-Port

Description: Specifies the TCP port on which the fax server listens for incoming fax data.

Usage: Specify a port number. The default is 0 (zero).

Example: `set incoming-fax-port = 100`

Dependencies: Incoming fax data is received from a fax machine redialer.

Location: IP-Fax

See Also: Outgoing-Fax-Port

Incoming-Procedure

Description: Specifies the type of incoming continuity checks to perform for all channels on a line.

Usage: Specify one of the following values:

- Loopback (the default) places the channel into loopback mode during the continuity test. This mode must be used if the line is provisioned for an incoming 4-wire continuity test.
- Transponder places the channel into Tone Transponder mode during the continuity test. In this mode, the channel can detect two tones: 2010Hz and 1780Hz (for a T1 line) or 2000Hz and 1780Hz (for an E1 line). When either tone is detected, the other one is returned. This mode should be used for lines provisioned for incoming 2-wire and 4-wire-to-2-wire continuity checks.

Example: `set incoming-procedure = transponder`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface > SS7-Continuity,
T1 {shelf-*N* slot-*N* *N*} > Line-Interface > SS7-Continuity

See Also: Outgoing-Procedure

Increment-Channel-Count

Description: Specifies the number of channels the TAOS unit adds for a manual or automatic bandwidth change during a call.

Usage: Specify an integer from 1 to 32. The default is 1.

Example: `set increment-channel-count = 3`

Location: Answer-Defaults > MPP-Answer, Connection *station* > MPP-Options

See Also: Add-Persistence, Bandwidth-Monitor-Direction, Base-Channel-Count, Decrement-Channel-Count, Dynamic-Algorithm, Maximum-Channels, Minimum-Channels, MPP-Answer, MPP-Options, Seconds-History, Sub-Persistence, Target-Utilization

Index

Description: In a Call-Route profile, specifies the address of the device that should receive the call if the call information matches other settings in the same Call-Route profile. In an Error profile, indicates the internal index of the entry.

In a Call-Route profile, the Index setting contains an entry number in the following format:

`{{{shelf slot port} logical-item } entry }`

The shelf number is always 1. A 0 (zero) in any field specifies *any*. That is, it matches any shelf, slot, port, or item. (For more information, see the description for Interface-Address.)

In an Error profile, the Index number is an integer.

Usage: If you have only one Call-Route profile for the specified address, accept the default of 0 (zero) for the entry number. When you specify the same address in more than one Call-Route profile, you must assign a nonzero entry number to distinguish the entries from one another in the database. You can assign any number, as long as it is unique for each entry. The entry numbers do not have to be sequential.

You can use the Index setting to clone Call-Route profiles. Just read an existing profile, and change the device address. You can also create multiple entries for a device by reading an existing profile and setting a new entry number.

In an Error profile, the Index setting is read only.

Example: `set index entry-number = 1`

Location: Call-Route {{{shelf-*N* slot-*N* *N*} *N*} *N*}, Error *index*

See Also: Call-Route-Type, Entry-Number, Interface-Address, Phone-Number, Preferred-Source, Trunk-Group

Inet-Profile-Type

Description: Specifies whether the nailed-up profile is a local profile or a Remote Authentication Dial-In User Service (RADIUS) profile.

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 *station*

See Also: Desired-State, Desired-Trip-State, Device-Address, SNMP-Interface, Station

Info

Description: Specifies the PPP startup message. If you specify a value, the TAOS unit displays it when an interactive user initiates a PPP session from the terminal-server interface.

Usage: Specify one of the following values:

- None specifies that no startup message appears.
- Mode-PPP specifies that the startup message is PPP Mode.
- Session-PPP (the default) specifies that the startup message is PPP Session.

Example: `set info = mode-ppp`

Dependencies: If terminal services are disabled, Info does not apply.

Location: Terminal-Server > PPP-Mode-Configuration,
Terminal-Server > SLIP-Mode-Configuration

See Also: IP-Add-Msg, PPP, PPP-Mode-Configuration

Init-Banner N

Description: Specifies the initial-banners for terminal-server logins, downloaded from Remote Authentication Dial-In User Service (RADIUS).

Usage: The Init-Banner setting is read only.

Example: `init-banner [1] = "Welcome"`

Location: Ext-Tsrv

See Also: Banner N, Hosts-Info N

Initial-Jitter-Buffer-Size

Description: Specifies the initial jitter buffer size for Voice over IP (VoIP) calls when the TAOS unit is configured to perform adaptive call jitter buffering. At startup, the jitter buffer is set to the number of packets specified by Initial-Jitter-Buffer-Size. During a call, the TAOS unit adjusts the jitter buffer to accommodate the number of audio packets on the basis of the incoming audio packet volume.

Usage: Specify a number from 1 to 18 (packets). The default is 2.

Example: `set initial-jitter-buffer-size = 5`

Dependencies: Consider the following:

- Changes to Initial-Jitter-Buffer-Size become effective with the next VoIP call.
- When you use adaptive jitter buffers, the minimum jitter buffer size might be less than the value assigned to Initial-Jitter-Buffer-Size. Under the appropriate conditions, adaptive jitter buffers might shrink to only 1 packet in size from the Initial-Jitter-Buffer-Size.

Location: VoIP {x y}

See Also: Ena-Adap-Jitter-Buffer, Max-Jitter-Buffer-Size

Input-Filters

Description: A subprofile containing 12 input-filter configuration subprofiles.

Usage: With a Filter profile as the working profile, use the List command to display the input filters in the Input-Filters subprofile.

Example: To list the contents of the Input-Filters subprofile:

```
admin> list input-filters
[in FILTER/test:input-filters]
input-filters[1] = { no no generic-filter { 0 0 no no +
input-filters[2] = { no no generic-filter { 0 0 no no +
input-filters[3] = { no no generic-filter { 0 0 no no +
input-filters[4] = { no no generic-filter { 0 0 no no +
...
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name*

See Also: Filter-Name, Input-Filters N, Output-Filters, Output-Filters N

Input-Filters N

Description: A subprofile containing the first level of an input-filter specification.

Usage: With a Filter profile as the working profile, use the List command to display an input filter. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Input-Filters *N* subprofile:

```
admin> list input-filters 1
[ in FILTER/test: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 +
route-filter = { 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0 none }
ipx-filter = { 00:00:00:00 00:00:00:00 00:00:00:00:00:00:00:00 +
tos-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 +
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name* > Input-Filters

See Also: Forward, Gen-Filter, IP-Filter, TOS-Filter (subprofile), Type, Valid-Entry

Input-IPX-SAP-Filters

Description: A subprofile that defines up to eight input filters for Service Advertising Protocol (SAP) packets. The TAOS unit applies input filters to all SAP packets it receives. Input filters screen advertised services and exclude them from (or include them in) the service table as specified by the filter conditions.

Usage: With an IPX-SAP-Filter as the working profile, use the List command to display one of the input filters for SAP packets. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Input-IPX-SAP-Filters[1] subprofile:

```
admin> list input-ipx-sap-filters 1
[ in IPX-SAP-FILTER/test:input-ipx-sap-filters[1]]
valid-filter = no
type-filter = exclude
server-type = 00:00
server-name = " "
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IPX-SAP-Filter

See Also: Server-Name, Server-Type, Type-Filter, Valid-Filter

Insert-Calling-Party-Addr

Description: Enables or disables insertion of the calling-party address in outgoing calls.

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

- Yes specifies that the system includes the calling-party address in outgoing calls.
- No specifies that the system does not include the calling-party address in outgoing calls.

Example: `set insert-calling-party-addr = no`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } > SVC-Options

Inter-Digit-Time-Out

Description: Specifies how long a MultiVoice gateway waits after receiving the last digit of a dial string before declaring DNIS/ANI collection complete.

Usage: For all configurations except those using E1 MRC R2 signaling, specify a number from 100ms to 6000ms. For configurations supporting E1 MRC R2 signaling, specify a number from 200ms to 6000ms. The default is 3000ms (3 seconds).

Example: `set inter-digit-time-out = 6000`

Dependencies: E1 MFC-R2 signaling is country specific. The Signaling-Mode and Country values must be set for the country-appropriate signaling in order for the MultiVoice gateway to properly detect dialed digits.

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Country, Signaling-Mode

Interface-Address

Description: Identifies an interface address in the following format:

`{ {shelf slot item} logical-item }`

This format specifies the physical address and a logical item. The shelf number is always 1. For information about the physical address format, see the description for Physical-Address. The logical item number is 0 (zero), except when the device is further divided, such as for a channelized T1 line. For a T1 line, each channel can have its own logical item number (1–24).

In an ATMSVC-Route profile, the Interface-Address setting specifies the interface address of the ATM-Interface profile.

Usage: In most cases, the Interface-Address value is obtained from the system. However, you can clone a profile by reading an existing one and changing its device address. To modify the value, use the List and Set commands.

Example: admin> **list interface-address**

```
[in ATALK-INTERFACE/{ { shelf-1 slot-8 } 5 }:interface-address]  
physical-address = { shelf-1 slot-8 5 }  
logical-item = 0
```

admin> **set logical-item = 11**

Or, you can use only the Set command:

admin> **set interface-address logical-item = 11**

Location: Atalk-Interface {shelf-*N* slot-*N* *N*}, ATM-Interface { {shelf-*N* slot-*N* *N*} *N* },
ATMSVC-Route *name*, Ether-Info {shelf-*N* slot-*N* *N*}, Ethernet {shelf-*N* slot-*N* *N*},
IP-Interface { {shelf-*N* slot-*N* *N*}, IPX-Global, IPX-Interface {shelf-*N* slot-*N* *N*}

See Also: Device-Address, Item-Number, Physical-Address, Shelf, Slot

Internal-Call-Processing

Description: Specifies how the TAOS unit processes incoming calls on a T1 line.

Usage: For the Internet Call Diversion (ICD) for softswitch signaling gateway, specify Internal-Processing.

Example: **set internal-call-processing = internal-processing**

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Signaling-Mode

Interval

Description: Specifies the number of seconds between signaling heartbeat messages.

Usage: Specify a number from 0 to 86400. The default is 3.

Example: **set interval = 5**

Location: SS7-Gateway > Signaling Heartbeat

See Also: Enabled

Inter-VRouter

Description: Specifies the name of a Virtual Router (VRouter) to use as the route's next hop. Packets destined for the Dest-Address are sent to the specified VRouter, which consults its routing table to route the packets.

Usage: Specify the name of a VRouter. The default is null.

Example: **set inter-vrouter = next-router**

Dependencies: You must set Gateway-Address to 0.0.0.0 for the Inter-VRouter setting to apply.

Location: IP-Route *name*

See Also: Dest-Address, Gateway-Address, VRouter

IP-Add-Msg

Description: Specifies a string that precedes the IP address when a terminal-server user initiates a PPP session.

Usage: Specify a text string of up to 20 characters. The default is `IP address is:`

Example: `set ip-add-msg = "Your IP address is: "`

Dependencies: If terminal services are disabled, IP-Add-Msg does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Info, Terminal-Mode-Configuration

IP-Address

Description: Specifies an IP address.

- In an IP-Interface profile, assigns an IP address to an Ethernet interface.
- In an OSPF-NBMA-Neighbor profile, specifies the IP address of the neighboring router.
- In a Static-Address subprofile, specifies the IP address to be assigned to a client with the associated Ethernet-Address.
- In a Table-Config subprofile, specifies an IP address for a local Domain Name System (DNS) table entry.
- In an Error profile, indicates the address or subnet from which an operator reset was requested.
- In a Hosts-Info *N* subprofile, specifies the address displayed in the list of hosts when the terminal server is in menu mode.

Usage: In all but the Error profile, specify an IP address in dotted decimal notation. The default is 0.0.0.0. In an Error profile, the IP-Address setting is read only.

Example: `set ip-address = 10.2.3.4/24`

Dependencies: Consider the following:

- The TAOS unit supports an internal soft IP interface that is always available. It is associated only with the primary controller and is hidden from the secondary controller. The TAOS system sets up the soft IP interface after you power on the unit and a controller becomes primary. If a switchover occurs and the secondary controller becomes primary, the soft IP interface is initialized and associated with the new primary controller. The soft IP interface address is reachable as long as one IP interface on the TAOS unit is operational.
- The IP-Interface profile with the zero index is reserved for the soft IP interface. You activate the soft interface by entering an address for `{ {any-shelf any-slot 0} 0 }` in the IP-Address setting.
- If Routing Information Protocol (RIP) is enabled, the TAOS unit advertises the soft IP interface address as a host route (with a prefix length of /32) using the loopback interface. If RIP is not enabled, routers one hop away from the TAOS unit must have a static route to the soft interface address.

- To allow the Auto-Update feature to build the local DNS table, accept the default for IP-Address in the Table-Config subprofile.
- In a Static-Address subprofile, you can define up to 100 pairs of IP and Ethernet Media Access Control (MAC) addresses. Only the host with a specified MAC address can obtain the associated IP address.

Location: Error, Ext-Tsrv > Hosts-Info *N*, IP-Global > DNS-Local-Table> Table-Config *N*, IP-Global > DHCP-Server > Static-Address, IP-Interface { {shelf-*N* slot-*N*} *N* }, OSPF-NBMA-Neighbor *name*

See Also: Auto-Update, Ethernet, Host-Name, IP-Direct, IP-Route, IP-Routing-Enabled

IP-Answer

Description: A subprofile containing default settings for IP calls, regardless of their encapsulation protocol.

Usage: With Answer-Defaults as the working profile, list the IP-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the IP-Answer subprofile:

```
admin> list ip-answer
[in ANSWER-DEFAULTS:ip-answer]
enabled = yes
vj-header-prediction = yes
assign-address = yes
routing-metric = 1
private-route-profile-required = no
pool-for-async-framed-user = 0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Assign-Address, Enabled, Private-Route-Profile-Required, Routing-Metric, VJ-Header-Prediction

IP-Direct

Description: Specifies the address to which the TAOS unit immediately directs all incoming IP traffic on the link, without consulting the IP-routing table. If you enable Routing Information Protocol (RIP) updates in both directions, the unit forwards all RIP packets to the IP address you specify.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0, which disables IP-Direct routing.

Example: `set ip-direct = 10.1.2.3/24`

Dependencies: When you use IP-Direct routing, a remote user cannot establish a Telnet session directly to the TAOS unit.

Location: Connection *station* > IP-Options

See Also: IP-Address, IP-Options, IP-Route, IP-Routing-Enabled

IP-Fax

Description: A profile that enables you to configure the TAOS unit to interact with a third-party fax server.

Usage: Use the Read and List commands to make IP-Fax the working profile and list its contents. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To make IP-Fax the working profile and list its contents:

```
admin> read ip-fax
[IPFAX read]

admin> list
ip-fax-enabled = no
outgoing-fax-port = 10001
server-login = ""
server-password = ""
incoming-fax-port = 0
all-calls-are-fax = no
fax-dnis = ["" "" "" "" "" "" "" "" ""]
fax-did = ["" "" "" "" "" "" "" "" ""]
fax-servers = [0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0]
dialer-type = mitel
fax-incoming-call-type = redialer
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
IP-FAX written
```

See Also: All-Calls-Are-Fax, Dialer-Type, Fax-DNIS, Fax-Incoming-Call-Type, Fax-Servers, Incoming-Fax-Port, IP-Fax-Enabled, Outgoing-Fax-Port, Server-Login, Server-Password

IP-Fax-Enabled

Description: Enables or disables IP fax support on the TAOS unit.

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

- Yes enables IP fax support.
- No disables IP fax support.

Example: `set ip-fax-enabled = yes`

Location: IP-Fax

See Also: Fax-DNIS, Fax-Servers

IP-Filter

Description: A subprofile containing an IP filter specification. An IP-Filter subprofile is in an Input-Filters *N* or Output-Filters *N* subprofile.

Usage: With a Filter profile as the working profile, list an IP-Filter subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the IP-Filter subprofile:

```
admin> list input-filters 1 ip-filter
[In FILTER/test:input-filters[1]:ip-filter]
protocol = 0
source-address-mask = 255.255.255.192
source-address = 200.100.50.128
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
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name* > Input-Filters > Input-Filters *N*,
Filter *filter-name* > Output-Filters > Output-Filters *N*

See Also: Dest-Address, Dest-Address-Mask, Dest-Port, Dst-Port-Cmp, Input-Filters *N*, Output-Filters *N*, Protocol, Source-Address, Source-Address-Mask, Source-Port, Src-Port-Cmp, TCP-Estab

IP-Global

Description: A profile that contains global settings for TCP/IP.

Usage: Use the Read and List commands to make IP-Global the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make IP-Global the working profile and list its contents:

```
admin> read ip-global
IP-GLOBAL read
```

```
admin> list
[ in IP-GLOBAL ]
domain-name = abc.com
dns-primary-server = 10.65.212.178
dns-secondary-server = 0.0.0.0
system-ip-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-base-address = [ 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 ]
pool-name = ""
rip-policy = poison-rvrs
summarize-rip-routes = no
bootp-enabled = no
ignore-icmp-redirects = no
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 = ""
shared-prof = no
dns-list-attempt = no
static-pref = 100
rip-pref = 100
ospf-pref = 10
ospf-ase-pref = 150
ospf-global = { yes }
rip-tag = c8:00:00:00
rip-ase-type = 1
pool-ospf-adv-type = type-1
iproute-cache-enable = yes
iproute-cache-size = 0
snmp-info = { no utc+0000 [ 0.0.0.0 0.0.0.0 0.0.0.0 ] }
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
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
ipport-cache-enable = yes
dns-local-table = [ no no table-config { "" 0.0.0.0. ""
0.0.0.0.+
icmp-reply-directed-bcast = yes
bootp-relay = [ no bootp-servers { 0.0.0.0 0.0.0.0 } ]
rip-trigger = yes
suppress-host-routes = no
default-filter-cache-time = 0
send-icmp-dest-unreachable = yes
default-prt-cache-time = 0
pool-chaining = no
throttle-no-port-match-udp-traffic-on-slot = no

```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```

admin> write
IP-GLOBAL written

```

See Also: Allow-As-Client-DNS-Info, Assign-Count, BOOTP-Enabled, Client-Primary-DNS-Server, Client-Secondary-DNS-Server, Default-Filter-Cache-Time, Default-Prt-Cache-Time, Dialout-Poison, DNS-List-Attempt, DNS-List-Size, DNS-Local-Table, DNS-Primary-Server, DNS-Secondary-Server, Domain-Name, Drop-Source-Routed-IP-Packets, Finger, ICMP-Reply-Directed-Bcast, Ignore-Def-Route, Ignore-ICMP-Redirects, IPPort-Cache-Enable, IPRoute-Cache-Enable, IPRoute-Cache-Size, Must-Accept-Address-Assign, NetBIOS-Primary-NS, NetBIOS-Secondary-NS, OSPF-ASE-Pref, OSPF-Global, OSPF-Pref, Pool-Base-Address, Pool-Chaining, Pool-Summary, RARP-Enabled, RIP-ASE-Type, RIP-Policy, RIP-Pref, RIP-Tag, RIP-Trigger, Sec-Domain-Name, Send-ICMP-Dest-Unreachable, Shared-Prof, Static-Pref, Summarize-RIP-Routes, Suppress-Host-Routes, System-IP-Addr, Telnet-Password, Throttle-No-Port-Match-UDP-Traffic-On-Slot, UDP-Cksum, User-Profile

IP-Interface

Description: A profile containing configuration options for an IP interface.

Each packet-handling slot card operates as a router subsystem with its own local interface table. The unit's router card holds the global interface table. The interface address of an IP-Interface profile is the local address on a slot card. Each interface has its own IP address.

When the TAOS unit generates IP packets, the packets have the source address of the IP interface on which they are forwarded. If the unit receives IP packets destined for one of its IP addresses, it accepts the packets, even if they arrive on a different interface and the destination-address interface is not active.

Usage: You can specify up to 16 IP-Interface profiles for each installed Ethernet card. Each profile specifies a single IP address.

The TAOS unit creates a default IP-Interface profile when it first detects the presence of an Ethernet card or a shelf-controller's Ethernet port. For example, for the first Ethernet port on a card in slot 12, the default IP-Interface profile uses the following index:

```
{ {1 12 1} 0 }
```

The index consists of a physical address and a logical-item number in the following format:

```
{{shelf slot item} logical-item}
```

The shelf number is always 1. The logical item number addresses a specific logical interface or port. The logical item number is 0 (zero), except when you configure multiple interfaces or the device supports multiple channels. For example, another IP-Interface profile for {1 12 1} might use the following index:

```
{ {1 12 1} 1 }
```

The logical-item numbers do not have to be consecutive, but they must be unique.

To specify an interface-independent address, create an IP-Interface profile with the default index. The IP-Interface profile with the default index is reserved for the interface-independent IP address.

Example: The following commands set the soft interface address to 11.168.7.100:

```
admin> new ip-interface
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } read
admin> set ip-address = 11.168.7.100
admin> write
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } written
```

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.

See Also: Directed-Broadcast-Allowed, Interface-Address, IP-Address, Management-Only-Interface, Multicast-Allowed, Multicast-Group-Leave-Delay, Multicast-Rate-Limit, OSPF, Proxy-Mode, RIP2-Use-Multicast, RIP-Mode

IP-Options

Description: A subprofile containing IP-routing settings.

Usage: With a Connection profile as the working profile, list the IP-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the IP-Options subprofile:

```
admin> list ip-options
[in CONNECTION/tim: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
multicast-allowed = no
address-pool = 0
ip-direct = 0.0.0.0
rip = routing-off
ospf-options = { no 0.0.0.0 normal 10 30 120 5 simple ***** +
multicast-rate-limit = 100
client-dns-primary-addr = 0.0.0.0
client-dns-secondary-addr = 0.0.0.0
client-dns-addr-assign = yes
client-wins-primary-addr = 0.0.0.0
client-wins-secondary-addr = 0.0.0.0
client-wins-addr-assign = yes
client-default-gateway = 0.0.0.0
route-filter = ""
if-remote-address = 0.0.0.0
multicast-group-leave-delay = 0
tos-options = { no 00 normal input }
tos-filter = ""
source-ip-check = no
private-route-profile-required = no
private-route-table = ""
auth-for-async-framed-user = required
max-pap-auth-retry = 0
pool-for-async-framed-user = 0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: IP-routing calls must be enabled in the Answer-Defaults profile.

Location: Connection *station*

See Also: Active, Address-Pool, Apply-To, Auth-For-Async-Framed-User, Client-Default-Gateway, Client-DNS-Addr-Assign, Client-DNS-Primary-Addr, Client-DNS-Secondary-Addr, Client-WINS-Addr-Assign, Client-WINS-Primary-Addr, Client-WINS-Secondary-Addr, Down-Preference, IP-Direct, IP-Routing-Enabled, Local-Address, Max-PAP-Auth-Retry, Multicast-Allowed, Multicast-Group-Leave-Delay, Multicast-Rate-Limit, OSPF-Options, Pool-For-Async-Framed-User, Precedence, Preference, Private-Route, Private-Route-Profile-Required, Private-Route-Table, Remote-Address, RIP, Routing-Metric, Source-IP-Check, Temporary-Route, Type-of-Service, VJ-Header-Prediction

IPPort-Cache-Enable

Description: Enables or disables card-to-card IP packet forwarding on the basis of the packet destination IP address and port.

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

- Yes specifies that packets destined for the TAOS unit itself are correctly forwarded from the receiving slot card to the destination slot card, bypassing the router.
- No specifies that packets destined for the TAOS unit itself are delivered to the router, and then forwarded to the digital modem card.

Example: `set ipport-cache-enable = no`

Location: IP-Global

See Also: IPRoute-Cache-Enable, IPRoute-Cache-Size

IP-Route

Description: A profile containing the information required by the IP router for setting up static routes. The TAOS unit passes the static routes to the router at startup, and updates the routing table whenever a route changes.

Usage: Use the Read and List commands to make IP-Route the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the IP-Route profile default the working profile and list its contents:

```
admin> read ip-route default
IP-ROUTE/default read

admin> list
[in IP-ROUTE/default]
name* = default
dest-address = 0.0.0.0/0
gateway-address = 0.0.0.0
metric = 1
cost = 1
preference = 100
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
private-route = yes
active-route = no
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
IP-ROUTE/default written
```

See Also: Active-Route, ASE-Tag, ASE-Type, Cost, Dest-Address, Gateway-Address, Metric, Nailed-Up-Group, Preference, Private-Route, Third-Party

IPRoute-Cache-Enable

Description: Enables or disables route caches.

A route cache enables a slot card to route IP packets to another slot, reducing the route-processing overhead on the shelf controller. The shelf controller is still responsible for managing routing protocols and the route caches themselves, but each slot card is able to check a small IP cache and route packets to a destination slot. When a slot card receives an IP packet for which it has no cache entry, it forwards that packet to the shelf controller, which routes it to the proper slot. The shelf controller then writes a cache entry and, using the control bus, downloads it to the route cache of each slot card.

Usage: Specify Yes or No. The default is Yes, which is the recommended setting.

- Yes enables the router on the shelf controller to offload some route processing to the slot cards.
- No specifies that all route processing occurs on the shelf controller.

Example: `set iproute-cache-enable = yes`

Location: IP-Global

See Also: IPRoute-Cache-Size

IPRoute-Cache-Size

Description: Specifies the limit for the number of cache entries in slot-card route caches.

Usage: Specify an integer. The default is 0 (zero), which sets no limit on cache size. In general, no limit is required. But you can set one if you need to control memory usage.

Example: `set iproute-cache-size = 16`

Location: IP-Global

See Also: IPRoute-Cache-Enable

IP-Routing-Enabled

Description: Enables or disables the routing of IP data packets for the connection.

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

- Yes enables IP routing for the link. For your setting to have any effect, IP routing must be enabled on both the dialing and answering sides of the link.
- No disables IP routing for the link.

Example: `set ip-routing-enabled = yes`

Location: Connection *station* > IP-Options

See Also: IP-Address, IP-Global, IP-Interface, IP-Options, IP-Route

IPSec

Description: A profile containing specifications for an IP Security (IPSec) endpoint and the IPSec transforms to use on the data stream transmitted to and from that endpoint.

Usage: Use the Read and List command to make IPSec the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the IPSec profile `greg` the working profile and list its contents:

```
admin> read ipsec greg
IPSEC/greg read

admin> list
[ in IPSEC/greg ]
name* = greg
active = no
encap-mode = transport
tunnel-address = 0.0.0.0
send-ah = { no 1 none no }
recv-ah = { no 1 none no }
send-esp = { no 1 0 none 32 none no }
recv-esp = { no 1 0 none 32 none no }
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
IPSEC/greg written
```

See Also: Active, Encap-Mode, Name, Recv-AH, Recv-ESP, Send-AH, Send-ESP, Tunnel-Address

IPSec-Profile

Description: Specifies the name of the IPSec profile that defines the transforms and endpoints for IP Security (IPSec) operations on traffic crossing Layer 2 Tunneling Protocol (L2TP) tunnels to the specified endpoint.

Usage: Specify the name of an IPSec profile. The default is null.

Example: `set ipsec-profile = myprofile`

Dependencies: If the Tunnel-Server profile does not specify an IPSec profile name, a normal, nonsecure UDP socket is assigned to the L2TP session. If an IPSec profile name is specified, a new UDP socket is opened and assigned the specified profile settings.

Location: Tunnel-Server *name*

See Also: IPSec

IPX-Answer

Description: A subprofile containing default settings for IPX calls.

Usage: With Answer-Defaults as the working profile, list the IPX-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the IPX-Answer subprofile:

```
admin> list ipx-answer
[in ANSWER-DEFAULTS:ipx-answer]
enabled = yes
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Enabled

IPX-Dialin-Pool

Description: Specifies a virtual IPX network that the TAOS unit assigns to dial-in NetWare clients.

Dial-in clients do not belong to an IPX network. Therefore, to establish a routing connection, the TAOS unit must assign each client an IPX network number. The unit advertises the route to the virtual network and assigns it as the network address for dial-in clients. The dial-in Netware client must accept the network number, although it can provide its own node number. If the client does not have a unique node address, the TAOS unit assigns the node address as well.

Usage: Specify an IPX network number that is unique in the IPX routing domain. The default is 00:00:00:00.

Example: `set ipx-dialin-pool = 00000001`

Dependencies: If IPX routing is globally disabled, IPX-Dialin-Pool does not apply. If you do not specify a dial-in pool in a VRouter profile, the unit uses the global VRouter pool specified in the IPX-Global profile.

Location: IPX-Global, VRouter *name*

See Also: Interface-Address, IPX-Frame, IPX-Net-Number, IPX-Options, IPX-Route, IPX-Routing-Enabled, IPX-SAP-Filter-Name, IPX-Type-20

IPX-Filter

Description: A subprofile containing an IPX filter specification. A Filter profile contains several levels of subprofiles. An IPX-Filter subprofile is in an Input-Filters *N* or Output-Filters *N* subprofile.

Usage: When a Filter profile is the working profile, list an IPX-Filter subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the IPX-Filter subprofile:

```
admin> list input-filters 1 ipx-filter
[in FILTER/test:input-filters[1]:ipx-filter]
src-net-address = 00:00:00:00
dest-net-address = 00:00:00:00
src-node-address = 00:00:00:00:00:00
dest-node-address = 00:00:00:00:00:00
src-socket = 00:00
src-socket-cmp = none
dest-socket = 0
dst-socket-cmp = none
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name* > Input-Filters > Input-Filters *N*,
Filter *filter-name* > Output-Filters > Output-Filters *N*

See Also: Dest-Net-Address, Dest-Node-Address, Dest-Socket, Dst-Socket-Cmp, Input-Filters *N*, Output-Filters *N*, Src-Net-Address, Src-Node-Address, Src-Socket, Src-Socket-Cmp

IPX-Frame

Description: Specifies the type of packet frame the TAOS unit will route on an Ethernet connection.

Usage: Specify one of the following values:

- None (the default) disables IPX-specific features. If you choose this setting, the TAOS unit can route IPX, but without automatic Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) handling.
- 802.2 (NetWare 3.12 or later) specifies that the IPX clients and servers on the local Ethernet cable follow the IEEE 802.2 protocol for the Media Access Control (MAC) header. The frame contains the Logical Link Control (LLC) header in addition to the MAC header.
- 802.3 (for NetWare 3.11 or earlier) specifies that IPX clients and servers on the local Ethernet cable follow the IEEE 802.3 protocol for the MAC header, also called Raw 802.3. The frame contains the MAC header, but not the LLC header.

- SNAP specifies that the IPX clients and servers on the local Ethernet network follow the SubNetwork Access Protocol (SNAP) for the MAC header. This specification includes the IEEE 802.3 protocol format plus additional information in the MAC header.
- Enet-II specifies that IPX clients and servers on the local Ethernet network follow the Ethernet II protocol for the MAC header.

Example: `set ipx-frame = 802.2`

Dependencies: Consider the following:

- If the TAOS unit does not route IPX on the specified interface, or if IPX routing is globally disabled, IPX-Frame does not apply.
- The TAOS unit routes only the IPX frame type specified by IPX-Frame. If a NetWare server transmits IPX in a different frame type, the TAOS unit drops the packets.

Location: IPX-Interface {shelf-*N* slot-*N* *N*}

See Also: Interface-Address, IPX-Dialin-Pool, IPX-Net-Number, IPX-Options, IPX-Route, IPX-Routing-Enabled, IPX-SAP-Filter-Name, IPX-Type-20

IPX-Global

Description: A profile that contains global settings for IPX.

Usage: Use the Read and List commands to make IPX-Global the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make IPX-Global the working profile and list its contents:

```
admin> read ipx-global
IPX-GLOBAL read

admin> list
[in IPX-GLOBAL]
interface-address = { { any-shelf any-slot 0 } }
ipx-routing-enabled = no
ipx-dialin-pool = 00:00:00:00
global-vrouter = main
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
IPX-GLOBAL written
```

See Also: Global-VRouter, Interface-Address, IPX-Dialin-Pool, IPX-Routing-Enabled

IPX-Header-Compression

Description: Specifies whether the TAOS unit should use IPX header compression on the connection if the encapsulation method in use supports it.

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

- Yes specifies that the TAOS unit should use IPX header compression if the encapsulation method supports it.
- No specifies that the TAOS unit should not use IPX header compression.

Example: `set ipx-header-compression = yes`

Dependencies: If the TAOS unit does not route IPX on the connection, or if IPX routing is globally disabled, IPX-Header-Compression does not apply.

Location: Connection *station* > IPX-Options

See Also: Dial-Query, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Alias, Net-Number, Peer-Mode, RIP, SAP, SAP-Filter

IPX-Interface

Description: A profile that contains configuration options for an IPX interface.

Usage: Use the Read and List commands to make IPX-Interface the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: On a MAX TNT unit:

```
admin> read ipx-interface { { shelf-1 controller 1 } 0 }
IPX-INTERFACE/{ { shelf-1 controller 1 } 0} read
admin> list
[in IPX-INTERFACE/{ { shelf-1 controller 1 } 0}]
interface-address* = { { shelf-1 controller 1 } 0 }
ipx-routing-enabled = no
ipx-frame = none
ipx-net-number = 00:00:00:00
ipx-type-20 = no
ipx-sap-filter-name = " "
vrouter = " "
admin> set ipx-routing-enabled = yes
admin> write
IPX-INTERFACE written
```

On an APX 8000 unit:

```
admin> read ipx-interface { { shelf-1 left-controller 1 } 0 }
IPX-INTERFACE/{ { shelf-1 left-controller 1 } 0} read

admin> list
[in IPX-INTERFACE/{ { shelf-1 left-controller 1 } 0}]
interface-address* = { { shelf-1 left-controller 1 } 0 }
ipx-routing-enabled = no
ipx-frame = none
ipx-net-number = 00:00:00:00
ipx-type-20 = no
ipx-sap-filter-name = ""
vrouter = ""

admin> set ipx-routing-enabled = yes

admin> write
IPX-INTERFACE written
```

See Also: Interface-Address, IPX-Frame, IPX-Net-Number, IPX-Routing-Enabled, IPX-SAP-Filter-Name, IPX-Type-20, VRouter

IPX-Net-Number

Description: Specifies the IPX network number of the remote router.

Usage: Specify the IPX network number of the remote device only when the router requires that the TAOS unit know its network number before connecting. If you specify a value for IPX-Net-Number, the TAOS unit creates a static route to the device. In addition, the unit becomes a seed router, and other routers can learn the IPX network number from it.

If there are other NetWare routers on the LAN interface, the IPX number assigned to the TAOS unit for that interface must be consistent with the number in use by the other routers. The best way to ensure consistency is to accept the default null address for IPX-Net-Number. The null address causes the TAOS unit to learn its network number from another router on the interface, or from the Routing Information Protocol (RIP) packets received from the local IPX server.

The default of 00000000 is appropriate for most installations. If you accept the default, the TAOS unit does not advertise the route until it makes a connection to the remote network.

Dependencies: If the TAOS unit does not route IPX on the specified interface, or if IPX routing is globally disabled, IPX-Net-Number does not apply.

Location: IPX-Interface {shelf-*N* slot-*N* *N*}

See Also: Interface-Address, IPX-Dialin-Pool, IPX-Frame, IPX-Options, IPX-Route, IPX-Routing-Enabled, IPX-SAP-Filter-Name, IPX-Type-20

IPX-Options

Description: A subprofile containing settings for IPX routing.

Usage: With a Connection profile as the working profile, list the IPX-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the IPX-Options subprofile:

```
admin> list ipx-options
[in CONNECTION/tim:ipx-options]
ipx-routing-enabled = no
peer-mode = router-peer
rip = both
sap = both
dial-query = no
net-number = 00:00:00:00
net-alias = 00:00:00:00
sap-filter = ""
ipx-sap-hs-proxy = no
ipx-sap-hs-proxy-net = [000000]
ipx-header-compression = yes
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: To globally enable IPX routing, set IPX-Routing-Enabled to Yes in the IPX-Global profile. To enable IPX routing for an interface, set IPX-Routing-Enabled to Yes in the IPX-Interface profile.

Location: Connection *station*

See Also: Dial-Query, IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Alias, Net-Number, Peer-Mode, RIP, SAP, SAP-Filter

IPX-Route

Description: A profile containing the information required by the IPX router to set up static routes. The TAOS unit passes the static routes to the router at startup, and updates the routing table whenever a route changes.

Usage: Use the Read and List commands to make IPX-Route the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the IPX-Route profile default the working profile and save your changes:

```
admin> read ipx-route default
IPX-ROUTE/default read
```

```
admin> list
[in IPX-ROUTE/default]
name* = default
server-type = 00:00
dest-network = 00:00:00:00
server-node = 00:00:00:00:00:00
server-socket = 00:00
hops = 8
ticks = 12
profile-name = " "
active-route = yes
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
IPX-ROUTE/default written
```

See Also: Active-Route, Dest-Network, Hops, Name, Profile-Name, Server-Node, Server-Socket, Server-Type, Ticks

IPX-Routing-Enabled

Description: Enables or disables the routing of IPX data packets, as follows:

- In the IPX-Global profile, IPX-Routing-Enabled controls IPX routing for the entire system. When you write the profile, the TAOS unit comes up in IPX-routing mode. At that time, it creates an IPX-Interface profile for each installed Ethernet port.
- In the IPX-Interface profile, IPX-Routing-Enabled controls IPX routing for the particular interface. To enable the TAOS unit to route IPX on an Ethernet interface, you must set both the IPX-Routing-Enabled and IPX-Frame values.
- In the IPX-Options subprofile of the Connection profile, IPX-Routing-Enabled controls IPX routing for a particular connection.
- In a VRouter profile, IPX-Routing-Enabled enables or disables IPX routing for the specified Virtual Router (VRouter).

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

- Yes enables IPX routing.
- No disables IPX routing.

Example: `set ipx-routing-enabled = yes`

Dependencies: Consider the following:

- IPX routing must be enabled on both the dialing and answering sides of the link.
- To enable IPX routing for a particular interface, you must set IPX-Routing-Enabled to Yes in both the IPX-Global and IPX-Interface profiles.

Location: Connection *station* > IPX-Options, IPX-Global, IPX-Interface { shelf-*N* slot-*N N* }, VRouter *name*

See Also: Dial-Query, Interface-Address, IPX-Dialin-Pool, IPX-Frame, IPX-Header-Compression, IPX-Net-Number, IPX-Options, IPX-Route, IPX-SAP-Filter-Name, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, IPX-Type-20, Net-Alias, Net-Number, Peer-Mode, RIP, SAP, SAP-Filter

IPX-SAP-Filter

Description: A profile containing IPX Service Advertising Protocol (SAP) filter specifications for including or excluding services from the TAOS unit's SAP table.

Usage: Use the Read and List commands to make IPX-SAP-Filter the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the IPX-SAP-Filter default the working profile and list its contents:

```
admin> read ipx-sap-filter default
IPX-SAP-FILTER/default read
admin> list
[ in IPX-SAP-FILTER/default ]
ipx-sap-filter-name* = default
input-ipx-sap-filters = [ { no exclude 00:00 " " } { no exclude +
output-ipx-sap-filters = [ { no exclude 00:00 " " } { no exclude +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
IPX-SAP-FILTER/myfilter written
```

See Also: Input-IPX-SAP-Filters, IPX-SAP-Filter-Name, Output-IPX-SAP-Filters

IPX-SAP-Filter-Name

Description: Specifies an IPX Service Advertising Protocol (SAP) filter, as follows:

- In the IPX-Interface profile, IPX-SAP-Filter-Name applies a SAP filter to the IPX interface.
- In the IPX-SAP-Filter profile, IPX-SAP-Filter-Name specifies the name of the SAP filter being configured.

Usage: Specify the name of an IPX SAP filter. You can enter up to 15 characters. The default is null.

Example: set ipx-sap-filter-name = filter1

Dependencies: If the TAOS unit does not route IPX on the specified interface, or if IPX routing is globally disabled, IPX-SAP-Filter-Name does not apply.

Location: IPX-Interface {shelf-*N* slot-*N* *N*}, IPX-SAP-Filter

See Also: Interface-Address, IPX-Dialin-Pool, IPX-Frame, IPX-Net-Number, IPX-Options, IPX-Route, IPX-Routing-Enabled, IPX-Type-20

IPX-SAP-HS-Proxy

Description: Enables or disables the home-server proxy feature.

For mobile NetWare clients, you can specify the network numbers of from one to six NetWare servers that should receive Service Advertising Protocol (SAP) queries across the connection. Without this feature, when the client is in a distant location and sends a Get Nearest Server Request query, the client receives responses from servers closer to that location, rather than the expected home server or servers. With the home-server proxy feature, mobile clients can bring up a connection to the server or servers they usually use.

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

- Yes enables the home-server proxy feature.
- No disables the home-server proxy features.

Example: `set ipx-sap-hs-proxy = yes`

Dependencies: If you set IPX-SAP-HS-Proxy to Yes, you must use IPX-SAP-HS-Proxy-Net to configure from one to six IPX network numbers. The TAOS unit then directs the client's SAP queries to the specified networks.

Location: Connection *station* > IPX-Options

See Also: Dial-Query, IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy-Net, Net-Alias, Net-Number, Peer-Mode, RIP, SAP, SAP-Filter

IPX-SAP-HS-Proxy-Net

Description: Specifies from one to six IPX networks to which the TAOS unit directs a client's Service Advertising Protocol (SAP) queries when IPX-SAP-HS-Proxy to Yes.

Usage: Specify from one to six IPX network numbers. The default is six null addresses.

Example: `set ipx-sap-hs-proxy-net = 00000002`

Dependencies: If IPX-SAP-HS-Proxy is set to No, IPX-SAP-HS-Proxy-Net does not apply.

Location: Connection *station* > IPX-Options

See Also: Dial-Query, IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, Net-Alias, Net-Number, Peer-Mode, RIP, SAP, SAP-Filter

IPX-Type-20

Description: Specifies whether IPX Type 20 (NetBIOS) packets are propagated on the IPX interface. Some applications, such as NetBIOS over IPX, use IPX Type 20 packets to broadcast names over a network. By default, these broadcasts are not propagated over routed links, and are not forwarded over links that have less than 1-Mbps throughput. However, if you are using an application such as NetBIOS over IPX, which requires these packets in order to operate, you can set the IPX-Type-20 value to direct the TAOS unit to forward the broadcast packets.

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

- Yes specifies that the TAOS unit forwards IPX Type 20 packets.
- No specifies that the TAOS unit does not forward IPX Type 20 packets.

Example: `set ipx-type-20 = yes`

Dependencies: If the TAOS unit does not route IPX on the specified interface, or if IPX routing is globally disabled, IPX-Type-20 does not apply.

Location: IPX-Interface {shelf-*N* slot-*N* *N*}

See Also: Interface-Address, IPX-Dialin-Pool, IPX-Frame, IPX-Net-Number, IPX-Options, IPX-Route, IPX-Routing-Enabled, IPX-SAP-Filter-Name

IS-Post

Description: 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. 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

See Also: Index, IP-Address, Loadname, Shelf, Slot, Stack-Trace, Type, User-Profile, Version

ISDN-Emulation-Side

Description: Specifies whether the TAOS unit functions as the user-side (terminal equipment) or network side (network-terminating equipment) for T1 or E1 ISDN connections.

Usage: Specify one of the following values:

- TE specifies the user side.
- NT specifies the network side.

Example: `set isdn-emulation-side = nt`

Dependencies: If you specify NT for E1 connections, you must first set the Switch-Type value to Net5-PRI.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface,
E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Switch-Type

Item-Number

Description: Specifies an item on a slot card. Items are numbered starting with #1 for the leftmost item on the card.

Usage: Specify a number from 0 to 65535. The default is 0 (zero), which denotes the entire slot.

Example: `set item-number = 24`

Location: Call-Route-Info, Device-Address, Physical-Address

See Also: Call-Route-Info, Device-Address, Physical-Address, Shelf, Slot

IV-Len

Description: Specifies the number of bits in the Initialization Vector (IV) for Encapsulating Security Payload version 2 (ESP-v2).

Usage: For ESP-v1, specify 32 (a 32-bit vector) or 64 (a 64-bit vector). The default is 32. For ESP-v2, IV-Len is set to 64 automatically.

Example: `set iv-len = 64`

Location: IPSec *name* > Recv-ESP, IPSec *name* > Send-ESP

See Also: Active, AH-Type, Auth-Key, Auth-Type, ESP-Type, Key, Key2, Key3, Replay-Protection, SPI, Version

K

Keep-Alive-Timeout

Description: Specifies the number of seconds that the TAOS unit waits for a Quick Transaction Protocol (QTP) status update from a transaction server.

Usage: Specify a number from 1 to 300. The default is 30.

Example: `set keep-alive-timeout = 150`

Location: Transaction-Server

See Also: Data-Ack-Timeout

Key

Description: Specifies an authentication key for hashing.

Usage: For Authentication Header (AH), specify a 64-byte text string that exactly matches the key specified in the IP Security (IPSec) AH configuration of the L2TP Network Server (LNS). For Encapsulating Security Payload (ESP), specify a 16-byte text string that exactly matches the key specified in the IPSec ESP configuration of the LNS. The default is null.

Example: `set key = 4142434445464748494A4B4C4D4E4F50`

Location: IPSec *name* > Recv-AH, IPSec *name* > Recv-ESP, IPSec *name* > Send-AH, IPSec *name* > Send-ESP

See Also: Active, AH-Type, Auth-Key, Auth-Type, ESP-Type, IV-Len, Key2, Key3, Replay-Protection, SPI, Version

Key2

Description: An authentication key used for the second pass of 3DES-CBC mode encryption.

Usage: Specify a 16-byte text string. The default is null.

Example: `set key2 = 1234`

Dependencies: For Key2 to have any effect, you must set ESP-Type to 3DES-CBC.

Location: IPSec *name* > Recv-ESP, IPSec *name* > Send-ESP

See Also: Active, AH-Type, Auth-Key, Auth-Type, ESP-Type, IV-Len, Key, Key3, Replay-Protection, SPI, Version

Key3

Description: An authentication key used for the third pass of 3DES-CBC mode encryption.

Usage: Specify a 16-byte text string. The default is null.

Example: `set key3 = 5678`

Dependencies: For Key3 to have any effect, you must set ESP-Type to 3DES-CBC and Key2 to an appropriate value.

Location: IPSec *name* > Recv-ESP, IPSec *name* > Send-ESP

See Also: Active, AH-Type, Auth-Key, Auth-Type, ESP-Type, IV-Len, Key, Key2, Replay-Protection, SPI, Version

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 to 255. The default is 0 (zero).

Example: `set key-id = 10`

Dependencies: Authen-Type must be set to MD5 for Key-ID to have any effect.

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF

See Also: Auth-Key, Authen-Type, IP-Options, OSPF, OSPF-Options

K-Frames-Outstanding

Description: Establishes the maximum number of data packets that can be outstanding in an X.75 connection before acknowledgment is required.

Usage: Specify a number between 2 and 7. The default is 7.

Example: `set k-frames-outstanding = 3`

Location: Answer-Defaults > X75-Answer
Connection > X75-Options

See Also: Frame-Length, N2-Retransmissions, T1-Retrans-Timer

L

L2F-Mode

Description: Enables or disables Layer 2 Forwarding (L2F) operations.

Usage: Specify one of the following values:

- NAS (Network Access Server) enables L2F on the TAOS unit. Currently, the TAOS unit can only operate in NAS mode.
- Disabled (the default) disables L2F on the TAOS unit.

Note: The TAOS unit can operate as an L2F NAS in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: L2-Tunnel-Global

See Also: L2F-Retry-Count, L2F-Retry-Interval, L2F-System-Name, L2F-Tunnel-Secret, UDP-Queue-Length

L2F-Retry-Count

Description: The number of times the TAOS unit resends Layer 2 Forwarding (L2F) control packets.

Usage: Specify a number from 1 to 16. The default is 4.

Example: `set l2f-retry-count = 8`

Dependencies: L2F-Retry-Count applies only if L2F-Mode is set to NAS.

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: L2-Tunnel-Global

See Also: L2F-Mode, L2F-Retry-Interval, L2F-System-Name, L2F-Tunnel-Secret, UDP-Queue-Length

L2F-Retry-Interval

Description: Specifies the retry interval in seconds.

Usage: Specify a number from 0 to 32. The default value of 0 (zero) specifies that an adaptive retry interval (based on the retry number plus 1) is used.

Example: `set l2f-retry-interval = 4`

Dependencies: L2F-Retry-Interval applies only if L2F-Mode is set to NAS.

Note: The TAOS unit can operate as a Layer 2 Forwarding (L2F) Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: L2-Tunnel-Global

See Also: L2F-Mode, L2F-Retry-Count, L2F-System-Name, L2F-Tunnel-Secret, UDP-Queue-Length

L2F-System-Name

Description: Specifies the system name of the TAOS unit. It is used to identify the TAOS unit to the Layer 2 Forwarding (L2F) home gateway during tunnel creation.

Usage: Specify a system name of up to 24 characters. The default is null.

Example: `set l2f-system-name=ny-1`

Dependencies: L2F-System-Name only applies if L2F-Mode is set to NAS.

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: L2-Tunnel-Global

See Also: L2F-Mode, L2F-Retry-Count, L2F-Retry-Interval, L2F-Tunnel-Secret, UDP-Queue-Length

L2F-Tunnel-Secret

Description: The authentication method used by the TAOS unit to authenticate Layer 2 Forwarding (L2F) tunnels.

Usage: Specify one of the following values:

- Shared-Tunnel-Secret (the default) specifies that tunnel authentication relies on a secret shared by the Network Access Server (NAS) and the home gateway.
- Distinct-Tunnel-Secrets specifies that tunnel authentication uses distinct secrets for authenticating the NAS to the home gateway, and the home gateway to the NAS.
- Either-Shared-or-Distinct-Tunnel-Secret specifies that the TAOS unit first tries to authenticate using the shared secret. If that attempt fails, the unit then tries to authenticate the tunnel using distinct secrets.

Example: `set l2f-tunnel-secret = distinct-tunnel-secrets`

Dependencies: L2F-Tunnel-Secret applies only if L2F-Mode is set to NAS.

Note: The TAOS unit can operate as an L2F NAS in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: L2-Tunnel-Global

See Also: L2F-Mode, L2F-Retry-Count, L2F-Retry-Interval, L2F-System-Name, UDP-Queue-Length

L2TP-Auth-Enabled

Description: Enables or disables Layer 2 Tunneling Protocol (L2TP) tunnel authentication.

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

- Yes specifies that the TAOS unit authenticates the L2TP Network Server (LNS) with a Shared-Secret before passing calls to the system.
- No specifies that the TAOS unit does not authenticate the LNS.

Example: `set l2tp-auth-enabled = yes`

Dependencies: If you are using Remote Authentication Dial-In User Service (RADIUS) with L2TP, the RADIUS server must be able to encrypt the Tunnel-Password attribute.

Location: L2-Tunnel-Global

See Also: L2TP-Mode, L2TP-RX-Window

L2TP-Config

Description: A subprofile that enables you to configure Layer 2 Tunneling Protocol (L2TP) timer values when the TAOS unit acts as an L2TP Access Concentrator (LAC).

Usage: With the L2-Tunnel-Global profile as the working profile, list the L2TP-Config subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the L2TP-Config subprofile:

```
admin> list
[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
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: L2-Tunnel-Global

See Also: Control-Connect-Establish-Timer, First-Retry-Timer, Hello-Timer, LAC-Incoming-Call-Timer, Retry-Count

L2TP-Mode

Description: Specifies the system-wide type of Layer 2 Tunneling Protocol (L2TP) functionality the TAOS unit supports.

Usage: Specify one of the following values:

- LAC specifies that the TAOS unit can function as an L2TP Access Concentrator (LAC) only.
- LNS specifies that the TAOS unit can function as an L2TP Network Server (LNS) only.
- Both specifies that the TAOS unit can function as either an LAC or an LNS.
- Disabled (the default) specifies that L2TP functionality on the TAOS unit is disabled.

Example: `set l2tp-mode = lac`

Location: L2-Tunnel-Global

See Also: L2TP-Auth-Enabled, L2TP-RX-Window

L2TP-RX-Window

Description: Specifies the advertised Layer 2 Tunneling Protocol (L2TP) receive window size for data channels.

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

Example: `set l2tp-rx-window = 10`

Location: L2-Tunnel-Global

See Also: L2TP-Auth-Enabled, L2TP-Mode

L2TP-System-Name

Description: Specifies a name to be passed to the L2TP Access Concentrator (LAC) when the TAOS unit initiates a Layer 2 Tunneling Protocol (L2TP) tunnel.

Usage: Enter a string of up to 31 characters. The default is null, which specifies that the system name and domain name are sent.

Example: `set l2tp-system-name = bungalow1912`

Dependencies: If you specify a value of more than 31 alphanumeric characters, the hostname passed to the L2TP endpoint is truncated and the + character is appended to it.

Location: L2-Tunnel-Global

See Also: L2TP-Auth-Enabled, L2TP-Config, L2TP-Mode, L2TP-RX-Window, PPTP-Enabled, Server-Profile-Required

L2-Tunnel-Global

Description: A profile that contains system-wide configuration options for Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) tunnels.

Usage: Use the Read and List commands to make L2-Tunnel-Global the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the L2-Tunnel-Global profile the working profile and list its contents:

```
admin> read l2-tunnel-global
L2-TUNNEL-GLOBAL read

admin> list
[ in L2-TUNNEL-GLOBAL ]
pptp-enabled = no
server-profile-required = no
l2tp-mode = disabled
l2tp-auth-enabled = no
l2tp-rx-window = 0
l2tp-system-name = ""
l2tp-config = { 1000 6 60 60 60 0 no }
udp-queue-length = 256
l2f-mode = disabled
l2f-system-name = ""
l2f-retry-count = 4
l2f-retry-interval = 0
l2f-tunnel-secret = shared-tunnel-secret
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
L2-TUNNEL-GLOBAL written
```

See Also: L2F-Mode, L2F-Retry-Count, L2F-Retry-Interval, L2F-System-Name, L2F-Tunnel-Secret, L2TP-Auth-Enabled, L2TP-Config, L2TP-Mode, L2TP-RX-Window, L2TP-System-Name, PPTP-Enabled, Server-Profile-Required, UDP-Queue-Length

LAC-Incoming-Call-Timer

Description: Specifies the number of seconds that the TAOS unit waits for call setup to complete. Any change you make to this value takes effect when the previous timer expires.

Usage: Specify a decimal number from 1 to 600. 60 is the default.

Example: `set lac-incoming-call-timer = 60`

Dependencies: LAC-Incoming-Call-Timer applies only if you have set L2TP-Mode to LAC.

Location: L2-Tunnel-Global > L2TP-Config

See Also: Control-Connect-Establish-Timer, First-Retry-Timer, Hello-Timer, Retry-Count

LAN-Modem

Description: A profile created by the system for each installed digital modem card.

Usage: Use the Read and List commands to make LAN-Modem the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the LAN-Modem profile with the index { shelf-1 slot-6 0 } the working profile and list its contents:

```
admin> read lan-modem {1 6 0}
LAN-MODEM/{ shelf-1 slot-6 0 } read
admin> list
[in LAN-MODEM/{ shelf-1 slot-6 0 }]
physical-address* = { shelf-1 slot-6 0 }
modem-disable-mode = [ enable enable enable enable enable +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
LAN-MODEM/{ shelf-1 slot-6 1 } written
```

Dependencies: The LAN-Modem profile exists until a different slot card is detected in the slot. Removing or downing a card does not delete the profile or change its contents.

See Also: Modem-Disable-Mode, Physical-Address

LAN-Modem-Enabled

Description: Specifies whether the system generates a trap when a digital modem is moved to the suspect list.

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

- Yes specifies that the system generates a trap when a digital modem is moved to the suspect list.
- No specifies that the system does not generate a trap when a digital modem is moved to the suspect list.

Example: `set lan-modem-enabled = no`

Location: Trap *host-name*

See Also: Modem-Disable-Mode

Last-Reboot

Description: Specifies the reason that the controller was last rebooted.

Usage: The Last-Reboot setting is read only. It can have one of the following 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 = local-manual-reboot`

Location: Redundancy-Stats > Context-Stats > Context-Stats *N*

See Also: Select-Reason

Layer3-End

Description: Specifies CCITT Layer 3, which must be set to its default when a Digital Private Network Signaling System (DPNSS) or DASS 2 switch type is in use.

Usage: Specify one of the following values:

- X-Side (the default) specifies that Layer 3 favors the outgoing call when a call collision occurs.
- Y-Side specifies that Layer 3 does not favor the outgoing call when a call collision occurs.

Example: `set layer3-end = x-side`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface, Switch-Type

Lease-Duration

Description: Specifies the number of seconds for which an address assigned by the Dynamic Host Configuration Protocol (DHCP) server is valid.

Usage: Specify an integer. The default is 0 (zero), which places no time limit on assigned leases.

Example: `set lease-duration = 86400`

Location: IP-Global > DHCP-Server

See Also: Active, Boot-File-Path, Default-Lease-Duration, Default-Max-Lease, Default-Pool, Server-Address, Static-Address, TFTP-Host-Name

Left-Status

Description: Specifies the default content of the left side of the status window.

Usage: Specify one of the following values:

- Session-List specifies that the TAOS unit displays current system administration sessions on the left side of the status window.
- Connection-List specifies that the TAOS unit displays current system WAN sessions on the left side of the status window.
- Callstats-List specifies that the TAOS unit displays the current system call statistics on the left side of the status window. These statistics include timed interval information about the number of calls connected and authenticated.

Example: `set left-status = connection-list`

Location: User *name*

See Also: Bottom-Status, Default-Status, Top-Status

Len

Description: Specifies the number of bytes to test in a frame. Starting at the specified Offset, the TAOS unit compares the contents of the bytes to the generic filter's Value setting.

Usage: Specify a number from 0 to 8. The default is 0 (zero), which specifies that the TAOS unit does not compare packet contents and that all packets match the filter.

Example: `offset = 2
len = 8
more = no
comp-neq = no
mask = 0f:ff:ff:ff:00:00:00:f0:00:00:00:00
value = 07:fe:45:70:00:00:00:90:00:00:00:00`

In this Gen-Filter specification, the filter applies the mask to the eight bytes following the two-byte offset.

Location: Filter *filter-name* > Input-Filters > Gen-Filter,
Filter *filter-name* > Output-Filters > Gen-Filter

See Also: Gen-Filter, Input-Filters, Output-Filters

Line-Config

Description: A subprofile containing line configuration options for an E3-ATM, OC3-ATM or Serial WAN (SWAN) card.

Usage: With E3-ATM, OC3-ATM or SWAN as the working profile, list the Line-Config subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Line-Config subprofile:

```
admin> list line-config
[in OC3-ATM { shelf-1 slot-1 0 }:line-config]
trunk-group = 0
nailed-group = 1
call-route-info = { any-shelf any-slot 0 }
loopback = no-loopback
framer-mode = sdh
framer-rate = STS-3c
rx-descramble-disabled = no
tx-scramble-disabled = no
rx-cell-payload-descramble-disabled = no
tx-cell-payload-scramble-disabled = no
loop-timing = yes
vpi-vci-range = 0-15/32-4095
clock-source = not-eligible
clock-priority = middle-priority
traffic-shapers = [ { no 1000 1000 2 no 0 } { no 1000 1000 2 +
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: DS3-ATM {shelf-*N* slot-*N* *N*}, E3-ATM {shelf-*N* slot-*N* *N*},
OC3-ATM {shelf-*N* slot-*N* *N*}, SWAN {shelf-*N* slot-*N* *N*}

See Also: Activation, Call-Route-Info, Maximum-Channels, MBONE-LAN-Interface,
Nailed-Group, Trunk-Group

Line-Interface

Description: A subprofile containing T1 PRI or E1 PRI line configuration options.

Usage: With a T1 or E1 profile as the working profile, list the Line-Interface subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: With a T1 profile as the working profile:

```
admin> list line-interface
[in T1:line-interface]
enabled = no
frame-type = d4
encoding = ami
clock-source = eligible
clock-priority = middle-priority
signaling-mode = inband
robbed-bit-mode = wink-start
default-call-type = digital
switch-type = att-pri
nfas-id = 0
call-by-call = 0
data-sense = normal
```

```
idle-mode = flag-idle
fdl = none
front-end-type = dsx
DSX-line-length = 1-133
CSU-build-out = 0-db
channel-config = { { switched-channel 9 "" { any-shelf +
maintenance-state = no
sendDisc-val = 0
hunt-grp-phone-number-1 = ""
hunt-grp-phone-number-2 = ""
hunt-grp-phone-number-3 = ""
overlap-receiving = yes
pri-prefix-number = 3069
trailing-digits = 2
t302-timer = 10000
r1-use-anir = no
r1-first-digit-timer = 240
r1-anir-delay = 350
r1-anir-timer = 200
r1-modified = no
collect-incoming-digits = no
dsp-dtmf-input-sample-count = one-sample
isdn-emulation-side = te
incoming-call-handling = internal-processing
ss7-continuity = { loopback single-tone-2010 }
t1-inter-digit-timeout = 3000
```

With an E1 profile as the working profile:

```
admin> list line-interface
[in E1:line-interface]
enabled = yes
frame-type = g703
clock-source = eligible
clock-priority = middle-priority
signaling-mode = isdn
switch-type = net5-pri
front-end-type = short-haul
channel-config = [ { unused-channel 9 "" { any-shelf any-slot +
layer3-end = x-side
nl-value = 64
loop-avoidance = 7
number-complete = end-of-pulsing
group-b-answer-signal = signal-b-6
group-b-busy-signal = signal-b-3
group-ii-signal = signal-ii-2
answer-delay = 200
caller-id = no-caller-id
overlap-receiving = yes
pri-prefix-number = 3069
trailing-digits = 2
t302-timer = 10000
isdn-emulation-side = te
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: E1 {shelf-*N* slot-*N* *N*}, T1 {shelf-*N* slot-*N* *N*}

See Also: Answer-Delay, Call-By-Call, Caller-ID, Channel-Config, Clock-Priority, Clock-Source, Collect-Incoming-Digits, CSU-Build-Out, Data-Sense, Default-Call-Type, DSP-DTMF-Input-Sample-Count, DSX-Line-Length, Enabled, Encoding, FDL, Frame-Type, Front-End-Type, Group-II-Signal, Group-B-Answer-Signal, Group-B-Busy-Signal, Hunt-Grp-Phone-Number-*N*, Idle-Mode, Incoming-Call-Handling, Layer3-End, Loop-Avoidance, Maintenance-State, NFAS-ID, NL-Value, Number-Complete, Overlap-Receiving, PRI-Prefix-Number, R1-ANIR-Delay, R1-ANIR-Timer, R1-First-Digit-Timer, R1-Modified, R1-Use-ANIR, Robbed-Bit-Mode, SendDisc-Val, Signaling-Mode, SS7-Continuity, Switch-Type, T1-Inter-Digit-Timeout, T302-Timer, Trailing-Digits

Line-Length

Description: Specifies the length of the Rx and Tx lines to a DSX-3 Cross Connect.

Usage: Specify either of the following values:

- 0-255 (0 to 255 feet)
- 226-450 (226 to 450 feet)

For a direct connection, double the values.

Location: T3 {shelf-*N* slot-*N* *N*}

See Also: Enabled, Frame-Type, Name, Physical-Address

Line-State

Description: Reports the state of a T1 PRI, T3, or Serial WAN (SWAN) line.

Usage: The Line-State setting is read only. You cannot set Line-State directly. For a T1 PRI line, the state can have one of the following values:

Value	Indicates
Does-Not-Exist	The line is not installed.
Disabled	The line is disabled.
Loss-Of-Sync	A red-alarm state has occurred.
Yellow-Alarm	A device on the line is detecting framing errors in the signal.
AIS-Receive	The line is receiving a keepalive signal.
No-D-Channel	A D-channel failure has occurred.
Active	Multipoint is established.

For a T3 line, the state can have the same values as a T1 PRI line (except No-D-Channel). In addition, a T3 line can have one of the following values:

- Idle-Receive indicates that the line is receiving an idle signal.
- Wrong-Frame indicates that the remote end is configured for a different T3 application.

Example: `line-state = active`

Location: SWAN-Stat {shelf-*N* slot-*N* *N*}, T1-Stat {shelf-*N* slot-*N* *N*},
T3-Stat {shelf-*N* slot-*N* *N*}

See Also: Channel-State, DS2-State

Link-Compression

Description: Specifies the link-compression method for a Point-to-Point Protocol (PPP)-encapsulated packet transmitted and received on the connection.

Usage: Specify one of the following values:

- None specifies no link compression. In the Answer-Defaults profile, None is the default.
- Stac specifies a modified version of draft 0 of the Compression Control Protocol (CCP), which predates RFC 1974. Older equipment supports this compression method. It is not recommended for use with IPX connections. In a Connection profile, Stac is the default.
- Stac-9 specifies draft 9 of the Stac LZS compression protocol, which is described in RFC 1974. Most devices use this compression method.
- MS-Stac specifies Microsoft/Stac compression (the method used by Windows 95). If the caller does not acknowledge Microsoft/Stac compression, the TAOS unit attempts to use standard Stac compression. If the caller does not acknowledge Stac compression, the link uses no compression.

Example: `set link-compression = stac-9`

Dependencies: Only PPP, Multilink Protocol (MP), and Multilink Protocol Plus (MP+) links support Link-Compression. Both sides of the connection must specify the same type of link compression. Otherwise, your setting has no effect.

By default, NetWare relies on the Data Link layer (also called Layer 2) to validate and guarantee data integrity. When you configure Stac compression, the system performs an 8-bit checksum, which is inadequate for NetWare data. Therefore, for NetWare connections, carry out one of the following tasks:

- Select Stac-9 or MS-Stac compression, which uses a more robust error-checking method.
- Disable link compression by setting Link-Compression to None. When you do so, the TAOS unit guarantees data integrity by means of PPP.
- Accept the default Stac setting, and enable IPX checksums on your NetWare servers and clients. Both the server and the client must support IPX checksums. If you enable checksums on your servers, but not on your clients, all logins will fail.

Location: Answer-Defaults > PPP-Answer, Connection *station* > PPP-Options

See Also: PPP-Answer, PPP-Options, VJ-Header-Prediction

LinkDown-Enabled

Description: Specifies whether the system generates a trap when a failure occurs in a communication link between the unit and the Simple Network Management Protocol (SNMP) manager.

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

- Yes specifies that the system generates a trap when a failure occurs in a communication link between the unit and the SNMP manager.
- 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 *host-name*

See Also: LinkUp-Enabled

Link-Mgmt

Description: Specifies the link management protocol to use between the TAOS unit and the Frame Relay switch. The Frame Relay administrator or service provider can tell you which value to use.

Usage: Specify one of the following values:

- None specifies no link management. The TAOS unit assumes that the physical link is up and that all Data Link Connection Identifiers (DLCIs) are active on the physical link. None 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 *fr-name*

See Also: DCEN392-Val, DCEN393-Val, FR-Name, Link-Type, N391-Val, N392-Val, N393-Val, T391-Val, T392-Val

Link-Mgmt-DLCI

Description: Specifies the Data Link Connection Identifier (DLCI) to use for link management on the Frame Relay datalink.

Usage: Specify DLCI0 (the default) or DLCI1023.

Example: `set link-mgmt-dlci = dlci1023`

Dependencies: When SVC signaling is enabled, the data link can use either ANSI or CCITT LMI, but Link-Mgmt-DLCI must be set to its default value of DLCI0.

Location: Frame-Relay *fr-name*

See Also: Link-Mgmt

Link-State

Description: Indicates the physical state of the LAN interface.

Usage: The Link-State setting can be Up, Down, or Unknown. The value can only be set by the Ethernet driver.

- Up specifies that the LAN interface can transmit and receive network traffic.
- Down specifies 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 down).
- Unknown specifies the shelf-controller Ethernet interface.

Location: Ether-Info {shelf-*N* slot-*N* *N*}

See Also: Interface-Address, Link-State-Enabled, MAC-Address

Link-State-Enabled

Description: Specifies whether the value of Link-State affects the IP routing tables.

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

- Yes specifies that the TAOS unit deletes routes to an interface when Link-State is Down, and adds them when the interface comes up again.
- No specifies that the TAOS unit routes packets to an interface regardless of the Link-State setting. If the interface is down, the unit discards the packets. They cannot use an alternative route.

Example: `set link-state-enabled = yes`

Location: Ethernet {shelf-*N* slot-*N* *N*}

See Also: Link-State

Link-Type

Description: Specifies the kind of logical interface between the TAOS unit and the Frame Relay network on the datalink:

- The UNI (User to Network Interface) is the interface between an end-user and a network endpoint (a router or a switch) on the Frame Relay network.
- A DCE (Data Circuit-Terminating Equipment) is a device that connects the DTE (Data Terminal Equipment) to a communications channel, such as a telephone line.
- A DTE refers to a device that an operator uses, such as a computer or a terminal.
- NNI (Network-to-Network Interface) operation allows the TAOS unit to act as a Frame Relay switch communicating with another Frame Relay switch.

Usage: Specify one of the following values:

- DCE specifies a UNI-DCE connection. The TAOS 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 TAOS unit operates as the user side, communicating with the network-side DCE switch.
- NNI specifies an NNI connection. The TAOS unit performs both DTE and DCE link management.

Example: `set link-type = dte`

Location: Frame-Relay *fr-name*

See Also: DCEN392-Val, DCEN393-Val, N391-Val, N392-Val, N393-Val, T391-Val, T392-Val

LinkUp-Enabled

Description: Specifies whether the system generates a trap when the communication link between the unit and the Simple Network Management Protocol (SNMP) manager comes back up.

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

- Yes specifies that the system generates a trap when the communication link between the unit and the SNMP manager comes back up.
- No specifies that the system does not generate a trap when the communication link between the unit and the SNMP manager comes back up.

Example: `set linkup-enabled = no`

Location: Trap *host-name*

See Also: LinkDown-Enabled

Loadname

Description: 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

See Also: Index, IP-Address, IS-Post, Shelf, Slot, Stack-Trace, Type, User-Profile, Version

Load-Select

Description: A profile that specifies which slot-card images to load to flash when you use a Load Tar command. Following a system reset, the TAOS unit creates the Load-Select profile if it is not present. The profile lists the entire set of supported slot-card images and an intended load action for each card type when the image is present in a tar file. It also contains an Unknown-Cards setting, which represents new cards that were not supported in the previous system version.

When loading the tar file, the system uses settings in the Load-Select profile to load only specific slot-card images. To prevent version-related problems, it then deletes code images that were present on the flash card but were not updated.

Usage: Use the Read and List commands to make Load-Select the working profile and list its contents.

Example: To make the Load-Select profile the working profile and list its contents:

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

admin> list
[in LOAD-SELECT]
unknown-cards = auto
8t1 = auto
8e1 = auto
t3 = auto
ut1 = auto
ue1 = auto
uds3 = auto
ds3-atm = auto
enet2 = auto
amdm = auto
hdlc2 = auto
swan = auto
```

Dependencies: An explicit Load command for a particular card type overrides the settings in the Load-Select profile. The Load-Select profile is read only.

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, T3, UDS3, UE1, Unknown-Cards, UT1

Local-Address

Description: Specifies an IP address for the local side of a numbered-interface connection.

Usage: Specify an IP address in dotted decimal notation. Separate the optional subnet mask from the address by entering a forward slash. The address must be unique to the connection. You can assign a fake IP address or an IP address from one of the local subnets. The TAOS unit accepts IP packets destined for the specified address and treats them as destined for the system itself. The packets might arrive on any interface, and the destination numbered interface need not be in the active state. The default is 0.0.0.0, which indicates an unnumbered interface.

Example: `set local-address = 10.2.3.4/24`

Dependencies: The Local-Address value cannot be an address assigned in an IP-Interface profile to one of the TAOS unit's physical LAN interfaces, nor can it be the IP address of the shelf-controller Ethernet port.

Location: Connection *station* > IP-Options

See Also: IP-Options, Remote-Address

Local-Echo

Description: Allows you to configure local-echo mode for a terminal-server session. Local-echo mode is a line-by-line mode. The line appears as the user types it, but is not transmitted until the user enters a carriage return. If local echo is enabled, the line transmitted is echoed on the local terminal screen. Local echo allows terminal-server users to connect to nonstandard Telnet ports and programs. If the remote server turns local echo on or off in its option negotiation for a Telnet session, the negotiated setting overrides the value of Local-Echo.

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

- Yes turns on local echo.
- No disables local echo.

Example: `set local-echo = yes`

Dependencies: If terminal services are disabled, Local-Echo does not apply. A terminal-server user can override the Local Echo setting from the command line by using the `-e` option of the Telnet command.

Location: Terminal-Server > Terminal-Mode-Configuration > Telnet-Options

See Also: Telnet-Options, Terminal-Mode-Configuration

Local-Profiles-First

Description: Specifies whether the TAOS unit should attempt local authentication before remote external authentication.

Usage: Specify one of the following settings:

- LPF-Yes (the default) specifies that the TAOS unit first attempts to authenticate the connection with a local profile. If the profile exists and the password matches, the unit allows the connection. If no local profile exists, or if a local profile exists but the password fails, the TAOS unit tries to authenticate the connection through an external authentication server.
- LPF-No specifies that the TAOS 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 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 TAOS unit attempts to authenticate the connection with a local profile.
- LPF-RNo specifies that the TAOS unit first tries to authenticate the connection through a remote authentication server. If the profile exists and the password matches, the unit allows the connection. If the server doesn't respond, the TAOS unit checks for a matching local profile. If the server NAKs the request and remote authentication fails, the TAOS 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 TAOS unit waits for the remote authentication to time out before attempting to authenticate locally. This timeout might take longer than the timeout specified for the connection and could cause all connection attempts to fail. Therefore, set the authentication timeout value low enough to guard against the line going down, but high enough to permit the unit to respond if it can. The recommended time is 3 seconds.

Location: External-Auth

See Also: Auth-Timeout, Auth-Type

Local-Retransmit-LSF

Description: Enables or disables local retransmission of a low-speed fax frame if no response is detected from the destination fax.

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

- Yes enables local retransmission of a low-speed fax frame if no response is detected from the destination fax. This setting is designed to reduce fax transmission errors on low packet loss networks.
- No disables local retransmission of a low-speed fax frame if no response is detected from the destination fax.

Example: `set local-retransmit-lsf = no`

Dependencies: For Local-Retransmit-LSF to apply, you must set RT-Fax-Enable to Yes.

Location: VoIP {x y} > RT-Fax-Options

See Also: Command-Spoof, ECM-Enable, Low-Latency-Mode, RT-Fax-Enable

Location

Description: Specifies the physical location of the TAOS unit. A Simple Network Management Protocol (SNMP) manager can both read and set the Location value.

Usage: Specify text describing where the TAOS unit is located. You can enter up to 80 characters. The default is null.

Example: `set location = building-64`

Location: SNMP

See Also: Contact

Log

Description: A profile that specifies event-logging settings. All settings except the Syslog-Format setting affect the first data stream only. The Syslog-Format setting controls the format of all Syslog streams.

Usage: Use the Read and List commands to make Log the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Log profile the working profile and list its contents:

```
admin> read log
LOG read

admin> list
[in LOG]
save-level = info
save-number = 100
call-info = none
syslog-enabled = no
host = 0.0.0.0
port = 514
facility = local0
syslog-format = tnt
log-software-version = no
syslog-level = info
auxiliary-syslog = [ { no info 0.0.0.0 514 local0 } { no info +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
LOG written
```

See Also: Auxiliary-Syslog, Call-Info, Facility, Host, Log-Software-Version, Save-Level, Save-Number, Syslog-Enabled, Syslog-Level

Log-Display-Level

Description: Specifies the lowest level of the log messages that the TAOS unit displays to a logged-in user.

Usage: Specify one of the following settings:

Setting	Lowest-level message indicates
None (the default)	The TAOS 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	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	State and status changes that are commonly not of general interest have occurred.
Debug	Helpful debugging information.

Example: `set log-display-level = debug`

Dependencies: Do not confuse Log-Display-Level with Save-Level in the Log profile. Save-Level determines which messages are displayed in the event-log status window.

Location: User *name*

See Also: Log, Save-Level

Login-Prompt

Description: Specifies the string that acts as a prompt for a username in the terminal-server interface.

Description: If Prompt-Format to No, you can specify up to 15 characters, not including a newline or tab character.

If Prompt-Format is set to Yes, you can specify up to 80 characters in multiple lines by including the newline (\n) and tab (\t) characters. To include an actual backslash character, you must precede it with another backslash.

Example: Suppose you enter the following string:

`Welcome to\n\t\\Lucent Remote Server\\\nEnter your username:`

The terminal server displays the following text as the login prompt:

```
Welcome to
  \Lucent Remote Server\
Enter your username:
```

Dependencies: If terminal services are disabled, Login-Prompt does not apply. Regardless of the Prompt-Format setting, the default setting for Login-Prompt is `Login:`.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Password-Prompt, Prompt, Prompt-Format, Terminal-Mode-Configuration, Third-Login-Prompt, Third-Prompt-Sequence

Login-Timeout

Description: Specifies the number of seconds a user can wait to log into the terminal server. When a user attempts to log into the terminal server in terminal mode, a login prompt appears. If the user does not proceed any further than the login prompt within the number of seconds you specify, the login times out.

Usage: Specify a number between 0 and 300. The default is 300. If you set Login-Timeout to 0 (zero), the login never times out.

Example: `set terminal-mode-configuration login-timeout = 60`

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Password-Prompt, Prompt, Prompt-Format, Terminal-Mode-Configuration, Third-Login-Prompt, Third-Prompt-Sequence

Log-Software-Version

Description: Enables or disables hourly log messages reporting the current software version. The messages are sent to the Syslog host.

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

- Yes enables hourly log messages reporting the current software version.
- No disables hourly log messages reporting the current software version.

Example: `set log-software-version = yes`

Dependencies: If Debug permission is enabled, the messages are displayed on the screen (as well as sent to the Syslog host).

Location: Log

See Also: Host, Save-Level, Save-Number, Syslog-Enabled

Loop-Avoidance

Description: Specifies the number of transit devices through which the TAOS unit can route a call.

Usage: Specify an integer from 1 to 26. The default is 7.

Example: `set loop-avoidance = 7`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface, NL-Value

Loopback

Description: Specifies whether to run a loopback test on the interface. While the interface is looped back, normal data traffic is interrupted.

Usage: For a DS3-ATM or OC3-ATM interface, specify one of the following settings:

- No-Loopback (the default). The interface is operating normally.
- Facility-Loopback. During a facility loopback, the interface returns the signal it receives on the line.
- Local-Loopback. During a local loopback, the interface's receive path is connected to the interface's transmit path. The transmitted signal is still sent to the network as well.

For a T3 interface, specify one of the following settings:

- No-Loopback (the default). The interface is operating normally.
- Line-Loopback. Loop the DS3 outwards (downstream).
- Local-Loopback. During a local loopback, the interface's receive path is connected to the interface's transmit path. The transmitted signal is still sent to the network as well.

Example: `set loopback = no-loopback`

Location: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
T3 {shelf-*N* slot-*N* *N*}

See Also: Network-Loopback

Loop-Timing

Description: Enables or disables deriving transmission timing from receiver inputs.

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

- Yes specifies that loop timing is enabled.
- No specifies that loop timing is disabled.

Example: `set loop-timing = no`

Location: OC3-ATM {shelf-*N* slot-*N* *N*} > Line-Config, STM {shelf-*N* slot-*N* *N*}

See Also: Loopback

Loss-Of-Carrier

Description: Indicates a loss of the carrier signal on a T1 line.

Usage: The Loss-Of-Carrier setting is read only. True indicates a loss of carrier. False indicates that the carrier is maintaining a connection.

Location: T1-Stat {shelf-*N* slot-*N* *N*}

See Also: AIS-Receive, BER-Receive, Carrier-Established, Loss-Of-Sync, Yellow-Receive

Loss-of-Frame

Description: Indicates a loss-of-frame signal on the line (also known as a Red Alarm).

Usage: The Loss-Of-Frame setting is read only. True indicates a loss of frame. False indicates no loss of frame.

Example: `loss-of-frame = False`

Location: T3-Stat {shelf-*N* slot-*N* *N*}

Loss-Of-Signal

Description: Indicates a loss of signal on the line.

Usage: The Loss-Of-Signal setting is read only. True indicates a loss of signal. False indicates no loss of signal.

Example: `loss-of-signal = False`

Location: T3-Stat {shelf-*N* slot-*N* *N*}

Loss-Of-Sync

Description: Indicates whether the T1 line has lost synchronization.

Usage: The Loss-Of-Sync setting is read only. True indicates that synchronization has been lost. False indicates that synchronization is intact.

Location: T1-Stat {shelf-*N* slot-*N* *N*}

See Also: AIS-Receive, BER-Receive, Carrier-Established, Loss-Of-Carrier, Yellow-Receive

Low-Latency-Mode

Description: Enables or disables low latency mode for real-time fax operations over networks with low packet loss and low latency characteristics. Low latency mode allows operation on networks with less than 2.5 seconds or less of aggregate latency between pages.

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

- Yes enables low latency mode.
- No disables low latency mode. When you specify No, a minimum of 10 seconds delay is added to processing fax calls to allow interpretation of T.30 frames and implement spoofing.

Example: `set low-latency-mode = no`

Dependencies: For Low-Latency-Mode to apply, you must set RT-Fax-Enable to Yes.

Location: VoIP {x y} > RT-Fax-Options

See Also: Command-Spoof, ECM-Enable, Local-Retransmit-LSF, RT-Fax-Enable

Low-Temperature-Trigger

Description: Specifies the low-temperature threshold setting for the fantray.

Usage: Specify a number from 0 to 60 degrees Celsius. The default is 34.

Example: `set low-temperature-trigger = 40`

Dependencies: If the fantray is in auto-regulation mode (Operation-Mode is set to Auto-Regulation) and the Low-Temperature-Trigger threshold is crossed, the system switches the fans to low noise speed and logs a message. If you specify a higher value than the High-Temperature-Trigger setting, the system displays an error message when you attempt to write the profile.

Location: Thermal

See Also: High-Temperature-Trigger, Operation-Mode

LQM

Description: Specifies whether the TAOS unit requests link-quality monitoring when answering a Point-to-Point Protocol (PPP) call. Link-quality monitoring counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link-quality problems. 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 specifies that the TAOS unit requests link-quality monitoring.
- No specifies that the TAOS unit does not request link-quality monitoring.

Example: `set lqm = yes`

Dependencies: The LQM value applies only to PPP links. When LQM is enabled, the system selects a random number (called a *magic number*) and negotiates that number with the remote device during LCP negotiation of the link. If the remote device does not negotiate magic numbers, the magic-number field in transmitted packets is set to 0 (zero). If the number is successfully negotiated, the local magic-number field is set to the selected random number. The WANDisplay command on an installed Hybrid Access card shows information about LQM magic number negotiations, and the periodic LQM reports show the assigned local and remote magic numbers.

The TAOS unit inspects the magic-number field in received packets. If it is equal to 0 (zero) or the peer's unique magic number, the packet is processed normally. If the magic-number field is equal to the local magic number, indicating a loopback link, the TAOS unit brings down the link.

Location: Answer-Defaults > PPP-Answer, Connection *station* > PPP-Options

See Also: LQM-Maximum-Period, LQM-Minimum-Period, PPP-Answer, PPP-Options

LQM-Maximum-Period

Description: Specifies the maximum period, in one-hundredths of a second, during which the TAOS unit will accept and send link-quality monitoring packets when answering a Point-to-Point Protocol (PPP) call.

Usage: Specify a number from 0 to 600. The default is 600.

Example: `set lqm-maximum-period = 300`

Dependencies: If LQM is set to No, LQM-Maximum-Period does not apply.

Location: Answer-Defaults > PPP-Answer, Connection *station* > PPP-Options

See Also: LQM, LQM-Minimum-Period, PPP-Answer, PPP-Options

LQM-Minimum-Period

Description: Specifies the minimum period, in one-hundredths of a second, during which the TAOS unit will accept link-quality monitoring packets when answering a Point-to-Point Protocol (PPP) call.

Usage: Specify a number from 0 to 600. The default is 600.

Example: `set lqm-minimum-period = 200`

Dependencies: If LQM is set to No, LQM-Minimum-Period does not apply.

Location: Answer-Defaults > PPP-Answer, Connection *station* > PPP-Options

See Also: LQM, LQM-Maximum-Period, PPP-Answer, 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 {shelf-*N* slot-*N* *N*}

See Also: Interface-Address, Link-State

Maintenance-State

Description: Allows you to Busy Out or take Out Of Service (OOS) a T1 PRI line. Doing so is known as *quiescing* the line to make it available for maintenance. Active calls on the line are not torn down. When an active call disconnects, the TAOS unit takes the channel out of service. When the entire line is out of service, it is available for maintenance.

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

- Yes quiesces the line, making it available for maintenance when all active calls have been dropped.
- No specifies that the line is available for active service. If you specify No after the line has been quiesced, it returns to service.

Example: `set maintenance-state = yes`

Dependencies: If the line's Signaling-Mode is not ISDN, Maintenance-State does not apply. When the TAOS unit reboots, all T1 PRI lines come up available for service.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface, Signaling-Mode

Management-Only-Interface

Description: Enables or disables management-only on the IP interface. The management-only interface can be a shelf-controller port or a port on an installed Ethernet card.

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

- Yes specifies that incoming traffic on the interface terminates in the system itself, and is not forwarded on any other interface. In addition, only traffic generated by the system is forwarded on the management-only interface. Traffic generated externally is dropped on the interface.
- No specifies that the management-only feature is disabled.

Example: `set management-only-interface = yes`

Location: IP-Interface {shelf-*N* slot-*N* *N*}

See Also: Directed-Broadcast-Allowed, Interface-Address, IP-Address, Multicast-Allowed, Multicast-Group-Leave-Delay, Multicast-Rate-Limit, OSPF, Proxy-Mode, RIP2-Use-Multicast, RIP-Mode

Mask

Description: Specifies a 12-byte mask to apply to a generic filter's Value setting before comparing the Value to the packet contents at the specified Offset. You can use the mask to specify exactly which bits you want to compare.

After translating Mask and Value into binary format, the TAOS unit applies the mask to the specified value by performing a logical AND. The mask hides the bits that appear behind each binary 0 (zero) in the mask. A mask of all ones (FF:FF:FF:FF:FF:FF:FF:FF) masks no bits, so the full specified value must match the packet contents.

Usage: Specify a hexadecimal number of up to 12 bytes. The default is 000000000000.

Example: `offset = 2`

`len = 8`

`more = no`

`comp-neq = no`

`mask = 0f:ff:ff:ff:00:00:00:f0:00:00:00:00`

`value = 07:fe:45:70:00:00:00:90:00:00:00:00`

Suppose you want to apply these Gen-Filter settings to the following packet contents:

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

The TAOS unit applies the mask as shown below, resulting in a value that matches the Value setting.

	2-byte Byte Offset	8-byte Comparison
	2A 31	97 FE 45 70 12 22 33 99 B4 80 75
Mask	-----	0F FF FF FF 00 00 00 F0
Result of mask	-----	07 FE 45 70 00 00 00 90
Value to test	-----	07 FE 45 70 00 00 00 90

The packet matches the filter. Because Forward is set to No, the TAOS unit drops the packet.

The byte comparison works as follows:

- The first two bytes, 2A and 31, are ignored because of the two-byte offset.
- The 9 in the third byte is ignored, because the mask has a 0 (zero) in its place. The 7 in the third byte matches the 7 in the Value setting for that byte.
- The F and E in the fourth byte match the Value setting for that byte.
- The 4 and 5 in the fifth byte match the Value setting for that byte.
- The 7 and 0 in the sixth byte match the Value setting for that byte.
- The 12, 22, and 33 in the seventh, eighth, and ninth bytes, respectively, are ignored because the mask has a 0 (zero) in those places.
- The first 9 in the tenth byte matches the Value setting of 9 in the first half of that byte. The second 9 in the packet's tenth byte is ignored because the mask has a 0 (zero) in its place.

Location: Filter *filter-name* > Input-Filters > Gen-Filter,
Filter *filter-name* > Output-Filters > Gen-Filter

See Also: Gen-Filter, Input-Filters, Output-Filters

Max-Baud-Rate

Description: Specifies the highest baud rate that digital modems should attempt to negotiate. Typically, the digital modems start with the highest possible baud rate (33600) and negotiate down to the rate accepted by the remote modem. You can adjust the maximum rate to bypass some of the negotiation cycles, provided that no incoming calls use a baud rate higher than the value you specify for Max-Baud-Rate.

Usage: Specify one of the following values:

33600-Max-Baud (the default)
31200-Max-Baud
28800-Max-Baud
26400-Max-Baud
2400-Max-Baud
21600-Max-Baud
19200-Max-Baud
16800-Max-Baud
14400-Max-Baud
12000-Max-Baud
9600-Max-Baud
7200-Max-Baud
4800-Max-Baud
2400-Max-Baud

Example: `set max-baud-rate = 31200-max-baud`

Dependencies: If terminal services are disabled, Max-Baud-Rate does not apply.

Location: Terminal-Server > Modem-Configuration

See Also: Modem-Configuration

Max-Bundle-Members

Description: Specifies the maximum number of data links allowed to join the MFR bundle.

Usage: Specify the maximum number of data links allowed to join the MFR bundle. The default value is 1. If you specify a number higher than 1, you can add bandwidth to the bundle up to the specified number of data links.

Example: If Max-Bundle-Members is set to 4 and the bundle has 2 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 slot card, the card'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 *name*

See Also: Active, MFR-Bundle-Name, MFR-Bundle-Type, Min-Bandwidth

Max-Burst-Size

Description: Specifies the Maximum Burst Size (MBS), which is the maximum number of cells that can be transmitted at Peak-Rate before the TAOS unit determines that the connection is exceeding the defined characteristics.

Usage: Specify an integer from 2 to 255. The default is 2.

Example: `set max-burst-size = 5`

Dependencies: The Max-Burst-Size value applies only to Variable Bit Rate (VBR) traffic.

Location: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*

See Also: Aggregate, Bit-Rate, Enabled, Peak-Rate, Priority

Max-Call-Duration

Description: Specifies the maximum number of minutes an incoming call can remain connected. For a multichannel call, the maximum applies to each channel.

Usage: Specify a number from 0 to 1440. The TAOS unit checks the connection once per minute, so the actual time the call is connected is slightly longer than the time you set. The default is 0 (zero), which specifies that the unit does not set a limit on the duration of an incoming call.

Location: Connection *station* > Session-Options

See Also: Session-Options

Maxcalls

Description: Specifies the maximum number of Voice over IP (VoIP) calls a TAOS unit can process simultaneously.

Usage: For a MAX TNT unit, specify a number from 1 to the maximum number of DSPs installed. The default is 256. For an APX 8000 unit, specify a number from 0 to the maximum call volume set by the VoIP hash code. The default is the maximum call-processing limit.

Example: `set maxcalls = 200`

Dependencies: Use Maxcalls when continued high call volumes on a network affect call quality. Lowering the value for Maxcalls enables a TAOS unit to allocate more system resources to processing fewer calls, resulting in improved call quality. When active calls exceed the Maxcalls limit, the caller receives a busy signal from the TAOS unit.

Location: VoIP {x y}

Max-Cc

Description: Specifies the maximum number of control Protocol Data Unit (PDU) retransmissions (BGN, END, RESYNC).

Usage: Specify an integer from 0 to 64. The default value is 4.

Example: `set max-cc = 10`

Location: ATM-Interface {{shelf-N slot-N N} N } > SVC-Options > QSAAL-Options

See Also: Max-Pd, Max-Stat, Tcc-ms, Tidle-ms, Tkeepalive-ms, Tnoresponse-ms, Tpoll-ms, Window-Size

Max-Dialout-Time

Description: Specifies the maximum number of seconds the system waits for a Call Setup Complete from the remote side when dialing out.

Usage: Specify an integer from 0 to 255. The default is 20 seconds. If set to Max-Dialout-Time to 0 (zero), the TAOS unit uses its internal default of 20 seconds.

Example: In the following example, the dial-out timer is set to 60 seconds:

```
admin> read system
SYSTEM read
admin> set max-dialout-time = 60
admin> write
SYSTEM written
```

Dependencies: Consider the following:

- The Max-Dialout-Time setting does not influence the modem timeout to detect carrier. Modems have an internal timer that counts down from dial-out to establishing carrier with the remote modem (including training), which for Rockwell modems has a default of 45 seconds.
- For Voice over IP (VoIP) processing, a setting of 60 or greater is recommended to allow sufficient time for the unit to establish the connection with the called destination. In addition, a setting of 60 makes this timer consistent with other internal H.323 timers, which are hardcoded to time out after 60 seconds. The unit can clear abandoned or failed outgoing calls more quickly and efficiently.

Location: System

See Also: Analog-Encoding, Call-Routing-Sort-Method, Idle-Logout, Name, Parallel-Dialing, Perm-Conn-Upd-Mode, SessionID-Base, Single-File-Incoming, System-Rmt-Mgmt, Userstat-Format, Use-Trunk-Groups

Maximum-Channels

Description: Specifies the maximum number of channels in a multichannel call.

Usage: Specify an integer from 1 to 32. The default is 2.

Example: `set maximum-channels = 5`

Location: Answer-Defaults > MP-Answer, Connection *station* > MP-Options

See Also: Base-Channel-Count, Enabled, Minimum-Channels, MP-Answer, MP-Options

Maximum-Connect-Time

Description: Specifies the maximum number of minutes an AppleTalk Remote Access (ARA) session can remain connected.

Usage: Specify an integer. The default is 0 (zero), which disables the timer. The maximum connect time for an ARA connection has nothing to do with the TAOS unit's idle timer. If you specify a maximum connect time, the TAOS unit initiates an ARA disconnect when that time is up. The ARA link goes down cleanly, but remote users are not notified. Users will find out the ARA link is gone only when they try to access a device.

Example: `set maximum-connect-time = 10`

Dependencies: For Maximum-Connect-Time to apply, you must set Enabled to Yes in the ARA-Answer subprofile, and ARA-Enabled to Yes in the ARA-Options subprofile.

Location: Connection *station* > ARA-Options

See Also: ARA-Enabled

Max-Jitter-Buffer-Size

Description: Specifies the maximum jitter buffer size for Voice over IP (VoIP) calls when the unit is configured to perform adaptive call jitter buffering. When you use adaptive mode, the jitter buffer can increase to accommodate up to the specified number of audio packets on the basis of the incoming audio packet volume.

Usage: Specify a number of packets from 1 to 19. The default is 19.

Example: `set max-jitter-buffer-size = 10`

Dependencies: Changes to Max-Jitter-Buffer-Size become effective with the next VoIP call.

Location: VoIP {x y}

See Also: Ena-Adap-Jitter-Buffer, Initial-Jitter-Buffer-Size

Maximum-Leases

Description: Specifies the maximum number of lease renewals allowed.

Usage: Specify an integer. The default is 4. When the limit is reached, the lease is not renewed.

Example: `set maximum-leases = 5`

Dependencies: To limit the amount of time a client with a Dynamic Host Configuration Protocol (DHCP)-assigned address can have access to the TAOS unit, you can use the value of Maximum-Leases with Lease-Duration in the IP-Global profile.

Location: Connection *station* > DHCP-Options

See Also: Lease-Duration, Pool-Number, Reply-Enabled

MAXLink-Client-Enabled

Description: Indicates whether the MAXLink client software is enabled.

Usage: The MAXLink-Client-Enabled setting is read only. Yes indicates that the MAXLink client software is enabled. No indicates that the MAXLink client software is not enabled.

Example: `maxlink-client-enabled = enabled`

Location: Base

See Also: Frame-Relay-Enabled, Modem-Dialout-Enabled

Max-PAP-Auth-Retry

Description: Determines the maximum number of retries allowed if PAP authentication for a network connection fails.

Usage: Specify a number from 0 to 5. The default is 0 (zero).

Example: `set max-pap-auth-retry = 3`

Dependencies: A read-only copy of the Max-PAP-Auth-Retry setting appears in the IP-Options subprofile.

Location: Answer-Defaults > PPP-Answer, Connection > PPP-Options

See Also: Auth-For-Async-Framed-User, Pool-For-Async-Framed-User

Max-Pd

Description: Specifies the maximum number of sequenced data PDFs between poll intervals.

Usage: Specify an integer from 1 to 64. The default value is 25.

Example: `set max-pd = 32`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options > QSAAL-Options

See Also: Max-Cc, Max-Stat, Tcc-ms, Tidle-ms, Tkeepalive-ms, Thoresponse-ms, Tpoll-ms, Window-Size

Max-QTP-PDU-Size

Description: Specifies the maximum number of bytes a Quick Transaction Protocol (QTP) message sent by the TAOS unit can contain.

Usage: Specify a number from 1 to 1460. The default is 512.

Example: `set max-qtp-pdu-size = 500`

Location: Transaction-Server

See Also: QTP-Port

Max-Rate

Description: Specifies how the unit modifies the rate negotiation between the originating and destination fax terminals.

Usage: Values assigned to this parameter affect the MultiVoice unit's rate negotiation as follows:

- 14400 (the default) specifies that the unit masks the fax capabilities in the DIS frames that support fax data transmission at rates higher than 14,400bps.
- 9600 specifies that the unit masks the fax capabilities in the DIS frames that support fax data transmission at rates higher than 9600bps.
- 4800 specifies that the unit masks the fax capabilities in the DIS frames that support fax data transmission at rates higher than 4800bps.
- 2400 specifies that the unit masks the fax capabilities in the DIS frames that support fax data transmission at rates higher than 2400bps.

Example: `set max-rate = 9600`

Dependencies: The Max-Rate setting does not apply when RT-Fax-Enable is set to No.

Location: VoIP { *x y* } > RT-Fax-Options

See Also: RT-Fax-Enable

Max-Restart

Description: Specifies the maximum number of unacknowledged transmit RESTART messages.

Usage: Specify an integer from 1 to 32. The default value is 2.

Example: `set max-restart = 1`

Location: ATM-Interface { {shelf-*N* slot-*N N*} *N* } > SVC-Options > Q93B-Options

See Also: Max-Statenv, T303-ms, T308-ms, T309-ms, T310-ms, T313-ms, T316-ms, T322-ms

Max-Source-Port

Description: Specifies the highest Rlogin source port value.

Usage: Specify an integer from 128 to 1023. The default is 1023. The value you specify should be greater than or equal to the setting of Min-Source-Port.

Example: `set max-source-port = 250`

Dependencies: Rlogin must be enabled for Max-Source-Port to have any effect.

Location: Terminal-Server > Terminal-Mode-Configuration > Rlogin-Options

See Also: Min-Source-Port, Rlogin

Max-Stat

Description: Specifies the maximum length of a STAT PDU.

Usage: Specify an integer from 32 to 128. The default value is 67.

Example: `set max-stat = 64`

Location: ATM-Interface { {shelf-*N* slot-*N N*} *N* } > SVC-Options > QSAAL-Options

See Also: Max-Cc, Max-Pd, Tcc-ms, Tidle-ms, Tkeepalive-ms, Tnoresponse-ms, Tpoll-ms, Window-Size

Max-Statenq

Description: Specifies the maximum number of unacknowledged transmit STATUS ENQ messages.

Usage: Specify an integer from 1 to 32. The default is 1.

Example: `set max-statenq = 2`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options > Q93B-Options

See Also: Max-Restart, T303-ms, T308-ms, T309-ms, T310-ms, T313-ms, T316-ms, T322-ms

Max-Tunnels

Description: Specifies the maximum number of Mobile Clients that can use Ascend Tunnel Management Protocol (ATMP) to tunnel into the home network at the same time through the connection.

Usage: Specify an integer. The default is 0 (zero), which specifies that no limit is enforced.

Example: `set max-tunnels = 5`

Dependencies: You must set Profile-Type to Gateway-Profile for Max-Tunnels to apply.

Location: Connection *station* > Tunnel-Options

See Also: Primary-Tunnel-Server, Secondary-Tunnel-Server

MBONE-LAN-Interface

Description: Specifies the interface address of the local Ethernet port on which the MBONE router resides (the MBONE interface). The address can denote a local Ethernet port or a WAN link, but not both.

Usage: Specify the MBONE interface address. The default is null.

Example: `set mbone-lan-interface = { {shelf-1 slot-6 2} 0 }`

Dependencies: Do not set both the MBONE-LAN-Interface and MBONE-Profile settings.

Location: IP-Global

See Also: Interface-Address, MBONE-Profile, Multicast-Forwarding

MBONE-Profile

Description: Specifies the name of a Connection profile the TAOS unit uses to reach the MBONE router.

Usage: Specify the name of a Connection profile. The default is null.

Example: `set mbone-profile = mbone`

Dependencies: Do not set both the MBONE-LAN-Interface and MBONE-Profile settings.

Location: IP-Global

See Also: MBONE-LAN-Interface, Multicast-Forwarding

Mcast-Monitor-Enabled

Description: Specifies whether the system generates a trap when multicast heartbeat monitoring is configured and the system did not receive the configured number of heartbeat packets on a multicast interface.

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

- Yes specifies that the system generates a trap when it does not receive the configured number of heartbeat packets on a multicast interface.
- No specifies that the system does not generate a trap when it does not receive the configured number of heartbeat packets on a multicast interface.

Example: `set mcast-monitor-enabled = no`

Location: Trap *host-name*

See Also: Multicast-Hbeat-Alarm-Threshold, Multicast-Hbeat-Number-Slot, Multicast-Hbeat-Port, Multicast-Hbeat-Slot-Time, Multicast-Hbeat-Src-Addr, Multicast-Hbeat-Src-Addr-Mask

MD5-Authen-Key

Description: Specifies the secret key to be used for the MD5 cryptographic authentication method.

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

See Also: MD5-Auth-Key

MD5-Auth-Key

Description: Specifies the secret key to be used for the 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-Authen-Key setting, because the Auth-Key value no longer applies.

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface {shelf-*N* slot-*N* *N*} > OSPF

See Also: MD5-Authen-Key

Media-Speed-Mbit

Description: Specifies the speed of the Ethernet port.

Usage: Specify one of the following settings:

- 10mb specifies 10Mbps.
- 100mb (the default) specifies 100Mbps.

Example: `set media-speed-mbit = 10mb`

Location: Ethernet {shelf-*N* slot-*N* *N*}

Megaco-Link-Status-Enabled

Description: Specifies whether a trap is generated to report the status of the link between the Signaling System 7 (SS7) media gateway and the TAOS unit. This trap indicates that the operational status of a media gateway control link has changed from any state to the UP state, or from the UP state to any other state. The trap contains the name of the link, which is always reported as `default`, and the new operational status.

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

- Yes specifies that a trap is generated to report the status of the link between the SS7 media gateway and the TAOS unit.
- No specifies that a trap is not generated to report the status of the link between the SS7 media gateway and the TAOS unit.

Example: `set megaco-link-status-enabled = yes`

Dependencies: Changes to the setting of Megaco-Link-Status-Enabled become effective when you write the Trap profile.

Location: Trap *name*

See Also: LinkDown-Enabled, LinkUp-Enabled

Menu-Mode-Options

Description: A subprofile containing terminal-server configuration options for menu mode.

Usage: With Terminal-Server as the working profile, list the Menu-Mode-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Menu-Mode-Options subprofile:

```
admin> list menu-mode-options
[ in TERMINAL-SERVER:menu-mode-options ]
start-with-menus = no
toggle-screen = no
remote-configuration = no
text-1 = " "
host-1 = 0.0.0.0
service-1 = telnet
port-1 = 0
user-1 = " "
text-2 = " "
host-2 = 0.0.0.0
service-2 = telnet
port-2 = 0
user-2 = " "
text-3 = " "
host-3 = 0.0.0.0
service-3 = telnet
port-3 = 0
user-3 = " "
text-4 = " "
host-4 = 0.0.0.0
service-4 = telnet
port-4 = 0
user-4 = " "
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server

See Also: Host-N, Port-N, Remote-Configuration, Service-N, Start-With-Menus, Text-N, Toggle-Screen, User-N

Metric

Description: Specifies a Routing Information Protocol (RIP)-style metric for the route.

Usage: Specify an integer from 1 to 15. In an IP-Route profile, the default is 1. In a Route-Description-List *N* subprofile, the default is 8. The higher the metric, the less likely that the TAOS unit uses the route.

Example: `set metric = 8`

Location: IP-Route *name*,
Private-Route-Table *name* > Route-Description-List > Route-Description-List *N*

See Also: RIP, RIP-Mode, Routing-Metric

Metric-Max

Description: Specifies the maximum metric for a transaction server. If the metric exceeds the maximum, the transaction server is removed from an active list.

Usage: Specify a number from 0 to 255. The default is 15.

Example: `set metric-max = 25`

Location: Transaction-Server

See Also: Hunting-Mechanism

MFR-Bundle-Name

Description: Specifies the name of a Multilink Frame Relay (MFR) bundle.

- In a Multi-Link-FR profile, MFR-Bundle-Name defines a name for the bundle.
- 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 to an MFR bundle.

Usage: Specify the name of a Multi-Link-FR profile. The name can contain up to 15 characters and must be unique system-wide.

Example: `set mfr-bundle-name = mfr 1`

Dependencies: Consider the following:

- All member data links must specify the name of the same Multi-Link-FR profile.
- To enable a line to support both MFR and non-MFR links, the bundle name in a Frame-Relay profile must be null.

Location: Connection *station* > FR-Options, Frame-Relay *fr-name*, Multi-Link-FR *name*

See Also: Active, MFR-Bundle-Type, Max-Bundle-Members, Min-Bandwidth

MFR-Bundle-Type

Description: Specifies the type of MFR configuration.

Usage: In this release, only the MFR-DTE type is supported.

Example: `set mfr-bundle-type = mfr-dte`

Location: Multi-Link-FR *name*

See Also: Active, Max-Bundle-Members, MFR-Bundle-Name, Min-Bandwidth

Min-Bandwidth

Description: Specifies the minimum aggregated bandwidth before the 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 *name*

See Also: Active, Max-Bundle-Members, MFR-Bundle-Name, MFR-Bundle-Type

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 = 1`

Location: Answer-Defaults > MP-Answer, Connection *station* > MP-Options

See Also: Base-Channel-Count, Enabled, Maximum-Channels, MP-Answer, MP-Options

Min-Source-Port

Description: Specifies the lowest Rlogin source port value.

Usage: Specify an integer from 128 to 1023. The default is 1023. The value you specify must be less than or equal to the setting of Max-Source-Port.

Example: `set min-source-port = 250`

Dependencies: Rlogin must be enabled for Min-Source-Port to have any effect.

Location: Terminal-Server > Terminal-Mode-Configuration > Rlogin-Options

See Also: Max-Source-Port, Rlogin

Mode-Callback-Control

Description: Specifies the method of Callback Control Protocol (CBCP) callback the TAOS unit offers the incoming caller.

Usage: Specify one of the following values:

- CBCP-No-Callback (the default) specifies that no callback method is offered. This setting applies to Windows NT or Windows 95 clients who must not be called back. Because CBCP has been negotiated initially, the Windows clients must have validation from the TAOS unit that no callback is used for the connection.
- CBCP-User-Number specifies that the caller supplies the number that the TAOS unit uses for the callback.
- CBCP-Profile-Num specifies that the TAOS unit uses the number specified by the Dial-Number setting for the callback.
- CBCP-All specifies that the caller has the option of supplying the number or specifying that no callback is used for the call. If no callback takes place, the call will not be disconnected by the TAOS unit.

Example: `set mode-callback-control = cbcp-user-number`

Location: Connection *station* > PPP-Options

See Also: CBCP-Enabled, Trunk-Group-Callback-Control

Modem-Configuration

Description: A subprofile containing options for configuring the unit's digital modems.

Usage: With Terminal-Server as the working profile, list the Modem-Configuration subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Modem-Configuration subprofile:

```
admin> list modem-configuration
[ in TERMINAL-SERVER:modem-configuration]
v42/mnp = will-v42
max-baud-rate = 33600-max-baud
modem-transmit-level = -10-db-mdm-trn-level
cell-mode-first = no
cell-level = -18-db-cell-level
7-even = no
AT-answer-string = " "
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server

See Also: 7-Even, AT-Answer-String, Cell-Level, Cell-Mode-First, Max-Baud-Rate, Modem-Transmit-Level, V42/MNP

Modem-Dialout-Enabled

Description: Indicates whether modem dial-out is enabled for the unit.

Usage: The Modem-Dialout-Enabled setting is read only. Yes indicates that modem dial-out is enabled. No indicates that modem dial-out is disabled.

Example: modem-dialout-enabled = yes

Location: Base

See Also: Modem-Configuration, Modem-Disable-Mode, Modem-Table-Index, Modem-Transmit-Level

Modem-Disable-Mode

Description: Specifies the state of each of the digital modems in a card. The setting might also affect a B channel of a T1 PRI line.

Usage: Specify one of the following values:

- Enable (the default) enables the modem. When you change the value from Disable or DIS-Channel to Enable, the TAOS unit removes the modem from the Disabled list and places it on the Good or the Suspect list, provided that the Device-State and Admin-State are both enabled.
- Disable disables the modem. The TAOS unit moves the modem to the Disabled list. If the modem has an active call, it is not disabled until the call terminates. For idle modems, changes are effective immediately.
- DIS-Channel temporarily disables the modem and an arbitrary idle B channel of a T1 PRI line. The TAOS unit moves the modem to the Disabled list. If the card goes down, the unit restores a DS0 channel for each modem whose setting is DIS-Channel. Restoring a channel might take a few minutes.

Even if the modem failed a Power On Self-Test (POST), the DIS-Channel setting still quiesces a DS0 channel. Although the modem cannot be made available, changing this setting to Enable restores the quiesced DS0 channel. If the unit has no T1 PRI lines enabled, the DIS-Channel setting has the same effect as Disable.

Example: To disable modem 20 in slot 6:

```
admin> read lan-modem {1 6 0}
LAN-MODEM/{ shelf-1 slot-6 0 } read
admin> list
[in LAN-MODEM/{ shelf-1 slot-6 0 }]
physical-address* = { shelf-1 slot-6 0 }
modem-disable-mode = [enable enable enable enable enable enable
+
admin> list modem-disable-mode
[in LAN-MODEM/{ shelf-1 slot-6 0 }:modem-disable-mode]
...(All 48 modem settings are displayed)
admin> list 20
admin> set modem-disable-mode = disable
```

Location: LAN-Modem {shelf-N slot-N N}

See Also: Modem-Configuration, Modem-Dialout-Enabled, Modem-Table-Index, Modem-Transmit-Level

Modem-Mod

Description: Sets the modem modulation to use when answering calls on a 56-Kbps modem.

Usage: Specify one of the following values:

- K56-Modulation specifies that the card can operate at a normal rate.
- V34-Modulation specifies that the card never exceeds V.34 speeds (33.6K) and does not send the V.8bis tone.
- V90-Modulation (the default) specifies that the card operates at V.90 modulation.

Example: `set modem-mod = v34-modulation`

Location: Terminal-Server > Modem Configuration

See Also: 7-Even, Cell-Level, Cell-Mode-First, Max-Baud-Rate, Modem-Transmit-Level, V42/MNP

Modem-Table-Index

Description: 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.

Location: Admin-State {shelf-*N* slot-*N* *N*}, Admin-State-Phys-If {shelf-*N* slot-*N* *N*}

See Also: Modem-Configuration, Modem-Dialout-Enabled, Modem-Disable-Mode, Modem-Transmit-Level

Modem-Transmit-Level

Description: Specifies the transmit attenuation level for a digital modem. When a modem calls, the TAOS unit attempts to connect at the transmit level you specify.

Usage: Generally, you do not need to change the transmit level. However, when the carrier is aware of line problems or irregularities, you might need to alter the modem's transmit level by specifying one of the following values:

- 13-dB-Mdm-Trn-Level (-13 dB, the default)
- 14-dB-Mdm-Trn-Level (-14 dB)
- 15-dB-Mdm-Trn-Level (-15 dB)
- 16-dB-Mdm-Trn-Level (-15 dB)
- 17-dB-Mdm-Trn-Level (-15 dB)
- 18-dB-Mdm-Trn-Level (-15 dB)

Example: `set modem-transmit-level = -13-db-mdm-trn-level`

Dependencies: If terminal services are disabled, Modem-Transmit-Level does not apply. For a 56-Kbps modem, accept the default of -10-dB-Mdm-Trn-Level.

Location: Terminal-Server > Modem-Configuration

See Also: Modem-Configuration, Modem-Dialout-Enabled, Modem-Disable-Mode, Modem-Table-Index

More

Description: Specifies whether the TAOS unit includes the next filter rule before determining whether the frame matches the generic filter.

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

- Yes links the current filter rule to the next one so that the filter can examine multiple noncontiguous bytes within a packet. The TAOS unit applies the next filter before determining whether to forward the packet. The match occurs only if *both* sets of noncontiguous bytes contain the specified values.
- No does not link the current filter rule to the next one. The TAOS unit makes its forwarding decision solely on the basis of the current rule.

Example: `set more = no`

Dependencies: If you set More to Yes, the next filter must be enabled. Otherwise, the TAOS unit ignores the filter.

Location: Filter *filter-name* > Input-Filters > Gen-Filter,
Filter *filter-name* > Output-Filters > Gen-Filter

See Also: Gen-Filter, Input-Filters, Output-Filters

MP-Answer

Description: An Answer-Defaults subprofile containing Multilink Protocol (MP) encapsulation settings.

Usage: With Answer-Defaults as the working profile, list the MP-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

```
admin> list mp-answer
[ in ANSWER-DEFAULTS:mp-answer ]
enabled = yes
minimum-channels = 1
maximum-channels = 2
bacp-enable = no
```

Location: Answer-Defaults

See Also: BACP-Enable, Enabled, Minimum-Channels, Maximum-Channels

MP-Options

Description: A Connection subprofile containing Multilink Protocol (MP) encapsulation settings.

Usage: With a Connection profile as the working profile, list the MP-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: admin> **list mp-options**
[in CONNECTION/tim:mp-options]
base-channel-count = 1
minimum-channels = 1
maximum-channels = 2
bacp-enable = no

Dependencies: MP encapsulation must be enabled in the Answer-Defaults profile.

Location: Connection *station*

See Also: BACP-Enable, Base-Channel-Count, Minimum-Channels, Maximum-Channels

MPP-Answer

Description: An Answer-Defaults subprofile containing Multilink Protocol Plus (MP+) encapsulation settings.

Usage: With Answer-Defaults as the working profile, list the MPP-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: admin> **list mpp-answer**
[in ANSWER-DEFAULTS:mpp-answer]
enabled = yes
dynamic-algorithm = quadratic
bandwidth-monitor-direction = transmit
increment-channel-count = 1
decrement-channel-count = 1
seconds-history = 15
add-persistence = 5
sub-persistence = 10
target-utilization = 70

Location: Answer-Defaults

See Also: Add-Persistence, Bandwidth-Monitor-Direction, Decrement-Channel-Count, Dynamic-Algorithm, Enabled, Increment-Channel-Count, Seconds-History, Sub-Persistence, Target-Utilization

MPP-Options

Description: A Connection subprofile containing Multilink Protocol Plus (MP+) encapsulation settings.

Usage: With a Connection profile as the working profile, list the MPP-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

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

Dependencies: MP+ encapsulation must be enabled in the Answer-Defaults profile.

Location: Connection *station*

See Also: Add-Persistence, Aux-Send-Password, Bandwidth-Monitor-Direction, Decrement-Channel-Count, Dynamic-Algorithm, Increment-Channel-Count, Seconds-History, Sub-Persistence, Target-Utilization

MRU

Description: Specifies the maximum number of bytes that the TAOS 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 a Point-to-Point Protocol (PPP) connection, the default is 1524. Accept the default unless the device at the remote end of the link cannot support it.
- For a Frame Relay connection, the default is 1532.

Example: **set mru = 1524**

Location: Answer-Defaults > PPP-Answer, Connection *station* > PPP-Options, Frame-Relay *fr-name*

See Also: MTU

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 *name*

See Also: Active-Enabled, Host-Port, Notify-Tag-List, Security-Level, Security-Model, Security-Name, Tag, Target-Params-Name

MTU

Description: Specifies the maximum number of bytes that the TAOS unit can send in a single packet.

Usage: Specify an integer from 128 to 1524 bytes. The default is 1524.

Example: `set mtu = 1500`

Location: Answer-Defaults > PPP-Answer, Connection *station* > PPP-Options

See Also: MRU

MTU-Limit

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

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

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

Example: `set mtu-limit = 1472`

Location: ATMP

See Also: Agent-Mode, Agent-Type, Force-Fragmentation, Password, Retry-Limit, Retry-Timeout, UDP-Port

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 *name*

See Also: Data-IP-Address, Multicast-Interface-IP-Address

Multicast-Allowed

Description: Enables or disables multicasting on the IP interface.

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

- Yes enables the TAOS unit to respond to IGMP client requests and responses.
- No specifies that the TAOS unit 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 TAOS 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 TAOS unit can forward multicast traffic.

Location: Connection *station* > IP-Options, IP-Interface {shelf-*N* slot-*N* *N*}

See Also: IP-Global, IP-Options, Multicast-Forwarding, Multicast-Member-Timeout, Multicast-Rate-Limit

Multicast-Forwarding

Description: Enables or disables multicast forwarding for the TAOS unit.

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

- Yes enables multicast forwarding.
- No disables multicast forwarding.

Example: `set multicast-forwarding = yes`

Dependencies: Consider the following:

- For Multicast-Forwarding to have any effect, you must set MBONE-LAN-Interface or MBONE-Profile to specify the interface on which the MBONE router resides.
- When the value of Multicast-Forwarding changes from No to Yes, the multicast subsystem reads the values in the IP-Global profile and initiates the forwarding function. If you modify a multicast value in the IP-Global profile, you must set Multicast-Forwarding to No and then Yes again to force a read of the new values.

Location: IP-Global

See Also: Multicast-Allowed, Multicast-Member-Timeout, MBONE-LAN-Interface, MBONE-Profile

Multicast-Group-Leave-Delay

Description: Specifies the number of seconds the TAOS unit waits before forwarding an Internet Group Management Protocol (IGMP) version 2 `leave group` message from a multicast client.

Usage: Specify a number of seconds from 0 to 120. The default is 0 (zero). If you specify a value other than the default, and the TAOS 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 TAOS unit does not receive a response from an active multicast client that belongs to the client group, it sends a `leave group` message when the time you specify expires.

If you accept the default, the TAOS unit forwards a `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, set Multicast-Group-Leave-Delay to a value of 10 to 20 seconds.

Example: `set multicast-group-leave-delay = 15`

Dependencies: Multicast-Group-Leave-Delay applies only if you set Multicast-Forwarding to Yes and Multicast-Allowed to Yes.

Location: Connection > IP-Options, IP-Interface

See Also: Multicast-Allowed, Multicast-Forwarding, Multicast-Member-Timeout, Multicast-Rate-Limit

Multicast-Hbeat-Addr

Description: Specifies a multicast address for heartbeat monitoring. The TAOS unit listens for packets to and from the associated group

When it runs as a multicast forwarder, the TAOS unit continually receives multicast traffic. Using heartbeat monitoring, you can monitor for possible connectivity problems by polling for multicast traffic. The TAOS unit generates a Simple Network Management Protocol (SNMP) alarm trap if a traffic breakdown occurs.

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: Consider the following:

- All the Multicast-Hbeat values interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.
- Using the Multicast-Hbeat-Port, Multicast-Hbeat-Src-Addr, and Multicast-Hbeat-Src-Addr-Mask settings, you can fine-tune the specification for which packets the TAOS unit monitors.

Location: IP-Global

See Also: Multicast-Hbeat-Alarm-Threshold, Multicast-Hbeat-Number-Slot, Multicast-Hbeat-Port, Multicast-Hbeat-Slot-Time, Multicast-Hbeat-Src-Addr, Multicast-Hbeat-Src-Addr-Mask

Multicast-Hbeat-Alarm-Threshold

Description: Specifies the minimum number of packets the TAOS unit can receive without generating an alarm trap.

Usage: Specify an integer. The default is 0 (zero), which disables heartbeat monitoring.

Example: `set multicast-hbeat-alarm-threshold = 3`

Dependencies: All the Multicast-Hbeat values interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Location: IP-Global

See Also: Multicast-Hbeat-Addr, Multicast-Hbeat-Number-Slot, Multicast-Hbeat-Port, Multicast-Hbeat-Slot-Time, Multicast-Hbeat-Src-Addr, Multicast-Hbeat-Src-Addr-Mask

Multicast-Hbeat-Number-Slot

Description: Specifies how many times the TAOS unit polls before comparing the number of multicast packets it received to the Multicast-Hbeat-Alarm-Threshold value.

Usage: Specify the number of times the TAOS unit polls for packets. The default is 0 (zero).

Example: `set multicast-hbeat-number-slot = 5`

In this example, if you set Multicast-Hbeat-Number-Slot to 5, and Multicast-Hbeat-Slot-Time to 3 seconds, the TAOS unit polls 5 times at 3-second intervals. After 60 seconds of elapsed time, it compares the number of multicast packets received to the alarm threshold.

Dependencies: All the Multicast-Hbeat values interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Location: IP-Global

See Also: Multicast-Hbeat-Addr, Multicast-Hbeat-Alarm-Threshold, Multicast-Hbeat-Port, Multicast-Hbeat-Slot-Time, Multicast-Hbeat-Src-Addr, Multicast-Hbeat-Src-Addr-Mask

Multicast-Hbeat-Port

Description: Specifies a UDP port number. If specified, heartbeat monitoring listens only for multicast packets received on that 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 heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Location: IP-Global

See Also: Multicast-Hbeat-Addr, Multicast-Hbeat-Alarm-Threshold, Multicast-Hbeat-Number-Slot, Multicast-Hbeat-Slot-Time, Multicast-Hbeat-Src-Addr, Multicast-Hbeat-Src-Addr-Mask

Multicast-Hbeat-Slot-Time

Description: Specifies the interval (in seconds) in which the TAOS 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 heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Location: IP-Global

See Also: Multicast-Hbeat-Addr, Multicast-Hbeat-Alarm-Threshold, Multicast-Hbeat-Number-Slot, Multicast-Hbeat-Port, Multicast-Hbeat-Src-Addr, Multicast-Hbeat-Src-Addr-Mask

Multicast-Hbeat-Src-Addr

Description: Specifies a multicast address. When it performs heartbeat monitoring, the TAOS unit ignores packets from the IP address you specify.

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

Example: `set multicast-hbeat-src-addr = 10.1.2.3`

Dependencies: All the Multicast-Hbeat values interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Location: IP-Global

See Also: Multicast-Hbeat-Addr, Multicast-Hbeat-Alarm-Threshold, Multicast-Hbeat-Number-Slot, Multicast-Hbeat-Port, Multicast-Hbeat-Slot-Time, Multicast-Hbeat-Src-Addr-Mask

Multicast-Hbeat-Src-Addr-Mask

Description: Specifies a subnet mask that the TAOS unit applies to the Multicast-Hbeat-Src-Addr value.

Usage: Specify a subnet mask in dotted decimal notation. The default is 0.0.0.0.

Example: `set multicast-hbeat-src-addr-mask = 255.255.255.0`

Dependencies: All the Multicast-Hbeat values interact to enable heartbeat monitoring. Heartbeat monitoring is an optional function. It is not required for multicast forwarding.

Location: IP-Global

See Also: Multicast-Hbeat-Addr, Multicast-Hbeat-Alarm-Threshold, Multicast-Hbeat-Number-Slot, Multicast-Hbeat-Port, Multicast-Hbeat-Slot-Time, Multicast-Hbeat-Src-Addr

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 *name*

See Also: Data-IP-Address, Multicast-Address

Multicast-Member-Timeout

Description: Specifies the timeout (in seconds) for client responses to multicast polling messages.

When you configure the TAOS unit as a multicast forwarder, it forwards polling messages generated by the multicast router, and keeps track of active memberships from its client interfaces. If no client responds to the polling messages within the amount of time you specify for Multicast-Member-Timeout, the TAOS unit stops forwarding multicast traffic on that interface.

Usage: Specify an integer from 60 to 65535. The default is 360.

Example: `set multicast-member-timeout = 60`

Dependencies: If Multicast-Forwarding is set to No, Multicast-Member-Timeout does not apply.

Location: IP-Global

See Also: Multicast-Allowed, Multicast-Forwarding

Multicast-Rate-Limit

Description: Determines the rate at which the TAOS unit accepts multicast responses from clients on the interface, and enables the unit to forward multicast traffic on the interface (provided that Multicast-Allowed is set to Yes). The Multicast-Rate-Limit setting helps the forwarder prevent multicast clients from creating response storms to multicast transmissions. It does not affect the MBONE interface.

Usage: To begin forwarding multicast traffic on the interface, specify an integer lower than 100. The default is 100, which disables the forwarding of multicast traffic on the interface.

Example: `set multicast-rate-limit = 5`

In this example, the TAOS unit accepts a packet from multicast clients on the interface every 5 seconds. The unit discards any subsequent packets received in that 5-second window.

Dependencies: If you set Multicast-Allowed to Yes and Multicast-Rate-Limit remains at the default of 100, the TAOS 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 unit can forward multicast traffic.

Location: Connection *station* > IP-Options, IP-Interface {shelf-*N* slot-*N* *N*}

See Also: Multicast-Allowed

Multi-Link-FR

Description: A profile that enables you to configure Multilink Frame Relay (MFR).

Usage: Use the Read and List commands to read a Multi-Link-FR profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Multi-Link-FR profile `robin` the working profile and list its contents:

```
admin> list
[ in MULTI-LINK-FR/robin ]
mfr-bundle-name* = robin
active = no
mfr-bundle-type = mfr-dte
max-bundle-members = 1
min-bandwidth = 0
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
MULTI-LINK-FR/robin written
```

See Also: Active, Max-Bundle-Members, MFR-Bundle-Name, MFR-Bundle-Type, Min-Bandwidth

Multi-Rate-Enabled

Description: Indicates whether the unit can make DWS calls.

Usage: The Multi-Rate-Enabled setting is read only. 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

See Also: R2-Signaling-Enabled, Switched-Enabled

Must-Accept-Address-Assign

Description: Instructs the TAOS unit to hang up if a caller rejects dynamic IP address assignment.

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

- Yes specifies that the caller must accept dynamic IP address assignment.
- No specifies that the TAOS unit allows the caller to reject the IP address offered by the unit and to present its own IP address for consideration.

Example: `set must-accept-address-assign = yes`

Location: IP-Global

See Also: Assign-Address, Assign-Count, Pool-Base-Address, Pool-Summary

N

N2-Retransmissions

Description: Specifies the retry limit—the maximum number of times the TAOS unit can resend a frame on an X.75 connection when the T1 Retransmission Timer expires.

Usage: Specify a number from 2 to 10. The default value is 10. A higher value increases the probability of a correct transfer of data. A lower value allows for quicker detection of an error condition.

Location: Answer-Defaults > X75-Answer
Connection > X75-Options

See Also: Frame-Length, K-Frames-Outstanding, T1-Retrans-Timer

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 indicates that after six status requests spaced T391-Val seconds apart, the User-to-Network Interface–Data Terminal 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 *fr-name*

See Also: Link-Type, T391-Val

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 N393-Val. 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 *fr-name*

See Also: Link-Type, N393-Val

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 N392-Val. 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 *fr-name*

See Also: Link-Type, N392-Val

Nailed-Group

Description: Assigns a group number to a T1, E1, DS3-ATM, E3-ATM, OC3-ATM, or Serial WAN (SWAN) line. You can then refer to the number in the Connection profile's Nailed-Groups setting to specify the nailed-up channels a connection uses.

Usage: Specify a number from 0 to 1024. The default is 0 (zero).

Example: `set nailed-group = 7`

Dependencies: Do not associate a group number with more than one active profile. For a T1 or E1 line, channels in a nailed-up group must be contiguous.

Location: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
E1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line Config,
SWAN {shelf-*N* slot-*N* *N*} > Line-Config,
T1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*

See Also: Channel-Config *N*, Line-Config, Line-Interface, Nailed-Groups

Nailed-Groups

Description: Specifies one or more nailed-up groups belonging to a session.

Usage: Specify a number assigned to a group of nailed-up channels. For a Multilink Protocol Plus (MP+) connection, you can assign more than one group number, separated by commas. The default is 1.

Example: `set nailed-groups = 1, 3`

Dependencies: Only MP+ supports the use of multiple nailed-up groups.

Location: Connection *station* > Telco-Options

See Also: Call-Type, Nailed-Group, Telco-Options

Nailed-Mode

Description: Specifies how the TAOS unit uses the link's nailed-up channels, and whether the link uses nailed-up channels alone, or a combination of nailed-up and switched channels.

Usage: Specify one of the following values:

- FT1 (the default) specifies that the link uses only nailed-up channels.
- Off specifies that the TAOS unit does not use nailed channels.

Example: `set nailed-mode = ft1`

Dependencies: When you set Nailed-Mode to Off, the Data Link Connection Identifier (DLCI) Connection profile must specify a switched call type, a dial number, and a Calling-Line ID (CLID) or called number.

Location: Frame-Relay *fr-name*

See Also: Nailed-Up-Group

Nailed-Up-Group

Description: Specifies the group number assigned to nailed channels in a line profile, such as a T1 or E1 profile.

Usage: Specify a number assigned to a group of nailed-up channels. The default is 1. The maximum value you can enter is 1024.

Example: `set nailed-up-group = 5`

Dependencies: If the channels are on a nailed T1 line, make sure that the number of channels the TAOS unit uses for the link matches the number of channels used by the device at the other end. In addition, confirm that only one T1 profile specifies the number to be used by the Frame Relay data link.

Location: Frame-Relay *fr-name*

See Also: Nailed-Mode

Name

Description: Specifies a name.

- In all but the SNMPv3-USM-User profile, the Name value assigns a name to a profile, user, route, host, Virtual Router (VRouter), stack, interface, or the TAOS unit itself;
- In the SNMPv3-USM-User profile, the Name value specifies the user for whom the TAOS unit exchanges an SNMPv3 User-based Security Model (USM) message.

Usage: Specify a descriptive name with no embedded spaces.

- For all profiles except the IP-Route, IPX-Route, STM, Stacking, Trap, and VRouter profiles, you can specify up to 24 characters.
- For the IP-Route, IPX-Route, and Trap profiles, you can specify up to 31 characters.
- For the Stacking, SNMPv3-Notification, and SNMPv3-Target-Param profiles, you can specify up to 16 characters.

- For the STM, VRouter, and ATM-Interface profiles, you can specify up to 15 characters.
- For the IPSec, Private-Route-Table, and SNMPv3-USM-User profiles, you can specify up to 23 characters. In the 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 string `test!`.

The default is null in all except User profiles, where the default is `default`.

Example: `set name = newyork`

Dependencies: Consider the following:

- If the TAOS unit uses the specified value for authentication, it is case sensitive.
- In the SWAN profile, the Name setting identifies the line for administrative purposes only. The unit uses only the Physical-Address setting to identify the Serial WAN (SWAN) line.
- In the Private-Route-Table profile, the Name value is used to associate a Remote Authentication Dial-In User Service (RADIUS) or Connection profile with the defined private routes.
- To group interfaces belonging to the VRouter, specify the value of Name in the IP-Interface or Connection profile.
- All members of a stack specify the same name. Stacking control packets include the Name value to identify members of the same stack. Multiple stacks can exist on the same Ethernet segment if the stacks have different names.
- In the ATM-Interface profile, the name is optional and is used for informational purposes only.

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* }, ATMSVC-Route *name*, DS3-ATM {shelf-*N* slot-*N* *N*}, E1 {shelf-*N* slot-*N* *N*}, E3-ATM {shelf-*N* slot-*N* *N*}, Firewall *name*, IPSec, IP-Route *name*, IPX-Route *name*, OC3-ATM {shelf-*N* slot-*N* *N*}, OSPF-NBMA-Neighbor *name*, Private-Route-Table *name* > Route-Description-List > Route-Description-List *N*, SNMPv3-Notification, SNMPv3-Target-Param, SNMPv3-USM-User *name*, Stacking *name*, STM {shelf-*N* slot-*N* *N*}, SWAN {shelf-*N* slot-*N* *N*}, System, T1 {shelf-*N* slot-*N* *N*}, T3 {shelf-*N* slot-*N* *N*}, Trap *host-name*, User *name*, VRouter *name*

See Also: E1, E3-ATM, Firewall, IPSec, IP-Route, IPX-Route, Physical-Address, Private-Route-Table (profile), SNMPv3-USM-User, SWAN (profile), STM, System, T1, T3 (profile), Trap, User (profile)

NAS-Port-Type

Description: Specifies the type of service for the session.

Usage: Specify one of the following values:

- Any (the default) specifies that the incoming call is routed to an analog, digital, or virtual modem.
- Digital specifies that the incoming call is routed to a digital modem. The Digital setting restricts the profile to synchronous links, V.110 connections, and V.120 connections.
- Analog specifies that the incoming call is routed to an analog modem. The Analog setting restricts the profile to asynchronous connections on an analog line.

Example: `set nas-port-type = digital`

Location: Connection *station* > Telco-Options

Net-Alias

Description: Specifies the IPX network number of a remote router. The TAOS unit uses this network number only when connecting to a non-TAOS router that uses numbered interfaces.

Usage: Specify the IPX network number of the remote device. The default of 00000000 is appropriate for most installations. If you accept the default, the TAOS unit does not advertise the route until it makes a connection to the remote network.

Dependencies: If the TAOS unit does not route IPX for the connection, or if IPX routing is globally disabled, Net-Alias does not apply.

Location: Connection *station* > IPX-Options

See Also: Dial-Query, IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Number, Peer-Mode, RIP, SAP, SAP-Filter

NetBIOS-Primary-NS

Description: Specifies the IP address of the primary NetBIOS server.

Usage: Specify the IP address in dotted decimal notation. The default is 0.0.0.0, which indicates that no NetBIOS server exists.

Example: `set netbios-primary-ns = 10.1.2.3/24`

Location: IP-Global

See Also: Domain-Name, NetBIOS-Secondary-NS

NetBIOS-Secondary-NS

Description: Specifies the IP address of the secondary NetBIOS server. The TAOS unit accesses the secondary server if the primary NetBIOS server is unavailable.

Usage: Specify the IP address in dotted decimal notation. The default is 0.0.0.0, which indicates that no secondary NetBIOS server exists.

Example: `set netbios-secondary-ns = 10.57.24.11/24`

Location: IP-Global

See Also: Domain-Name, NetBIOS-Primary-NS

Netmask

Description: Specifies the subnet mask of the destination IP address for a private route.

Usage: Specify a subnet mask in dotted decimal notation. The default is 0.0.0.0.

Example: `set netmask = 255.255.255.240`

Dependencies: The value of Netmask is set automatically when you specify a prefix length as part of the IP address.

Location: Private-Route-Table *name* > Route-Description-List > Route-Description-List *N*

See Also: Dest-Address

Net-Number

Description: Specifies the IPX network number of the remote router.

Usage: Specify the IPX network number of the remote device only when the router requires that the TAOS unit know its network number before connecting. If you specify a value for Net-Number, the unit creates a static route to the device. In addition, the TAOS unit becomes a seed router, and other routers can learn the IPX network number from it.

If there are other NetWare routers on the LAN interface, the IPX number assigned to the TAOS unit for that interface must be consistent with the number in use by the other routers. The best way to ensure consistency is to accept the default null address for Net-Number. The null address causes the TAOS unit to learn its network number from another router on the interface, or from the Routing Information Protocol (RIP) packets received from the local IPX server.

The default of 00000000 is appropriate for most installations. If you accept the default, the TAOS unit does not advertise the route until it makes a connection to the remote network.

Dependencies: If the TAOS unit does not route IPX for the connection, or if IPX routing is globally disabled, Net-Number does not apply.

Location: Connection *station* > IPX-Options

See Also: Dial-Query, IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Alias, Peer-Mode, RIP, SAP, SAP-Filter

Network-Loopback

Description: Indicates whether the T1 line is looped back to the network.

Usage: The Network-Loopback setting is read only. True indicates that the T1 line is looped back to the network. False indicates that the T1 line is not looped back to the network.

Location: T1-Stat {shelf-*N* slot-*N* *N*}

See Also: AIS-Receive, BER-Receive, Carrier-Established, Channel-State, Error-Count, Line-State, Loss-Of-Carrier, Loss-Of-Sync, Physical-Address, Port-Enabled, Yellow-Receive

Network-Management-Enabled

Description: Indicates whether the network-management license is enabled.

Usage: The Network-Management-Enabled option is read only. Yes indicates that the network-management option is enabled. No indicates that the network-management option is disabled.

Example: `network-management-enabled = yes`

Dependencies: Consider the following:

- TAOS units with the network-management license enabled support security enhancements based on the SNMPv3 User-based Security Model (USM), which is compliant with RFC 2574.
- With the network-management license, the SNMPv3-USM-User profile is available. TAOS units support up to 100 configured SNMPv3-USM-User profiles. Configuring the profile enables the USM security features for the specified user.
- At present, encryption is not supported.

Location: Base

See Also: Network-Mgmt-VoIP-Enabled

Network-Mgmt-VoIP-Enabled

Description: Indicates whether the license for network management with Voice over IP (VoIP) is enabled.

Usage: The Network-Mgmt-VoIP-Enabled setting is read only. Yes indicates that the VoIP network-management option is enabled. No indicates that the VoIP network-management option is disabled.

Example: `network-mgmt-voip-enabled = yes`

Location: Base

See Also: Network-Management-Enabled

Network-Type

Description: Specifies the type of network to which the interface connects.

Usage: Specify one of the following settings:

- Broadcast specifies any broadcast-capable network, such as Ethernet.
- 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 (the default) specifies an interface connected to one other node on the remote end.

Example: `set network-type = broadcast`

Dependencies: The Non-Multicast value 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.

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF

See Also: Poll-Interval

NFAS-Group-ID

Description: Specifies the number of a Non-Facility Associated Signaling (NFAS) group.

Some sites require multiple NFAS groups on a single card to enable grouped DS1s. An NFAS group contains a minimum of two PRIs, so the T1 card supports up to four NFAS groups, and the T3 card supports up to 14 NFAS groups.

Usage: For a T1 card, set NFAS-Group-ID to a value from 0 to 3. For a T3 card, valid values are from 0 to 13. Lines with the same NFAS-Group-ID value are in the same NFAS group.

Example: Two NFAS groups are configured on a T1 card, each containing four lines. This example uses the NFAS group IDs 1 and 2, but you can assign any valid NFAS-Group-ID values. The following commands configure NFAS group 1, which contains lines 1 through 4:

```
admin> read t1 {1 2 1}
T1/{ shelf-1 slot-2 1 } read

admin> set line-interface signaling-mode = isdn-nfas
admin> set line-interface nfas-id = 0
admin> set line-interface nfas-group-id = 1
admin> set channel-config 24 channel-usage = nfas-primary
admin> write
T1/{ shelf-1 slot-2 1 } written

admin> read t1 {1 2 2}
T1/{ shelf-1 slot-2 2 } read

admin> set line-interface signaling-mode = isdn-nfas
admin> set line-interface nfas-id = 1
admin> set line-interface nfas-group-id = 1
admin> set line-interface channel-config 24 channel-usage =
nfas-secondary
admin> write
T1/{ shelf-1 slot-2 2 } written

admin> read t1 {1 2 3}
T1/{ shelf-1 slot-2 3 } read

admin> set line-interface signaling-mode = isdn-nfas
admin> set line-interface nfas-id = 2
admin> set line-interface nfas-group-id = 1
```

```
admin> write
T1/{ shelf-1 slot-2 3 } written
admin> read t1 {1 2 4}
T1/{ shelf-1 slot-2 4 } read
admin> set line-interface signaling-mode = isdn-nfas
admin> set line-interface nfas-id = 3
admin> set line-interface nfas-group-id = 1
admin> write
T1/{ shelf-1 slot-2 4 } written
```

The following commands configure NFAS group 2, which contains lines 5 through 8:

```
admin> read t1 {1 2 5}
T1/{ shelf-1 slot-2 5 } read
admin> set line-interface signaling-mode = isdn-nfas
admin> set line-interface nfas-id = 0
admin> set line-interface nfas-group-id = 2
admin> set channel-config 24 channel-usage = nfas-primary
admin> write
T1/{ shelf-1 slot-2 5 } written
admin> read t1 {1 2 6}
T1/{ shelf-1 slot-2 6 } read
admin> set line-interface signaling-mode = isdn-nfas
admin> set line-interface nfas-id = 1
admin> set line-interface nfas-group-id = 2
admin> set line-interface channel-config 24 channel-usage =
nfas-secondary
admin> write
T1/{ shelf-1 slot-2 6 } written
admin> read t1 {1 2 7}
T1/{ shelf-1 slot-2 7 } read
admin> set line-interface signaling-mode = isdn-nfas
admin> set line-interface nfas-id = 2
admin> set line-interface nfas-group-id = 2
admin> write
T1/{ shelf-1 slot-2 7 } written
admin> read t1 {1 2 8}
T1/{ shelf-1 slot-2 8 } read
admin> set line-interface signaling-mode = isdn-nfas
admin> set line-interface nfas-id = 3
admin> set line-interface nfas-group-id = 2
admin> write
T1/{ shelf-1 slot-2 8 } written
```

Dependencies: To configure multiple NFAS groups, you must set both NFAS-Group-ID and NFAS-ID for each DS1. Within the group, all PRIs share the same NFAS-Group-ID value and have different, unique NFAS-ID values.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: NFAS-ID

NFAS-ID

Description: Specifies a group ID for T1 lines that use Non-Facility Associated Signaling (NFAS). You must ask your service provider about the NFAS ID number to specify for each line. For an SS7 configuration, the NFAS-ID value specifies an interface ID for the T1 or E1 line used as an SS7 line.

Usage: Specify a number from 0 to 31.

Example: `set nfas-id = 2`

Dependencies: Consider the following:

- You assign a T1 line to an NFAS group by setting Signaling-Mode to ISDN-NFAS.
- Within the NFAS group, configure only a single line to provide the primary ISDN D channel, and another line to provide the secondary (backup) D channel.
- The NFAS-ID setting applies to SS7 lines only when the Q.931+ control protocol is used.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface, Signaling-Mode, Switch-Type

NL-Value

Description: Specifies the number of retransmissions the TAOS unit sends on the line.

Usage: Specify an integer from 1 to 255. The default is 64. You must accept the default when the line connects to a Digital Private Network Signaling System (DPNSS) or DASS 2 switch.

Example: `set nl-value = 64`

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface, Signaling-Mode, Switch-Type

NoAttr6-Use-Termsrv

Description: Specifies how the system behaves when it does not receive Remote Authentication Dial-In User Service (RADIUS) attribute 6 (User-Service).

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

- Yes specifies that the TAOS unit initiates a terminal-server login if Attribute 6 is not received, regardless of whether Attribute 7 is received or not.
- No specifies one of the following:
 - If Attribute 6 is not received, but Attribute 7 is received, a framed-protocol login is initiated.
 - If neither Attribute 6 nor 7 is received, a terminal-server login is initiated.

Example: The commands in the following example instruct the TAOS unit to start a framed-protocol login if Attribute 7 is received without Attribute 6:

```
admin> read external-auth
EXTERNAL-AUTH read
admin> set noattr6-use-termsrv = no
admin> write
EXTERNAL-AUTH written
```

Location: External-Auth

See Also: Acct-Type, Auth-Type, Local-Profiles-First, Rad-Acct-Client, Rad-Auth-Client, Rad-Auth-Server, Rad-Serv-Enable, Tac-Auth-Client, TacPlus-Acct-Client, TacPlus-Auth-Client

No-Conn-Ack-Increment

Description: Specifies the number by which to increase a transaction server's current metric if it does not send a Quick Transaction Protocol (QTP) Connect Acknowledgement in response to a QTP Connect Request sent by the TAOS unit.

Usage: Specify a number from 0 to 255. The default is 8.

Example: `set no-conn-ack-increment = 100`

Location: Transaction-Server

See Also: No-First-Status-Metric, No-Second-Status-Metric

No-First-Status-Metric

Description: Specifies a number to use as a transaction server's current metric the first time it does not send a Quick Transaction Protocol (QTP) Status Message within the timeout interval.

Usage: Specify a number from 0 to 255. The default is 10.

Example: `set no-first-status-metric = 100`

Location: Transaction-Server

See Also: No-Second-Status-Metric

Non-Multicast

Description: Specifies whether all multicast packets are remapped to a directed neighbor address.

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

- Yes specifies that all multicast packets are remapped to a directed neighbor address, enabling adjacencies to form between neighbors. This setting is ignored on Ethernet (a broadcast network). Its use is not recommended for unnumbered interfaces. If you specify it for a non-numbered interface, the TAOS unit drops the packets.
- No specifies that multicast packets are not remapped to a directed neighbor address.

Example: `set non-multicast = yes`

Location: Connection *station* > IP-Options > OSPF-Options

See Also: Active, Area, Area-Type, ASE-Tag, ASE-Type, Authen-Type, Auth-Key, Cost, Dead-Interval, Hello-Interval, Key-ID, Priority, Retransmit-Interval, Transit-Delay

No-Second-Status-Metric

Description: Specifies a number to use as a transaction server's current metric the second time it does not send a Quick Transaction Protocol (QTP) Status Message within the timeout interval.

Usage: Specify a number from 0 to 255. The default is 16.

Example: `set no-second-status-metric = 100`

Location: Transaction-Server

See Also: No-First-Status-Metric

Notify-Tag-List

Description: Specifies the tag list indicated by the Tag parameter value in each SNMPv3-Notification profile.

Usage: Specify the Tag value(s) you set in one or more SNMPv3-Notification profiles.

Example: `set notify-tag-list = default1`

Location: Trap *name*

See Also: Active-Enabled, Host-Port, Msg-Proc-Model, Security-Level, Security-Model, Security-Name, Tag, Target-Params-Name

Number-Complete

Description: Specifies the condition the MultiVoice gateway uses to determine the length of the dial string. Or, enables detection and collection of up to 15 digits for inbound dialed telephone numbers on MultiVoice gateways using E1 trunks supporting inband CMF R2.

Usage: Specify one of the following values:

- 1-Digits, 2-Digits, and so on, up to 15-Digits, specifies how many digits the MultiVoice gateway must receive before it accepts an incoming call.
- End-Of-Pulsing (the default) specifies that the MultiVoice gateway can accept the call when the end-of-pulsing signal is received. For call-routing purposes, the digits received before the call is answered are considered the called number.
- Time-Out specifies that the MultiVoice gateway resets the network idle timer after the initial digit is received, and then waits for silence. When silence is detected, the unit waits for the end of the interval specified by the Inter-Digit-Time-Out setting before collecting the next digit. The MultiVoice gateway continues to collect digits while waiting for the network idle timer to expire before continuing with call processing.

Example: `set number-complete = time-out`

Dependencies: Consider the following:

- E1 MFC-R2 signaling is country specific. For E1 MFC-R2 signaling, the MultiVoice gateway continues to collect digits until the on/off pulsing used to transmit the dial string is complete.
- The Signaling-Mode parameter, and the Country parameter in the System profile, must be set for the country-appropriate signaling in order for the MultiVoice gateway to properly detect dialed digits.
- Number-Complete does not apply when Signaling-Mode is set to E1-Kuwait-Signaling, ISDN, P7, DPNSS, or None.

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Country, Inter-Digit-Time-Out, Signaling-Mode, Switch-Type

Numbering-Plan

Description: Specifies the type of Switched Virtual Circuit (SVC) address.

Usage: Specify one of the following settings:

- Undefined (the default) specifies that an address has not been configured on the interface.
- ISDN specifies an E.164 address.
- AESA specifies an ATM End System Address (AESA).

The Unknown and X121 values are currently unsupported and have the same effect as the default Undefined.

Example: `set numbering-plan = ISDN`

Location: ATM-Interface { {shelf-*N* slot-*N* *N*} *N* } > SVC-Options > ATM-Address, Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr, Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr

See Also: E164-Native-Address, SVC-Address-Info

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.

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.

Dependencies: Consider the following:

- When the TAOS unit is configured to interoperate with an external application for dial-out, the external system and the TAOS unit *must agree* about the number of digits in a trunk-group number. Otherwise, telephone numbers will not be parsed correctly and calls will fail.
- Use-Trunk-Groups must be set to Yes for Num-Digits-Trunk-Groups to have an effect.
- Currently, the IP-Fax server supports 2-digit trunk groups, but the trunk-group specification must be within the range of 2 to 9. The TAOS unit and the IP-Fax server must agree about the number of digits in a trunk group. Otherwise, telephone numbers are not parsed correctly, and calls fail.

Location: System

See Also: Trunk-Group, Use-Trunk-Groups

O

OC3-ATM

Description: A profile containing configuration settings for an OC3-ATM card.

Usage: To make OC3-ATM the working profile and list its contents, use the Read and List commands. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the OC3-ATM profile with the { shelf-1 slot-1 0 } the working profile and list its contents:

```
admin> read oc3-atm { 1 1 0 }
OC3-ATM/{ shelf-1 slot-1 0 } read

admin> list
[in OC3-ATM/{ shelf-1 slot-1 0 }]
name = " "
physical-address* = { shelf-1 slot-1 0 }
enabled = no
line-config = { 0 1 { any-shelf any-slot 0 } no-loopback sdh +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
OC3-ATM/{ shelf-1 slot-1 0 } written
```

See Also: Enabled, Line-Config, Name, Physical-Address

Offset

Description: Specifies a byte-offset from the start of a frame to the data that the TAOS unit tests against the generic 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 endpoint 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`

Location: Filter *filter-name* > Input-Filters > Gen-Filter,
Filter *filter-name* > Output-Filters > Gen-Filter

See Also: Gen-Filter, Input-Filters, Output-Filters

Operational-Count

Description: 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

See Also: Device-Class, Disabled-Count, Total-Count

Operation-Mode

Description: Specifies the mode of operation in which to run the fantray.

Usage: Specify one of the following settings:

- Full-Speed-Only (the default) specifies that the fans in the fantray operate at full speed at all times.
- Lownoise-Speed-Only specifies that the fans operate at the low noise speed (as specified by the Fantray-Lownoise-RPM setting) at all times.
- Auto-Regulation specifies that the fan speeds are controlled dynamically on the basis of temperature. In Auto-Regulation mode, the fans run at low noise speed when the system starts up. The system monitors the unit temperature, and when it reaches a high-temperature threshold (as specified by the High-Temperature-Trigger setting), it switches the fans to full speed and logs a message. When the unit temperature falls below the low-temperature threshold (as specified by the Low-Temperature-Trigger setting), the system switches the fans back to low noise speed.

Example: `set operation-mode = lownoise-speed-only`

Location: Thermal

See Also: Fantray-Lownoise-RPM, High-Temperature-Trigger, Low-Temperature-Trigger

OSPF

Description: A subprofile that enables you to configure Open Shortest Path First (OSPF) routing on an Ethernet interface.

Note: For information about how to display statistical information related to OSPF routing, see “OSPF” on page 1-82.

Usage: With IP-Interface as the working profile, list the OSPF subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the OSPF subprofile:

```
admin> list ospf
[in IP-INTERFACE/{ { shelf-1 slot-15 2 } 0 }:ospf]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 10
dead-interval = 40
priority = 5
authen-type = simple
key-id = 0
auth-key = unit0
cost = 1
ase-type = type-1
```

```
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
network-type = point-to-point
poll-interval = 0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IP-Interface { {shelf-*N* slot-*N* *N*} *N*}

See Also: Active, Area, Area-Type, ASE-Tag, ASE-Type, Authen-Type, Auth-Key, Cost, Dead-Interval, Hello-Interval, Key-ID, Network-Type, Poll-Interval, Priority, Retransmit-Interval, Transit-Delay

OSPF-Approaching-Overflow-Enabled

Description: Enables or disables trap 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 Yes or No. The default is No.

- Yes enables generation of OSPF Trap 15.
- No disables generation of OSPF Trap 15.

Example: `set ospf-approaching-overflow-enabled = yes`

Location: Trap *name*

See Also: OSPF-LSDB-Overflow-Enabled,

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 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

Example: `set ospf-ase-pref = 100`

Location: IP-Global

See Also: Down-Preference, OSPF-Pref, Preference, RIP-Pref, Static-Pref

OSPF-Enabled

Description: Enables or disables generation of Open Shortest Path First (OSPF) traps to signal the occurrence of any of the following events:

OspfIfStateChange
OspfIfRxBadPacket
OspfTxRetransmit
OspfNbrStateChange
OspfVirtIfConfigError
OspfVirtIfAuthFailure
OspfVirtIfStateChange
OspfVirtIfRxBadPacket
OspfVirtIfTxRetransmit
OspfVirtNbrStateChange
OspfOriginateLsa
OspfMaxAgeLsa
OspfLsdbOverflow
OspfLsdbApproachingOverflow

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

- Yes specifies that trap generation depends on whether the specific OSPF trap is enabled.
- No specifies that OSPF traps are generated regardless of individual OSPF trap settings in the profile.

Example: `ospf-enabled = yes`

Location: Trap *name*

See Also: OSPF-Approaching-Overflow-Enabled, OSPF-IF-Auth-Failure-Enabled, OSPF-IF-Config-Error-Enabled, OSPF-IF-RX-Bad-Packet, OSPF-IF-State-Change-Enabled, OSPF-LSDB-Overflow-Enabled, OSPF-MaxAgeLSA-Enabled, OSPF-NBR-State-Change-Enabled, OSPF-OriginateLSA-Enabled, OSPF-TX-Retransmit-Enabled, OSPF-Virt-IF-Auth-Failure-Enabled, OSPF-Virt-IF-Config-Error-Enabled, OSPF-Virt-IF-RX-Bad-Packet, OSPF-Virt-IF-State-Change-Enabled, OSPF-Virt-IF-TX-Retransmit-Enabled, OSPF-Virt-NBR-State-Change-Enabled

OSPF-Global

Description: A subprofile that enables you to define global Open Shortest Path First (OSPF) behavior.

Usage: With IP-Global as the working profile, list the OSPF-Global subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the OSPF-Global subprofile:

```
admin> list ospf-global
[ in IP-GLOBAL:ospf-global ]
as-boundary-router = yes
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IP-Global

See Also: AS-Boundary-Router

OSPF-IF-Auth-Failure-Enabled

Description: Enables or disables trap generation if a packet has been received on a nonvirtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type (OSPF Trap 6).

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

- Yes specifies that OSPF Trap 6 is generated if a packet has been received on a nonvirtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.
- No specifies that OSPF Trap 6 is not generated if a packet has been received on a nonvirtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.

Example: `set ospf-if-auth-failure-enabled = yes`

Location: Trap *name*

See Also: OSPF-IF-Config-Error-Enabled, OSPF-IF-RX-Bad-Packet, OSPF-IF-State-Change-Enabled

OSPF-IF-Config-Error-Enabled

Description: Enables or disables trap 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: Specify Yes or No. The default is No.

- 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 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 *name*

See Also: OSPF-IF-Auth-Failure-Enabled, OSPF-IF-RX-Bad-Packet, OSPF-IF-State-Change-Enabled

OSPF-IF-RX-Bad-Packet

Description: Enables or disables trap generation if an Open Shortest Path First (OSPF) packet has been received on a nonvirtual interface that cannot be parsed (OSPF Trap 8).

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

- Yes specifies that OSPF Trap 8 is generated if an OSPF packet has been received on a nonvirtual interface that cannot be parsed.
- No 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 *name*

See Also: OSPF-IF-Auth-Failure-Enabled, OSPF-IF-Config-Error-Enabled, OSPF-IF-State-Change-Enabled

OSPF-IF-State-Change-Enabled

Description: Enables or disables trap 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: Specify Yes or No. The default is No.

- Yes specifies that OSPF Trap 16 is generated if the state of a nonvirtual OSPF interface has changed.
- No 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 *name*

See Also: OSPF-IF-Auth-Failure-Enabled, OSPF-IF-Config-Error-Enabled, OSPF-IF-RX-Bad-Packet

OSPF-LSDB-Overflow-Enabled

Description: Enables or disables trap generation if the number of Link-State Advertisements (LSAs) in the router's link-state database has exceeded `OSPFExtLsdbLimit` (OSPF Trap 14).

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

- Yes specifies that OSPF Trap 14 is generated if the number of LSAs in the router's link-state database has exceeded `OSPFExtLsdbLimit`.
- No 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 *name*

See Also: OSPF-Approaching-Overflow-Enabled

OSPF-MaxAgeLSA-Enabled

Description: Enables or disables trap generation if a Link-State Advertisement (LSA) in the router's link-state database has aged to `MaxAge` (OSPF Trap 13).

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

- Yes specifies that OSPF Trap 13 is generated if an LSA in the router's link-state database has aged to `MaxAge`.
- No 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 *name*

See Also: OSPF-OriginateLSA-Enabled

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: Use the Read and List commands to read an OSPF-NBMA-Neighbor profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the OSPF-NBMA-Neighbor profile megan the working profile and list its contents:

```
admin> read ospf-nbma-neighbor megan
OSPF-NBMA-NEIGHBOR/megan read

admin> list
[ in OSPF-NBMA-NEIGHBOR/megan ]
name* = megan
host-name = " "
ip-address = 0.0.0.0
dr-capable = no
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
OSPF-NBMA-NEIGHBOR/megan written
```

See Also: DR-Capable, Host-Name, IP-Address, Name

OSPF-NBR-State-Change-Enabled

Description: Enables or disables trap generation if the state of a nonvirtual Open Shortest Path First (OSPF) neighbor has changed (OSPF Trap 2).

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

- Yes specifies that OSPF Trap 2 is generated if the state of a nonvirtual OSPF neighbor has changed.
- No 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 (DR). A DR transitioning to Down is noted by `OSPFIfStateChange`.

Location: Trap *name*

See Also: OSPF-IF-State-Change-Enabled

OSPF-Options

Description: A subprofile that contains settings for Open Shortest Path First (OSPF) routing.

Usage: With a Connection profile as the working profile, list the OSPF-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the OSPF-Options subprofile:

```
admin> list ip-options ospf-options
[In CONNECTION/tim:ip-options:ospf-options]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 30
dead-interval = 120
priority = 5
authen-type = simple
key-id = 0
auth-key = unit0
cost = 10
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 = 0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station* > IP-Options

See Also: Active, Area, Area-Type, ASE-Tag, ASE-Type, Authen-Type, Auth-Key, Cost, Dead-Interval, Hello-Interval, Key-ID, Network-Type, Non-Multicast, Poll-Interval, Priority, Retransmit-Interval, Transit-Delay

OSPF-OriginateLSA-Enabled

Description: Enables or disables trap generation if a new Link-State Advertisement (LSA) has been originated by this router due to a topology change (OSPF Trap 12).

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

- 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 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 *name*

See Also: OSPF-MaxAgeLSA-Enabled

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 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 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

See Also: Down-Preference, OSPF-ASE-Pref, Preference, RIP-Pref, Static-Pref

OSPF-TX-Retransmit-Enabled

Description: Enables or disables trap 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: Specify Yes or No. The default is No.

- Yes specifies that the unit generates OSPF Trap 10 if an OSPF packet has been retransmitted on a nonvirtual interface.
- No 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 *name*

See Also: OSPF-IF-RX-Bad-Packet

OSPF-Virt-IF-Auth-Failure-Enabled

Description: Enables or disables trap generation if a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type (OSPF Trap 7).

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

- Yes specifies that the unit generates OSPF Trap 7 if a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.
- No specifies that the unit does not generate OSPF Trap 7 if a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.

Example: `set ospf-virt-if-auth-failure-enabled = yes`

Location: Trap *name*

See Also: OSPF-Virt-IF-Config-Error-Enabled, OSPF-Virt-IF-RX-Bad-Packet, OSPF-Virt-IF-State-Change-Enabled, OSPF-Virt-IF-TX-Retransmit-Enabled, OSPF-Virt-NBR-State-Change-Enabled

OSPF-Virt-IF-Config-Error-Enabled

Description: Enables or disables trap generation if a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters (OSPF Trap 5).

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

- Yes specifies that the unit generates OSPF Trap 5 if a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.
- No specifies that the unit does not generate OSPF Trap 5 if a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.

Example: `set ospf-virt-if-config-error-enabled = yes`

Dependencies: The event `optionMismatch` causes a trap only if it prevents an adjacency from forming.

Location: Trap *name*

See Also: OSPF-Virt-IF-Auth-Failure-Enabled, OSPF-Virt-IF-RX-Bad-Packet, OSPF-Virt-IF-State-Change-Enabled, OSPF-Virt-IF-TX-Retransmit-Enabled, OSPF-Virt-NBR-State-Change-Enabled

OSPF-Virt-IF-RX-Bad-Packet

Description: Enables or disables trap generation if an Open Shortest Path First (OSPF) packet has been received on a virtual interface that cannot be parsed (OSPF Trap 9).

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

- 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 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 *name*

See Also: OSPF-Virt-IF-Auth-Failure-Enabled, OSPF-Virt-IF-Config-Error-Enabled, OSPF-Virt-IF-State-Change-Enabled, OSPF-Virt-IF-TX-Retransmit-Enabled, OSPF-Virt-NBR-State-Change-Enabled

OSPF-Virt-IF-State-Change-Enabled

Description: Enables or disables trap generation if the state of an Open Shortest Path First (OSPF) virtual interface has changed (OSPF Trap 1).

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

- Yes specifies that the unit generates OSPF Trap 1 if the state of an OSPF virtual interface has changed.
- No 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 *name*

See Also: OSPF-Virt-IF-Auth-Failure-Enabled, OSPF-Virt-IF-Config-Error-Enabled, OSPF-Virt-IF-RX-Bad-Packet, OSPF-Virt-IF-TX-Retransmit-Enabled, OSPF-Virt-NBR-State-Change-Enabled

OSPF-Virt-IF-TX-Retransmit-Enabled

Description: Enables or disables trap 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 an LSDB entry. The LS type, LS ID, and Router ID are used to identify a link-state database entry.

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

- Yes specifies that the unit generates OSPF Trap 11 if an OSPF packet has been retransmitted on a virtual interface.
- No specifies that the unit does not generate OSPF Trap 11 if an OSPF packet has been retransmitted on a virtual interface.

Example: `set ospf-virt-if-tx-retransmit-enabled = yes`

Location: Trap *name*

See Also: OSPF-Virt-IF-Auth-Failure-Enabled, OSPF-Virt-IF-Config-Error-Enabled, OSPF-Virt-IF-RX-Bad-Packet, OSPF-Virt-IF-State-Change-Enabled, OSPF-Virt-NBR-State-Change-Enabled

OSPF-Virt-NBR-State-Change-Enabled

Description: Enables or disables trap generation if the state of an Open Shortest Path First (OSPF) virtual neighbor has changed (OSPF Trap 3).

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

- Yes specifies that the unit generates OSPF Trap 3 if the state of an OSPF virtual neighbor has changed.
- No 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 *name*

See Also: OSPF-Virt-IF-Auth-Failure-Enabled, OSPF-Virt-IF-Config-Error-Enabled, OSPF-Virt-IF-RX-Bad-Packet, OSPF-Virt-IF-State-Change-Enabled, OSPF-Virt-IF-TX-Retransmit-Enabled

Outgoing-Called-Addr

Description: A subprofile that enables you to specify the Asynchronous Transfer Mode (ATM) address of the remote end of a dial-out Switched Virtual Circuit (SVC) connection.

Usage: With a Connection profile as the working profile, enter `list atm-options svc-options outgoing-called-addr`. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Outgoing-Called-Addr subprofile:

```
admin> list atm-options svc-options outgoing-called-addr
[In CONNECTION/robin:atm-options:svc-options:outgoing-called-addr]
numbering-plan = undefined
e164-native-address = ""
aesa-address = { undefined { "" "" } { "" "" "" } }
svc-address-info = ""
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: To configure an SVC that can be initiated by either a dial-in or dial-out call, specify the same ATM address in both the Incoming-Caller-Addr and Outgoing-Called-Addr subprofiles.

Location: Connection *station* > ATM-Options > SVC-Options

See Also: AESA-Address, E164-Native-Address, Numbering-Plan, SVC-Address-Info

Outgoing-Fax-Port

Description: Specifies the TCP port on which to accept outgoing fax data from a fax server.

Usage: Specify a port number. The default is 10001.

Example: `set outgoing-fax-port = 100`

Dependencies: Outgoing fax data is received from the Internet and requires a dial-out to a destination fax machine.

Location: IP-Fax

See Also: Incoming-Fax-Port

Outgoing-Procedure

Description: Specifies the type of outgoing continuity checks to perform for all channels on a line.

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

- Single-Tone-2010 (the default) specifies that the TAOS unit sends a 2010Hz tone and expects to receive a 2010Hz tone in return. This procedure is generally known as a *4-wire continuity check*.
- Send-2010-Expect-1780 specifies that the TAOS unit sends a 2010Hz tone and expects to receive a 1780Hz tone in return. This procedure is generally known as a *2-wire continuity check*.
- Send-1780-Expect-2010 specifies that the TAOS unit sends a 1780Hz tone and expects to receive a 2010Hz tone in return. This procedure is generally known as a *4-wire-to-2-wire continuity check*.

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

- Single-Tone-2000 (the default) specifies that the TAOS unit sends a 2000Hz tone and expects to receive a 2000Hz tone in return. This procedure is generally known as a *4-wire continuity check*.
- Send-2000-Expect-1780 specifies that the TAOS unit sends a 2000Hz tone and expects to receive a 1780Hz tone in return. This procedure is generally known as a *2-wire continuity check*.
- Send-1780-Expect-2000 specifies that the TAOS unit sends a 1780Hz tone and expects to receive a 2000Hz tone in return. This procedure is generally known as a *4-wire-to-2-wire continuity check*.

Example: `set outgoing-procedure = send-2010-expect-1780`

Dependencies: If you change the type of continuity check, the new type is used for new continuity check requests on the line as soon as the line profile is saved. Existing check-loops that are already active on the line are not modified or canceled when the profile is saved.

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface > SS7-Continuity, T1 {shelf-*N* slot-*N* *N*} > Line-Interface > SS7-Continuity

See Also: Incoming-Procedure

Output-Filters

Description: A subprofile containing 12 output-filter configuration subprofiles. The TAOS unit applies output filters to outgoing packets.

Usage: With a Filter profile as the working profile, use the List command to display the 12 subprofiles of the Output-Filters subprofile.

Example: To list the contents of the Output-Filters subprofile:

```
admin> list output-filters
[in FILTER/test:output-filters]
output-filters[1] = { no no generic-filter { 0 0 no no +
output-filters[2] = { no no generic-filter { 0 0 no no +
output-filters[3] = { no no generic-filter { 0 0 no no +
output-filters[4] = { no no generic-filter { 0 0 no no +
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name*

See Also: Filter-Name, Input-Filters, Input-Filters N, Output-Filters N

Output-Filters N

Description: A subprofile containing one of the 12 levels of an output-filter specification in an Output-Filters subprofile.

Usage: With a Filter profile as the working profile, list one of the 12 subprofiles. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Output-Filters[1] subprofile:

```
admin> list output-filters 1
[in FILTER/test: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 +
ip-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 +
route-filter = { 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0 none }
ipx-filter = { 00:00:00:00 00:00:00:00 00:00:00:00:00:00 +
tos-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 +
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name* > Output-Filters

See Also: Filter-Name, Forward, Gen-Filter, Input-Filters, Input-Filters N, IP-Filter, Output-Filters, TOS-Filter (subprofile), Type, Valid-Entry

Output-IPX-SAP-Filters

Description: A subprofile that defines up to eight output filters for Service Advertising Protocol (SAP) packets. The TAOS unit applies output filters to SAP response packets it transmits. If it receives a SAP request packet, the unit applies output filters before transmitting the SAP response, and excludes services from (or includes them in) the response packet as specified by the filter conditions.

Usage: With IPX-SAP-Filter as the working profile, use the List command to display one of the Output-IPX-SAP-Filters subprofiles. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Output-IPX-SAP-Filters subprofile:

```
admin> list output-ipx-sap-filters 1
[ in IPX-SAP-FILTER/test:output-ipx-sap-filters[1]]
valid-filter = no
type-filter = exclude
server-type = 00:00
server-name = ""
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IPX-SAP-Filter

See Also: Server-Name, Server-Type, Type-Filter, Valid-Filter

Overlap-Receiving

Description: Enables or disables overlap receiving for incoming calls on the PRI line. Overlap receiving affects the procedure of establishing an incoming call received on a T1 or E1 PRI line in the TAOS unit. When you enable overlap receiving, the unit can gather the complete called number from the network switch via a series of Information messages, enabling the use of features such as called-number authentication.

The Q.931 specification states that either en-bloc receiving or overlap receiving can be used to handle an incoming call. With en-bloc receiving, the Setup message received from the network switch must contain all information required to process the call. With overlap receiving, the Setup message can contain incomplete called number information. The remainder of the call information (if any) is sent in one or more additional Information messages after the network switch receives a Setup Acknowledge message from the called unit.

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

- Yes enables overlap receiving.
- No disables overlap receiving.

Example: `set overlap-receiving = yes`

Dependencies: If Overlap-Receiving = No, the PRI-Prefix-Number, Trailing-Digits, and T302-Timer settings do not apply.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface, E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: PRI-Prefix-Number, T302-Timer, Trailing-Digits

P

Packet-Audio-Mode

Description: Specifies the preferred audio codec used by Voice over IP (VoIP) gateways to compress and uncompress analog speech and digital audio frames.

Usage: Specify one of the following values:

- G711-ULaw (the default) specifies a codec that uses G.711 U-Law encoding.
- G711-ALaw specifies a codec that uses G.711 A-Law encoding.
- G723 specifies a codec that uses G.723 5.3Kbps encoding.
- G729 specifies a codec that uses G.729 encoding.
- G723-6.4kps specifies a codec that uses G.723 6.4Kbps encoding.
- RT24 specifies a codec that uses RT24 encoding. RT-24 is a Lucent Technologies proprietary codec, which is available only on MultiVoice gateways running TAOS 8.0. MultiVoice cannot use this codec when communicating with a third-party VoIP gateway.
- G728 specifies a codec that uses G728 encoding.
- FRGSM specifies the Full Rate GSM audio codec.

Example: `set packet-audio-mode = rt24`

Dependencies: Consider the following:

- The Packet-Audio-Mode setting does not prevent other supported audio codecs from being dynamically selected during call setup.
- The Silence-Det-Change value is ignored when you choose either G711-ULaw or G711-ALaw.
- Changes to the Packet-Audio-Mode setting take effect with the next call.

When either G.723.1 codec is selected:

- Silence-Det-Cng can be enabled or disabled for 6.4Kbps processing only (Packet-Audio-Mode=G723-6.4kps).
- Comfort noise generation can be enabled or disabled for 5.3Kbps processing.
- Comfort noise generation cannot be enabled for 5.3Kbps processing unless the adaptive jitter buffer is disabled.
- Silence detection and suppression cannot be enabled for 6.4Kbps processing unless the adaptive jitter buffer is disabled.
- Adaptive jitter buffer processing can be enabled for 6.4 Kbps processing when silence detection or suppression is disabled, or for 5.3 Kbps processing when comfort noise generation is disabled.
- The actual maximum size of the adaptive jitter buffer is limited to nine frames per packet for G.723.1 rates.

Location: VoIP {x y}

See Also: Allow-Coder-Fallback, Allow-G711-Fallback, Ena-Adap-Jitter-Buffer, Initial-Jitter-Buffer-Size, Max-Jitter-Buffer-Size, Silence-Det-Cng

Packet-Redundancy

Description: Specifies the number of previously sent fax packets that the TAOS unit appends to the current packet. On networks experiencing measurable packet loss, the Packet-Redundancy setting can improve the reliability of the fax transmission.

Usage: Specify one of the following values:

- 0—No change from the default packet behavior.
- 1—Append and send the previous fax packet with the current fax packet.
- 2—Append and send the two previous fax packets with the current fax packet.
- 3—Append and send the three previous fax packets with the current fax packet.
- 4—Append and send the four previous fax packets with the current fax packet.
- 5—Append and send the five previous fax packets with the current fax packet.

Example: `set packet-redundancy = 3`

Dependencies: Packet-Redundancy does not apply when Fixed-Packets is set to Yes. Depending upon the amount of measurable packet loss for a network, set the Packet-Redundancy parameter as follows:

Network condition	Recommended value(s)
Packet loss occurs in frequent bursts.	1 through 5
Occasional packet loss (less than one percent).	0 (the default)
Occasional packet loss (greater than one percent).	1 or 2

The additional bandwidth required for each fax call is proportional to the level of redundancy, amounting to an additional 50 bytes of packet data per increment.

Location: VoIP {x y} > RT-Fax-Options

See Also: Fixed-Packets

Parallel-Dialing

Description: Specifies the number of call-setup requests that the system sends to the network side at any given time.

Usage: Specify an integer from 1 to 64. If the TAOS unit cannot establish an initial connection at the full bandwidth for calls from the United States to another country, reduce the Parallel-Dialing value to 1. The default is 2.

Example: `set parallel-dialing = 12`

Dependencies: Consider the following:

- 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. If the network side is delayed more than 30 to 40 seconds, the modems can time out.
- For a Voice over IP (VoIP) configuration, a setting of 32 is recommended. This setting decreases the chances that a VoIP caller will wait for a silent interval while the unit completes a call that has been queued. Accepting the default value of 2 causes frequent delays in connecting calls.

Location: System

See Also: Dial-Number

Partly-Congested-Metric

Description: Specifies a number from 0 to 255 to use as a transaction server's current metric if it sends a Quick Transaction Protocol (QTP) status message with a Flow Control Attribute set to Partly-Congested.

Usage: Specify a number from 0 to 255. The default is 4.

Example: `set partly-congested-metric = 5`

Location: Transaction-Server

See Also: Available-Metric, Congested-Metric, Shutdown-Metric

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 TAOS unit.
- In a Tunnel-Options subprofile configured for Layer 2 Forwarding (L2F), the Password setting specifies a shared secret for authenticating tunnels.
- 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. 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 string `test !`.

Example: `set password = unit0`

Dependencies: Consider the following:

- You must set Agent-Mode to Home-Agent for the Password setting to apply in a Tunnel-Options subprofile.
- If you specify a Password value for an L2F configuration, the TAOS unit uses it to authenticate L2F tunnels, and ignores the Shared-Secret setting in the Tunnel-Server profile.
- In an SNMPv3-USM-User profile, you must specify a password if the Auth-Protocol setting is a value other than No-Auth.

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: ATMP, Connection *station* > Tunnel-Options, SNMPv3-USM-User *name*, User *name*

See Also: Auth-Protocol, Aux-Send-Password, Recv-Password, Security-Mode, Send-Password, System-Password, Telnet-Password

Password-Enabled

Description: Specifies whether all failed Telnet login attempts generate a trap.

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

- Yes specifies that all failed Telnet login attempts generate a trap.
- No specifies that all 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 *host-name*

See Also: Security-Enabled

Password-For-Direct-Access

Description: Specifies the password that the user must enter when Security-For-Direct-Access is set to Global.

Usage: Specify a password of up to 64 characters. The default is null.

Example: `set password-for-direct-access = mypassword`

Dependencies: Consider the following:

- If Security-For-Direct-Access is not set to Global, the Password-For-Direct-Access setting is ignored.
- If Direct-Access is set to No, Password-For-Direct-Access does not apply.

Location: Terminal-Server > Dialout-Configuration

See Also: Direct-Access, Port-For-Direct-Access, Security-For-Direct-Access

Password-Profile

Description: A subprofile containing settings for Calling-Line ID (CLID) and Dialed Number Information Service (DNIS) passwords set in a RADIUS profile.

Usage: Use the Read and List commands to make Password-Profile the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To list the contents of Password-Profile:

```
admin> list
[ in EXTERNAL-AUTH:password-profile ]
clid = Ascend-CLID
dnis = Ascend-DNIS
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
EXTERNAL-AUTH written
```

See Also: CLID, DNIS

Password-Prompt

Description: Specifies the string that the terminal server uses to prompt for the System-Password when authentication is in use and an interactive user initiates a connection.

Usage: Specify up to 15 characters. The default is Password:

Example: `set password-prompt = Your Password:`

Dependencies: If terminal services are disabled, Password-Prompt does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Login-Prompt, Prompt, Prompt-Format, Terminal-Mode-Configuration, Third-Login-Prompt, Third-Prompt-Sequence

Peak-Rate

Description: Specifies the maximum effective bit rate (in kilobits per second) for transmitting traffic to the network.

Usage: Specify an integer. For DS3-ATM interfaces, the maximum effective rate is 36.864Mbps for C-bit-PLCP framing and 40.038 Mbps for C-bit-ADM framing. For E3-ATM, the valid range is from 0 to 34368. For OC3-ATM, the valid range is from 0 to 135631. The default is 1000 (1 Mbps).

Example: `set peak-rate = 1500`

Dependencies: For Constant Bit Rate (CBR) traffic, the Peak-Rate value specifies the static bit rate. For VBR traffic, the Peak-Rate value specifies the upper boundary of the variable bit rate.

Location: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*

See Also: Aggregate, Bit-Rate, Enabled, Max-Burst-Size, Priority

Peer-Mode

Description: Specifies whether the remote IPX caller is an IPX router or a dial-in client.

Usage: Specify one of the following values:

- Router-Peer (the default) specifies that the caller is an IPX router.
- Dialin-Peer specifies a dial-in client.

Example: `set peer mode = dialin-peer`

Dependencies: Consider the following:

- If you specify Dialin-Peer, the TAOS unit negotiates a routing session with the client by assigning the client a node address on the virtual IPX network defined by IPX-Dialin-Pool. The client must accept the network number that the unit assigns. If the client has its own node number, the TAOS unit uses that number to form the full network address. If the client does not have a node number, the unit assigns it a unique node address on the virtual network.
- For dial-in clients, the TAOS unit does not send Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) advertisements across the connection, and it ignores RIP and SAP advertisements received from the remote end. However, it does respond to RIP and SAP queries it receives from dial-in clients.
- If the TAOS unit does not route IPX for the connection, or if IPX routing is globally disabled, Peer-Mode does not apply.

Location: Answer-Defaults > IPX-Answer, Connection *station* > IPX-Options

See Also: Atalk-Peer-Mode, Dial-Query, IPX-Dialin-Pool, IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Alias, Net-Number, Peer-Mode, RIP, SAP, SAP-Filter

Perm-Conn-Upd-Mode

Description: Specifies under what circumstances the TAOS unit performs nonintrusive remote updates on the configurations of permanent connections.

Usage: Specify one of the following values:

- All (the default) specifies that, if they are fetched from the Remote Authentication Dial-In User Service (RADIUS) server, all existing permanent connections will be torn down and reestablished following the update. This setting causes service interruption every time any nailed profile is updated or added.
- Changed specifies that only changed permanent connections will be torn down and reestablished.

Example: `set perm-conn-upd-mode = changed`

Location: System

See Also: Analog-Encoding, Call-Routing-Sort-Method, Idle-Logout, Name, Parallel-Dialing, SessionID-Base, Single-File-Incoming, System-Rmt-Mgmt, Use-Trunk-Groups

Permit-List

Description: A subprofile that enables you to specify up to 20 devices with Telnet access to the TAOS unit.

Usage: With TACL as the working profile, list a Permit-List subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Permit-List subprofile:

```
admin> list permit-list 1
[in TACL:permit-list[1]]
valid-entry = no
source-address = 0.0.0.0/0
source-address-mask = 0.0.0.0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: TACL

See Also: Source-Address, Source-Address-Mask, Valid-Entry

Phone-Number

Description: Specifies a telephone number.

- In a Call-Route profile, the Phone-Number setting specifies that any calls received on this number must be routed to the index address.
- In a Frame-Relay profile, the Phone-Number setting specifies the number that the TAOS unit dials to reach the switch.
- In a T1 or E1 profile, the Phone-Number setting assigns a channel an add-on number for outgoing calls.

Usage: Specify a telephone number of up to 24 characters. Limit your specification to the following:

1234567890 () [] ! z - * |

The default is null.

In a T1 or E1 profile, you build multichannel calls by specifying add-on numbers. A multichannel call begins as a single-channel connection to one telephone number. The calling unit then requests additional telephone numbers it can dial to connect those channels, and stores the add-on numbers it receives from the answering unit. The calling unit must integrate the add-on numbers with the telephone number it dialed initially to add channels to the call.

Typically, the telephone numbers assigned to the channels share a group of leading (leftmost) digits. Enter only the rightmost digits identifying each telephone number, excluding the digit(s) that are in common. If the add-on number in the called unit is shorter than the telephone number dialed by the calling unit, only the rightmost digits are replaced. If the add-on number is longer than the telephone number dialed, the extra digits are discarded.

The most common reason multichannel calls fail to connect beyond the initial connection is that the answering unit sends the calling unit add-on numbers it cannot use to dial the other channels.

Example: `set phone-number = 1212`

Dependencies: If a nailed-up Frame-Relay datalink connection is in use, Phone-Number does not apply.

Location: Call-Route {{{shelf-*N* slot-*N* *N*} *N*} *N*},
E1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*, Frame-Relay *fr-name*,
T1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*

See Also: Call-Route-Type, Channel-Config *N*, Index, Line-Interface, Preferred-Source, Trunk-Group

PHS-Support

Description: Indicates whether support for the Personal Handyphone System (PHS) is enabled.

Usage: The PHS-Support setting is read only. Yes indicates that PHS support is enabled. No indicates that PHS support is disabled.

Example: `phs-support = yes`

Location: Base

See Also: Countries-Enabled, MAXLink-Client-Enabled, Multi-Rate-Enabled, R2-Signaling-Enabled, Selectools-Enabled

Physical-Address

Description: Identifies a physical address.

Usage: The physical address has the format {*shelf slot item*}, where:

Syntax element	Description
----------------	-------------

<i>shelf</i>	Specifies the shelf in which the item resides. The shelf number is always 1.
<i>slot</i>	Specifies the number of the item's expansion slot.
<i>item</i>	Specifies an item, such as a digital modem or T1 line, on the slot card.

In most cases, the value of Physical-Address is obtained from the system. However, you can clone a profile by reading an existing one and changing its physical address. Use the List and Set commands to modify the Physical-Address value.

Example: admin> **list physical-address**
 [in T1/{ shelf-1 slot-1 1 }:physical-address]
 shelf = shelf-1
 slot = slot-9
 item-number = 37
 admin> **set slot = slot-8**

As an alternative, you can just use the Set command. For example:

admin> **set physical-address slot = slot-8**

Location: DS3-ATM {shelf-*N* slot-*N* *N*}
 E1 {shelf-*N* slot-*N* *N*},
 E3-ATM {shelf-*N* slot-*N* *N*},
 LAN-Modem {shelf-*N* slot-*N* *N*},
 OC3-ATM {shelf-*N* slot-*N* *N*},
 Serial {shelf-*N* slot-*N* *N*},
 STM {shelf-*N* slot-*N* *N*},
 SWAN {shelf-*N* slot-*N* *N*},
 SWAN-Stat {shelf-*N* slot-*N* *N*},
 T1 {shelf-*N* slot-*N* *N*},
 T1-Stat {shelf-*N* slot-*N* *N*},
 T3 {shelf-*N* slot-*N* *N*},
 T3-Stat {shelf-*N* slot-*N* *N*}

See Also: Device-Address, Interface-Address, Item-Number, Shelf, Slot

Ping

Description: Enables and disables the terminal-server Ping command.

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

- Yes enables terminal-server users to use the Ping command.
- No disables the Ping command in the terminal-server interface.

Example: **set ping = yes**

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: PPP, Rlogin, SLIP, TCP, Telnet, Terminal-Mode-Configuration, Traceroute

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. The default is 0 (zero), which 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 of 10 seconds.

Example: `set poll-interval = 120`

Location: Connection *station* > IP-Options > OSPF-Options,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF

See Also: Network-Type

Poll-Rate

Description: Specifies the number of milliseconds between polls.

Usage: Specify a number from 500 to 5000. The default 5000.

Example: `set poll-rate = 2000`

Location: Connection *station* > HDLC-NRM-Options

See Also: Poll-Retry-Counter, Poll-Timeout

Poll-Retry-Counter

Description: Specifies the number of times that the TAOS unit retries the poll after a response timeout.

Usage: Specify a number from 0 to 255. The default is 2.

Example: `set poll-retry-counter = 5`

Location: Connection *station* > HDLC-NRM-Options

See Also: Poll-Rate, Poll-Timeout

Poll-Timeout

Description: Specifies the number of milliseconds that the TAOS unit waits for a response from the caller (the secondary station) to a poll sent by the TAOS unit (the primary station).

Usage: Specify a number from 0 to 255000. The default is 60000.

Example: `set poll-timeout = 50000`

Location: Connection *station* > HDLC-NRM-Options

See Also: Poll-Rate, Poll-Retry-Counter

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.

Note: 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 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, VRouters 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 *name*

See Also: Assign-Address, Assign-Count, Must-Accept-Address-Assign, Pool-Name, Pool-Summary, VRouter-IP-Address

Pool-Chaining

Description: Enables or disables IP pool chaining.

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

- Yes enables IP 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 disables IP pool chaining.

Example: `set pool-chaining = yes`

Dependencies: Consider the following:

- Address pools must be defined either locally or in Remote Authentication Dial-In User Service (RADIUS) pseudo-user profiles.
- Address assignment must be enabled in the Answer-Defaults profile.

Location: IP-Global

See Also: Address-Pool, Assign-Address, Assign-Count, Pool-Base-Address

Pool-For-Async-Framed-User

Description: Specifies an IP address pool for incoming asynchronous framed users without authentication.

Usage: Specify an IP pool number from 0 to 512. The default is 0 (zero), which allows the unit to assign an address from any pool.

Example: `set pool-for-async-framed-user = 5`

Dependencies: Consider the following:

- If the Auth-For-Async-Framed-User parameter is set to Not-Required, you must assign a pool number to provide IP addresses for incoming asynchronous framed users who are not authenticated.
- Because the pool you specify is for the sole use of asynchronous framed users who are not authenticated, the unit cannot allocate an IP address from the same pool to incoming users who *are* authenticated.
- A read-only copy of the Pool-For-Async-Framed-User setting appears in the PPP-Options subprofile.

Location: Answer-Defaults > IP-Answer, Connection > IP-Options

See Also: Auth-For-Async-Framed-User, Max-PAP-Auth-Retry

Pool-Name

Description: Assigns a name to an IP address pool for Terminal Access Controller Access Control Plus (TACACS+) authentication or Virtual Router (VRouter) operation. 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).

Usage: Specify a name of up to 11 characters. The default is null.

Example: `set pool-name 1 = newyork`

Dependencies: Consider the following:

- If TACACS+ authentication is not in use, the TAOS unit treats a pool name specification as a comment.
- In a VRouter profile, the address pool is exclusive to one VRouter. If you do not specify an address pool in a VRouter profile, VRouters can share the address pools defined in the IP-Global profile.

Location: IP-Global, VRouter

See Also: Assign-Address, Assign-Count, Must-Accept-Address-Assign, Pool-Base-Address, Pool-Summary, VRouter-IP-Address

Pool-Number

Description: Specifies the number of the address pool from which the client's address is obtained.

Usage: Specify an integer. The default is 1.

Example: `set pool-number = 5`

Dependencies: The Pool-Number setting has no effect if the system finds a match for the client's hardware address in the static assignment list.

Location: Connection *station* > DHCP-Options

See Also: Maximum-Leases, Reply-Enabled

Pool-OSPF-Adv-Type

Description: Specifies how to import summarized pool addresses into Open Shortest Path First (OSPF).

Usage: Specify one of the following values:

- Type-1 (the default) instructs the TAOS unit to import the pool addresses into OSPF as external Type-1 routes.
- Type-2 instructs the TAOS unit to import the pool addresses into OSPF as external Type-2 routes.
- Internal instructs the TAOS 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

See Also: Active, Pool-Summary

Pool-Summary

Description: Specifies whether pool summarization is in use.

When Pool-Summary is set to Yes, the TAOS 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 TAOS unit either bounces the packet back to the remote network or silently discards it. When you use pool summarization, you significantly reduce the size of routing table advertisements.

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

- Yes enables pool summarization.
- No disables pool summarization.

Example: `set pool-summary = yes`

Dependencies: 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, VRouters can share the address pools defined in the IP-Global profile.

If you set Pool-Summary to Yes, you must create a network-aligned pool that adheres to the following rules:

- The value of Assign-Count must be 2 less than the total number of addresses in the pool. Add 2 to Assign-Count for the total number of addresses in the subnet, and calculate the subnet mask for the subnet on the basis of the total.
- Pool-Base-Address must be the first host address. Subtract 1 from the Pool-Base-Address to obtain the base address for the subnet.

For example, the following configuration creates a network-aligned address pool and enables pool summarization:

```
admin> set pool-base-address = 10.12.253.1
admin> set assign-count = 62
admin> set pool-summary = yes
```

Note the following:

- When you subtract 1 from the value of Pool-Base-Address in this example, you get 10.12.253.0, which is a valid base address for the 255.255.255.192 subnet mask. (Note that 10.12.253.64, 10.12.253.128, and 10.12.253.192 are also valid zero addresses for the same subnet mask.) The resulting address pool network is 10.12.253.0/26.
- When you add 2 to Assign-Count, you get 64. The subnet mask for 64 addresses is 255.255.255.192 (256–64=192). The TAOS notation for a 255.255.255.192 subnet mask is /26.

Location: IP-Global, VRouter

See Also: Assign-Count, Pool-Base-Address, Pool-Name, VRouter-IP-Address

Port

Description: Specifies the port number, as follows:

- In the Auxiliary-Syslog [1] subprofile, the Port value specifies the destination port of the Syslog host that receives the second data stream. In the Auxiliary-Syslog [2] subprofile, the Port value specifies the destination port of the Syslog host that receives the third data stream.
- In a Connection profile, the Port setting specifies a port on the login host to which TCP-Clear sessions 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 TAOS unit returns a TCP connection error to the dial-in client.

- In the Terminal-Server profile, the Port setting specifies the port on the login host to which the user connects in immediate mode.
- In a Log profile, the Port setting specifies the destination port of the Syslog host that receives the first data stream.
- In a Hosts-Info *N* subprofile, indicates the port associated with the host displayed in the terminal-server menu.

Usage: Specify a port number. For a Connection or Terminal-Server profile, the default is 0 (zero). For the Log profile and Auxiliary-Syslog subprofiles, the default is 514.

Example: The following example specifies two login host-port combinations:

```
admin> read connection fred
CONNECTION/fred read

admin> set tcp-clear-options host 1 = mercury
admin> set tcp-clear-options host 2 = venus
admin> set tcp-clear-options port 1 = 155
admin> set tcp-clear-options port 2 = 256
admin> write
CONNECTION/fred written
```

Dependencies: In the Log profile, Port does not apply if Syslog is disabled. The settings in the Auxiliary-Syslog subprofile affect an individual Syslog stream, and override the values specified in the Log profile.

Location: Connection *station* > TCP-Clear-Options, Ext-Tsrv > Hosts-Info *N*, Log, Log > Auxiliary-Syslog, Terminal-Server > Immediate-Mode-Options

See Also: Facility, Host, Host2, Host3, Host4, Immediate-Mode-Options, Port2, Port3, Port4, Save-Level, Save-Number, Service, Syslog-Enabled, TCP-Clear-Options

Port2

Description: Specifies a port on the second login host to which a TCP-Clear session attempts to connect.

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
```

Dependencies: 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 TAOS unit returns a TCP connection error to the dial-in client.

Location: Connection *station* > TCP-Clear-Options

See Also: Facility, Host, Host2, Host3, Host4, Immediate-Mode-Options, Port, Port3, Port4, Save-Level, Save-Number, Service, Syslog-Enabled, TCP-Clear-Options

Port3

Description: Specifies a port on the third login host to which a TCP-Clear session attempts to connect.

Usage: Specify a port number. The default is 0 (zero).

Example: The following example specifies three 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 host3 = neptune
admin> set tcp-clear-options port = 155
admin> set tcp-clear-options port2 = 256
admin> set tcp-clear-options port3 = 170
admin> write
CONNECTION/fred written
```

Dependencies: 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 TAOS unit returns a TCP connection error to the dial-in client.

Location: Connection *station* > TCP-Clear-Options

See Also: Facility, Host, Host2, Host3, Host4, Immediate-Mode-Options, Port, Port2, Port4, Save-Level, Save-Number, Service, Syslog-Enabled, TCP-Clear-Options

Port4

Description: Specifies a port on the fourth login host to which a TCP-Clear session attempts to connect.

Usage: Specify a port number. The default is 0 (zero).

Example: The following example specifies four 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 host3 = neptune
admin> set tcp-clear-options host4 = pluto
admin> set tcp-clear-options port = 155
admin> set tcp-clear-options port2 = 256
admin> set tcp-clear-options port3 = 170
admin> set tcp-clear-options port4 = 180
admin> write
CONNECTION/fred written
```

Dependencies: 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 TAOS unit returns a TCP connection error to the dial-in client.

Location: Connection *station* > TCP-Clear-Options

See Also: Facility, Host, Host2, Host3, Host4, Immediate-Mode-Options, Port, Port2, Port3, Save-Level, Save-Number, Service, Syslog-Enabled, TCP-Clear-Options

Port-N

Description: Specifies the port to use for contacting the Telnet host specified by Host-N.

Usage: Specify a number from 0 to 65535. The default is 0 (zero).

Example: `set port-1 = 50`

Dependencies: Port-N applies only when Service-N is set to Telnet.

Location: Terminal-Server > Menu-Mode-Options

See Also: Host-N

Port-Enabled

Description: Specifies whether the TAOS unit sends trap Protocol Data Units (PDUs) to the Simple Network Management Protocol (SNMP) manager.

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

- Yes specifies that the TAOS unit sends trap-PDUs to the host specified by Host-Address.
- No specifies that the TAOS unit does not send trap-PDUs.

Example: `set port-enabled = yes`

Location: Trap *host-name*

See Also: Alarm-Enabled, Community-Name, Host-Address, Host-Name, Security-Mode

Port-For-Direct-Access

Description: Specifies a Telnet port number to use for direct-access dial-out service.

To dial out, a local operator uses Telnet to connect to the specified port. When the connection to the modem is established, the user can issue AT commands to the modem as if connected locally to its asynchronous port.

Usage: Specify a port number from 5000 to 32767. The default is 5000.

Example: `set port-for-direct-access = 5001`

Dependencies: If terminal services are disabled or Direct-Access is set to No, Port-For-Direct-Access does not apply.

Location: Terminal-Server > Dialout-Configuration

See Also: Dialout-Allowed, Dialout-Configuration, Direct-Access, Password-For-Direct-Access, Port-For-Direct-Access, Security-For-Direct-Access, Telnet

Port-Number

Description: Specifies the port number to be compared with the destination port of a packet.

Usage: Specify a port number. The default is 0 (zero). TCP and UDP port numbers are typically assigned to services. For a list of assigned port numbers, see RFC 1700, *Assigned Numbers*.

Example: `set port-number = 80`

Location: Connection *station* > Port-Redirect-Options

See Also: Protocol, Redirect-Address

Port-Redirect-Options

Description: A subprofile that enables you to redirect certain packet types to a specified server.

Usage: With a Connection profile as the working profile, list the Port-Redirect-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Port-Redirect-Options subprofile:

```
admin> list
[ in CONNECTION/robin:port-redirect-options ]
protocol = none
port-number = 0
redirect-address = 0.0.0.0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: Port-Number, Protocol, Redirect-Address

Power-Supply-Enabled

Description: Specifies whether the system generates a trap when a power supply module is added or removed.

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

- Yes specifies that the system generates a trap when a power supply module is added or removed.
- 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 *host-name*

See Also: Trap

PPP

Description: Enables or disables the use of the PPP command in the terminal-server interface.

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

- Yes enables the use of the PPP command in the terminal-server interface.
- No disables the use of the PPP command in the terminal-server interface.

Example: `set ppp = yes`

Dependencies: If terminal services are disabled, PPP does not apply.

Location: Terminal-Server > PPP-Mode-Configuration

See Also: Ping, PPP-Mode-Configuration, Rlogin, SLIP, TCP, Telnet, Terminal-Mode-Configuration, Traceroute

PPP-Answer

Description: A subprofile containing default settings for Point-to-Point Protocol (PPP) calls. The TAOS unit also uses the PPP-Answer settings for the PPP variants, Multilink Protocol (MP) and Multilink Protocol Plus (MP+).

Usage: With Answer-Defaults as the working profile, list the PPP-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the PPP-Answer subprofile:

```
admin> list ppp-answer
[ in ANSWER-DEFAULTS:ppp-answer ]
enabled = yes
receive-auth-mode = no-ppp-auth
disconnect-on-auth-timeout = yes
link-compression = none
mru = 1524
lqm = no
lqm-minimum-period = 600
lqm-maximum-period = 600
bi-directional-auth = none
substitute-recv-name = " "
substitute-send-name = " "
mtu = 1524
auth-for-async-framed-user = required
max-pap-auth-retry = 5
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Auth-For-Async-Framed-User, Bi-Directional-Auth, Disconnect-On-Auth-Timeout, Enabled, Link-Compression, LQM, LQM-Maximum-Period, LQM-Minimum-Period, Max-PAP-Auth-Retry, MRU, MTU, Receive-Auth-Mode, Substitute-Recv-Name, Substitute-Send-Name

PPP-Mode-Configuration

Description: A subprofile containing terminal-server options for Point-to-Point Protocol (PPP) sessions.

Usage: With Terminal-Server as the working profile, list the PPP-Mode-Configuration subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the PPP-Mode-Configuration subprofile:

```
admin> list ppp-mode-configuration
[ in TERMINAL-SERVER:ppp-mode-configuration]
ppp = yes
delay = 5
direct = no
info = session-ppp
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server

See Also: Delay, Direct, Info, PPP

PPP-Options

Description: A subprofile that contains settings for Point-to-Point Protocol (PPP) calls. The TAOS unit also uses the PPP-Options settings for the PPP variants, Multilink Protocol (MP) and Multilink Protocol Plus (MP+).

Usage: With a Connection profile as the working profile, list the PPP-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the PPP-Options subprofile:

```
admin> list ppp-options
[ in CONNECTION/tim:ppp-options]
send-password = ""
recv-password = ""
enabled = yes
link-compression = stac
mru = 1524
lqm = no
disconnect-on-auth-timeout = yes
lqm-minimum-period = 600
lqm-maximum-period = 600
split-code-dot-user-enabled = no
cbcp-enabled = no
mode-callback-control = cbcp-no-callback
trunk-group-callback-control = 9
```

```
mtu = 1524
substitute-send-name = " "
auth-for-async-framed-user = required
max-pap-auth-retry = 5
pool-for-async-framed-user = 0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: PPP calls must be enabled in the Answer-Defaults profile.

Location: Connection *station*

See Also: Auth-For-Async-Framed-User, CBCP-Enabled, Disconnect-On-Auth-Timeout, Enabled, Link-Compression, LQM, LQM-Maximum-Period, LQM-Minimum-Period, Max-PAP-Auth-Retry, Mode-Callback-Control, MRU, MTU, Pool-For-Async-Framed-User, Recv-Password, Send-Password, Split-Code-Dot-User-Enabled, Substitute-Send-Name, Trunk-Group-Callback-Control

PPTP-Enabled

Description: Enables or disables Point-to-Point Tunneling Protocol (PPTP) tunneling.

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

- Yes enables PPTP tunneling.
- No disables PPTP tunneling.

Example: `set pptp-enabled = yes`

Location: L2-Tunnel-Global

See Also: Server-Profile-Required

Precedence

Description: Specifies the priority level of the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits used to set precedence for priority queuing. When TOS is enabled, you can set those bits to one of the following values (most significant bit first):

- 000 specifies normal priority (the default).
- 001 specifies priority level 1.
- 010 specifies priority level 2.
- 011 specifies priority level 3.
- 100 specifies priority level 4.
- 101 specifies priority level 5.
- 110 specifies priority level 6.
- 111 specifies priority level 7 (the highest priority).

Example: `set precedence = 001`

Dependencies: For the Precedence setting to apply, you must set Active to Yes in the TOS-Options subprofile, or Type to TOS-Filter in the Input-Filters or Output-Filters subprofile.

Location: Connection *station* > IP-Options > TOS-Options,
Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter,
VoIP {*x y*} > TOS-Options

Location: Active, Apply-To, Type-of-Service

Preference

Description: Specifies the preference for the route.

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, 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 Routing Information Protocol (RIP)
- 100—Static routes
- 100—Ascend Tunnel Management Protocol (ATMP) routes

Example: `set preference = 100`

Location: Connection *station* > IP-Options, IP-Route *name*

See Also: Down-Preference, IP-Options, OSPF-ASE-Pref, OSPF-Pref, RIP-Pref, Static-Pref

Preferred-Source

Description: Specifies the address of a network port used as a T1 or E1 channel. The Preferred-Source setting indicates that any calls received on this channel must be routed to the index address.

Usage: Specify the address of a T1 or E1 channel. The default is null.

Example: `set preferred-source = {{1 7 7} 0}`

Location: Call-Route {{{shelf-*N* slot-*N N*} *N*} *N*}

See Also: Call-Route-Type, Index, Phone-Number, Trunk-Group

Primary

Description: Specifies whether the dial-in unit is a primary station.

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

- Yes specifies that the dial-in unit is a primary station. The TAOS unit acts as a secondary station for this connection (usually for test purposes).
- No specifies that the dial-in unit is a secondary station. The TAOS unit acts as a primary station for this connection.

Example: `set primary = yes`

Location: Connection *station* > HDLC-NRM-Options

See Also: Async-Drop

Primary-IP-Address

Description: Specifies the primary IP address to use for communicating with the primary signaling gateway.

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

Example: `set primary-ip-address = 10.1.2.3`

Dependencies: Consider the following:

- To enable Signaling System 7 (SS7) operations, you must set Enabled to Yes and then specify valid values for Primary-IP-Address and Primary-TCP-Port.
- If Enabled is set to No in the SS7-Gateway profile, Primary-IP-Address does not apply.

Location: SS7-Gateway

See Also: Primary-TCP-Port, Secondary-IP-Address

Primary-Preference

Description: Specifies the preference level for electing this controller as primary at the next system reset.

Usage: Specify one of the following values:

- No-Preference (the default) leaves the decision to the system. The system chooses the controller that was primary most recently, or selects the controller located in the left controller slot.
- Left-Controller-Preferred gives preference to the controller in the left shelf-controller slot. If the shelf controller in the first slot is not available, the shelf controller in the right slot is made primary controller.
- Right-Controller-Preferred gives preference to the controller in the right shelf-controller slot. If that shelf controller is not available, the shelf controller in the left slot is made primary.

Example: `set primary-preference = left-controller-preferred`

Dependencies: Consider the following:

- Make your settings on the primary controller. Values written on the secondary controller might be overwritten.
- The Primary-Preference setting persists when you reboot the TAOS unit.

Location: Redundancy

Primary-Retries

Description: Specifies the maximum number of attempts the TAOS unit makes when it tries to reregister with the MultiVoice Access Manager (MVAM) at the IP address specified by Gatekeeper-IP.

Usage: Specify a number from 0 to 200. The default is 1. Setting Primary-Retries to 0 (zero) disables the feature.

Example: `set primary-retries = 5`

Dependencies: Any change to the value of Primary-Retries becomes effective in the next registration cycle.

Location: VoIP {x y}

See Also: Gatekeeper-IP, Registration-Retries

Primary-TCP-Port

Description: Specifies the primary TCP port to use for communicating with the primary signaling gateway.

Usage: Specify a port number. The default is 0 (zero).

Example: `set primary-tcp-port = 5000`

Dependencies: Consider the following:

- To enable Signaling System 7 (SS7) operations, you must set Enabled to Yes and then specify valid values for Primary-IP-Address and Primary-TCP-Port.
- If Enabled is set to No in the SS7-Gateway profile, Primary-TCP-Port does not apply.

Location: SS7-Gateway

See Also: Primary-IP-Address, Secondary-TCP-Port

Primary-Tunnel-Server

Description: Specifies the IP address or hostname of the Ascend Tunnel Management Protocol (ATMP) primary Home Agent, L2TP Network Server (LNS) endpoint, PPTP Network Server (PNS) endpoint, Layer 2 Forwarding (L2F) Home Gateway endpoint, or intermediate destination that will decapsulated IP packets that use 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 TAOS unit 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:

```
admin> set primary-tunnel-server = 10.11.22.33:8877
```

The following setting specifies a hostname:

```
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.

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: Connection *station* > Tunnel-Options

See Also: Home-Network-Name, Max-Tunnels, Password, Profile-Type, Secondary-Tunnel-Server, Tunneling-Protocol, UDP-Port

Prior-Function

Description: After a switchover, specifies whether the controller is was functional and, if so, whether it was a primary controller or a secondary controller.

Usage: The Prior-Function setting is read only. Its possible values are No-Function, Primary, or Secondary.

Example: prior-function = primary

Location: Redundancy-Stats > Context-Stats > Context-Stats *N*

See Also: Function

Priority

Description: Specifies a priority value.

- In a Connection profile or IP-Interface profile, the Priority value specifies the priority of the Open Shortest Path First (OSPF) router with regard to designated-router (DR) and backup designated-router (BDR) election.
- In a DS3-ATM or OC3-ATM profile, the Priority value specifies the priority of this shaper relative to other shapers on the interface.
- In an E3-ATM profile, the Priority value specifies the Asynchronous Transfer Mode (ATM) service value.

Usage: Specify an integer.

- In a Connection profile or IP-Interface profile, the TAOS unit can function as either a DR or a BDR. However, many sites choose to assign these functions to LAN-based routers in order to dedicate the TAOS unit to WAN processing. The default is 5.
- In a DS3-ATM or OC3-ATM profile, the valid range is from 0 to 15. The default of 0 (zero) indicates the highest priority, and 15 indicates the lowest.
- In an E3-ATM profile, the default value of 0 (zero) specifies Constant Bit Rate (CBR) service. A value of 1 specifies Variable Bit Rate Non-Real Time (VBR-NRT) service. A value of 2 specifies Unspecified Bit Rate (UBR) service.

Example: `set priority = 10`

Dependencies: Choose the DR and BDR election priority on the basis of each device's processing power and reliability. Assigning a priority of 1 or greater places the TAOS unit on the list of possible DRs and BDRs. A priority value of 0 (zero) excludes the unit from becoming a DR or BDR. The higher the priority value of the TAOS unit relative to other OSPF routers on the network, the better the chances that it will become a DR or BDR.

Location: Connection *station* > IP-Options > OSPF-Options,
DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line-Config > Traffic-Shapers > Traffic-Shapers *N*,
IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF

See Also: Aggregate, Bit-Rate, IP-Options, Max-Burst-Size, OSPF, OSPF-Options, Peak-Rate, Priority

PRI-Prefix-Number

Description: Specifies the portion of the line's telephone number to be used for matching the called-party number in the Setup message from the network switch.

When overlap receiving is in use, the number you specify enables the TAOS unit to quickly determine when the called-party number is complete. The unit uses this number and the specified number of trailing digits to recognize that the called-party number is complete, even if the caller did not include a Sending Complete code (for example, by dialing the pound sign).

Usage: Specify a prefix. Typically, the PRI prefix is an ISDN-subscriber number, which can include an area code or an area-and-country code combination. The area code or area-and-country code must be separated from the ISDN-subscriber number by a hyphen. The TAOS unit searches for just the first match of PRI-Prefix-Number against the called-party number in the Setup message (first with an area code, and if that fails, without an area code).

The default null value disables the T302-Timer optimization.

Example: `set pri-prefix-number = 413-555-1234`

Dependencies: You must set Overlap-Receiving to Yes for PRI-Prefix-Number to have any effect.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface, E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Overlap-Receiving, T302-Timer, Trailing-Digits

Private-Route

Description: Specifies whether the TAOS unit advertises route information by means of routing protocols.

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

- Yes makes the route private. The TAOS unit uses the route internally, but does not advertise it.
- No specifies that the TAOS unit advertises the route by means of routing protocols.

Example: `set private-route = yes`

Location: IP-Route *name*, Connection *station* > IP-Options

See Also: IP-Options, IP-Routing-Enabled, OSPF, RIP, RIP-Mode

Private-Route-Profile-Required

Description: In the Answer-Defaults profile, specifies whether the system drops the call if it cannot locate the Private-Route-Table profile indicated in the Remote Authentication Dial-In User Service (RADIUS) user profile. In a Connection profile, specifies whether the system drops the call if it cannot locate the Private-Route-Table profile indicated in the Connection profile.

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

- Yes specifies that the system drops the call if it cannot locate the Private-Route-Table profile.
- No specifies that the system establishes the link even if it cannot locate the Private-Route-Table profile.

Example: `set private-route-profile-required = yes`

Dependencies: The unit uses the Private-Route-Profile-Required value in the Answer-Defaults profile only if the Ascend-Private-Route-Required attribute is not set in a RADIUS private-route profile.

Location: Answer-Defaults > IP-Answer, Connection *station* > IP-Options

See Also: Default-Prt-Cache-Time, Private-Route-Table

Private-Route-Table

Description: Specifies the private routing table for the connection.

Usage: Specify the name of the Private-Route-Table profile associated with the connection. You can enter up to 23 characters. The default is null.

Example: `set private-route-table = private-rt-1`

Location: Connection *station* > IP-Options

See Also: Private-Route-Profile-Required

Private-Route-Table (profile)

Description: A profile that enables you to define a private routing table.

Usage: Use the Read and List commands to make Private-Route-Table the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Private-Route-Table profile `robin` the working profile and list its contents:

```
admin> read private-route-table robin
[PRIVATE-ROUTE-TABLE/robin read

admin> list
[in PRIVATE-ROUTE-TABLE/robin]
name* = robin
route-description-list = [ { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 } {+
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
PRIVATE-ROUTE-TABLE/robin written
```

See Also: Name, Route-Description-List

Priv-Key

Description: Specifies a privacy key for SNMPv3 USM users.

Usage: In most cases, you do not set the 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 10 (16D in hexadecimal) if Message Digest 5 (MD5) is in use and 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 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 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 this value as the following Priv-Key value:

```
'\x0a\xdcu\xf8\x98\xe5|L\x03"}\xdd\xac\x0d\xef
```

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.
- If Priv-Protocol is set to No-Auth, Priv-Key does not apply.

Location: SNMPv3-USM-User *name*

See Also: Priv-Protocol

Priv-Protocol

Description: Enables or disables encryption of messages sent on behalf of the user to or from the SNMP engine, and if enabled, the type of privacy protocol to be used.

Usage: Specify one of the following values:

- No-Priv (the default) specifies that no encryption is required and that privacy is disabled.
- DES-Priv specifies that DES-based privacy is required. Incoming messages that are DES-encrypted are interpreted, and outgoing responses are encrypted using DES. Note that outgoing reports are not encrypted.

Dependencies: The TAOS unit's SNMPv3 engine does not support encryption or decryption.

Location: SNMPv3-USM-User *name*

See Also: Active-Enabled, Auth-Protocol, Name, Password, Priv-Key, Read-Write-Access

Proceed-Progress-Indicator

Description: Specifies the type of call-progress events captured and reported by the MultiVoice gateway in the Q.931 Proceeding message progress-indicator information element (IE).

Usage: Specify one of the following values:

- No-Progress-Indicator (the default) disables alert reporting of call-routing events on the egress switched telephone network.
- None-End2End-ISDN specifies that the egress MultiVoice gateway reports when calls are connected to an egress switched telephone network that does not use ISDN signaling. The egress switched telephone network can support robbed-bit or detectable DTMF.

- **Dest-Non-ISDN** specifies that the egress MultiVoice gateway reports when calls are connected to an egress switched telephone network that does not use ISDN signaling (for example, a transit network or private network) and that does not return call-progress signals to the MultiVoice gateway.
- **Orig-Non-ISDN** specifies that the ingress MultiVoice gateway reports when calls are received from a local switched telephone network that does not use ISDN signaling (for example, a transit network or private network) and that does not provide call-progress signals to the MultiVoice gateway.
- **Return-To-ISDN** specifies that the egress MultiVoice gateway reports when calls connected across a transit network are routed back on to a trunk supporting ISDN signaling.
- **Interworking-Occurred** specifies that the egress MultiVoice gateway reports whether interworking occurs upon connection to the switched telephone network. Such interworking events occur when the selected bearer capability is not supported or when a resource or route with the preferred capability is not available.
- **Inband-Info-Available** specifies that the egress MultiVoice gateway reports whether inband call-progress signaling or other supported non-ISDN signaling is available from the switched telephone network for the connected call.

Example: `set proceed-progress-indicator = dest-non-isdn`

Location: VoIP { *x y* } > PSTN-Attribute

See Also: Alert-Progress-Indicator

Profile-Name

Description: Specifies the name of the Connection profile that the TAOS unit uses to reach the IPX network. When the unit receives a query for the specified server or a packet addressed to that server, it finds the Connection profile and dials the connection.

Usage: Specify a text string representing the name of the Connection profile. You can enter up to 24 characters. The default is null.

Example: `set profile-name = tim`

Location: IPX-Route *name*

See Also: Active-Route, Dest-Network, Host, Name, Server-Node, Server-Socket, Server-Type, Ticks

Profiles-Required

Description: Specifies whether the TAOS unit rejects incoming calls for which it cannot 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 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: Specify Yes or No. The default is Yes.

- Yes specifies that the TAOS unit requires a configured profile for all callers. The unit rejects calls for which it cannot find a configured profile.
- No specifies that if the TAOS 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

See Also: Local-Profiles-First, Receive-Auth-Mode

Profile-Type

Description: Specifies the type of Ascend Tunnel Management Protocol (ATMP), Layer 2 Tunneling Protocol (L2TP), or Layer 2 Forwarding (L2F) connection.

Usage: Specify one of the following values:

- Disabled (the default) specifies that the connection is not used for tunneling.
- Mobile-Client specifies that the Connection profile is used to authenticate a Mobile Client, or that L2F tunneling is in use.
- Gateway-Profile specifies that the Connection profile sets up a gateway connection to a home network.

Example: `set profile-type = gateway-profile`

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: Connection *station* > Tunnel-Options

See Also: Home-Network-Name, Max-Tunnels, Password, Primary-Tunnel-Server, Secondary-Tunnel-Server, UDP-Port

Prompt

Description: Specifies a string that the TAOS unit uses as a command-line prompt.

Usage: Specify a string to be used as a prompt. You can specify up to 15 characters.

Example: `set prompt = virginia>`

Location: Terminal-Server > Terminal-Mode-Configuration, User *name*

See Also: Login-Prompt, Password-Prompt, Prompt-Format, Terminal-Mode-Configuration, Third-Login-Prompt, Third-Prompt-Sequence

Prompt-Format

Description: Specifies whether the TAOS unit interprets carriage-return/linefeed and tab characters in the string specified by Login-Prompt.

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

- Yes causes the TAOS unit to interpret carriage-return/linefeed and tab characters in the string specified by Login-Prompt.
- No causes the TAOS unit to ignore carriage-return/linefeed or tab characters in the string specified by Login-Prompt.

Example: `set prompt-format = no`

Dependencies: If terminal services are disabled, Prompt-Format does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Login-Prompt, Password-Prompt, Prompt, Terminal-Mode-Configuration, Third-Login-Prompt, Third-Prompt-Sequence

Protocol

Description: Specifies a protocol type. The default is 0 (zero).

- The TAOS unit compares the number you specify in a Filter profile to the protocol number field in a packet.
- When you specify a Protocol setting in the Port-Redirect-Options subprofile of the Connection profile, the value indicates the type of redirected packet.

Usage: In a Port-Redirect-Options subprofile, specify one of the following settings:

- None (the default) disables port redirection.
- UDP specifies User Datagram Protocol.
- TCP specifies Transmission Control Protocol.

In a Filter profile, specify one of the following settings:

- 0—Disregard protocol type.
- 1—ICMP (Internet Control Message Protocol)
- 2—IGMP (Internet Group Management Protocol)
- 3—GGP (Gateway-to-Gateway Protocol)
- 4—IP (Internet Protocol)
- 5—ST (Stream)

- 6—TCP (Transmission Control Protocol)
- 7—UCL
- 8—EGP (Exterior Gateway Protocol)
- 9—Any private interior gateway protocol
- 10—BBN-RCC-MON (BBN RCC Monitoring)
- 11—NVP-II (Network Voice Protocol II)
- 12—PUP
- 13—ARGUS
- 14—EMCOM
- 15—XNET (Cross-Net Debugger)
- 16—CHAOS
- 17—UDP (User Datagram Protocol)
- 18—MUX (Multiplexing)
- 19—DCN-MEAS (DCN Measurement Subsystems)
- 20—HMP (Host Monitoring Protocol)
- 21—PRM (Packet Radio Measurement)
- 22—XNS IDP (Xerox Networking System Internetwork Datagram Protocol)
- 23—TRUNK-1
- 24—TRUNK-2
- 25—LEAF-1
- 26—LEAF-2
- 27—RDP (Reliable Data Protocol)
- 28—IRTP (Internet Reliable Transport Protocol)
- 29—ISO-TP4 (International Standards Organization Transport Protocol Class 4)
- 30—NETBLT (Bulk Data Transfer Protocol)
- 31—MFE-NSP (MFE Network Services Protocol)
- 32—MERIT-INP (MERIT Internodal Protocol)
- 33—SEP (Sequential Exchange Protocol)
- 34—3PC (Third Party Connect Protocol)
- 35—IDPR (Inter-Domain Policy Routing Protocol)
- 36—XTP
- 37—DDP (Datagram Delivery Protocol)
- 38—IDPR-CMTP (IDPR Control Message Transport Protocol)
- 39—TP++ (TP++ Transport Protocol)
- 40—IL (IL Transport Protocol)
- 41—SIP (Simple Internet Protocol)
- 42—SDRP (Source Demand Routing Protocol)
- 43—SIP-SR (SIP Source Route)
- 44—SIP-FRAG (SIP Fragment)
- 45—IDRP (Inter-Domain Routing Protocol)
- 46—RSVP (Reservation Protocol)
- 47—GRE (General Routing Encapsulation)
- 48—MHRP (Mobile Host Routing Protocol)
- 49—BNA
- 50—SIPP-ESP (SIPP Encapsulation Security Payload)
- 51—SIPP-AH (SIPP Authentication Header)
- 52—I-NLSP (Integrated Net Layer Security Protocol)
- 53—SWIPE (IP with Encryption)
- 54—NHRP (Next Hop Resolution Protocol)
- 55-60—Unassigned
- 61—Any Host Internet Protocol
- 62—CFTP

63—Any local network
64—SAT-EXPAK (SATNET and Backroom EXPAK)
65—KRYPTOLAN
66—RVD (MIT Remote Virtual Disk Protocol)
67—IPPC (Internet Pluribus Packet Core)
68—Any distributed file system
69—SAT-MON (SATNET Monitoring)
70—VISA (VISA Protocol)
71—IPCU (Internet Packet Core Utility)
72—CPNX (Computer Protocol Network Executive)
73—CPHB (Computer Protocol Heart Beat)
74—WSN (Wang Span Network)
75—PVP (Packet Video Protocol)
76—BR-SAT-MON (Backroom SATNET Monitoring)
77—SUN-ND PROTOCOL-Temporary
78—WB-MON (WIDEBAND Monitoring)
79—WB-EXPAK (WIDEBAND EXPAK)
80—ISO-IP (International Standards Organization Internet Protocol)
81—VMTP
82—SECURE-VMTP
83—VINES
84—TTP
85—NSFNET-IGP (National Science Foundation Network Interior Gateway Protocol)
86—DGP (Dissimilar Gateway Protocol)
87—TCF
88—IGRP
89—OSPF (Open Shortest Path First)
90—Sprite-RPC
91—LARP (Locus Address Resolution Protocol)
92—MTP (Multicast Transport Protocol)
94—IPIP (IP-within-IP)
95—MICP (Mobile Internetworking Control Protocol)
96—SCC-IP (Semaphore Communications Security Protocol)
97—ETHERIP (Ethernet-within-IP)
98—ENCAP (Encapsulation Header)
99—Any private encryption scheme
100—GMTP
101-254—Unassigned
255—Reserved

Example: `set protocol = 94`

Dependencies: In a Port-Redirect-Options subprofile, the Protocol setting, together with the Port-Number setting, defines a type of packet. For example, TCP with a Port-Number of 21 represents FTP traffic, and TCP with a Port-Number of 23 represents Telnet traffic.

Location: Connection *station* > Port-Redirect-Options,
Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter,
Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter

See Also: Input-Filters, IP-Filter, Output-Filters, Port-Number, Redirect-Address, Type

Proxy-Mode

Description: Specifies under what conditions the TAOS unit responds to Address Resolution Protocol (ARP) requests with its own Media Access Control (MAC) address.

Usage: Specify one of the following values:

- Off (the default) specifies that the TAOS unit does not use its own MAC address as a proxy for any addresses.
- Active specifies that the TAOS unit responds to an ARP request with its own MAC address if the request matches an active Connection profile over which the unit routes IP.
- Inactive specifies that the TAOS unit 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 TAOS unit 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`

Dependencies: You need to use proxy ARP only if both the following conditions are true:

- The supplied IP addresses are within the local subnet of the TAOS unit.
- The hosts on the local subnet need to send packets to the dial-in hosts.

Location: IP-Interface

See Also: Atalk-Peer-Mode, RARP-Enabled

PSTN-Attribute

Description: A subprofile that specifies PSTN settings for a VoIP call.

Usage: With a VoIP profile as the working profile, list the PSTN-Attribute subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the PSTN-Attribute subprofile:

```
admin> list pstn-attribute
[in VOIP/{ 0 0 }:pstn-attribute]
cause-code-transparency = no
alert-progress-indicator = no-progress-indicator
proceed-progress-indicator = no-progress-indicator
bearer-capability = speech
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: VoIP { x y }

See Also: Alert-Progress-Indicator, Bearer-Capability, Cause-Code-Transparency, Proceed-Progress-Indicator

Q

Q93B-Options

Description: A subprofile that enables you to configure Q.93B layer settings.

Usage: With an ATM-Interface profile as the working profile, enter `list svc-options q93b-options` to display the Q93B-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Q93B-Options subprofile:

```
admin> list svc-options q93b-options
[ in ATM-INTERFACE/{ {any-shelf any-slot 0}
0}:svc-options:q93b-options]
max-restart = 2
max-statenq = 1
t303-ms = 4000
t308-ms = 30000
t309-ms = 0
t310-ms = 10000
t313-ms = 4000
t316-ms = 120000
t322-ms = 4000
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: ATM-Interface { {shelf-N slot-N N} N } > SVC-Options

See Also: Max-Restart, Max-Statennq, T303-ms, T308-ms, T309-ms, T310-ms, T313-ms, T316-ms, T322-ms

QSAAL-Options

Description: A subprofile that enables you to configure Q.SAAL layer settings.

Usage: With an ATM-Interface profile as the working profile, enter `list svc-options qsaal-options` to display the QSAAL-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the QSAAL-Options subprofile:

```
admin> list svc-options qsaal-options
[ in ATM-INTERFACE/{ {any-shelf any-slot
0}0}:svc-options:qsaal-options]
window-size = 64
max-cc = 4
max-pd = 25
max-stat = 67
tcc-ms = 1000
tpoll-ms = 0
tkeepalive-ms = 0
tnoresponse-ms = 0
tidle-ms = 15000
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options

See Also: Max-Cc, Max-Pd, Max-Stat, Tcc-ms, Tidle-ms, Tkeepalive-ms, Tnoresponse-ms, Tpoll-ms, Window-Size

QTP-Port

Description: Specifies the UDP port on which Quick Transaction Protocol (QTP) listens for incoming QTP connections.

Usage: Specify a port number from 1 to 65535. The default is 3350.

Example: `set qtp-port = 20`

Location: Transaction-Server

See Also: Max-QTP-PDU-Size

Queue-Depth

Description: Specifies the maximum size of the queue for Simple Network Management Protocol (SNMP) requests.

Usage: Specify the maximum number of requests from 0 to 1024. The default is 0 (zero), which prevents the TAOS unit from dropping packets, no matter how far behind the SNMP subsystem gets. If a queue grows too large in a heavily loaded routing environment, the system can ultimately run out of memory.

Example: `set queue-depth = 32`

Location: SNMP

See Also: RIP-Queue-Depth

R

R1-ANIR-Delay

Description: Specifies the time in milliseconds that the unit waits before sending the Automatic Number ID Request (ANIR) signal after receipt of the ST pulse from the switch.

Usage: Specify a number from 300 to 2000. The default is 350.

Example: `set r1-anir-delay = 5000`

Dependencies: You must set Signaling-Mode to R1-Inband for R1-ANIR-Delay to have any effect.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: R1-ANIR-Timer, R1-First-Digit-Timer, R1-Modified, R1-Use-ANIR, Signaling-Mode

R1-ANIR-Timer

Description: Specifies the duration in milliseconds of the Automatic Number ID Request (ANIR) signal.

Usage: Specify a number from 180 to 400. The default is 200.

Example: `set r1-anir-timer = 300`

Dependencies: You must set Signaling-Mode to R1-Inband for R1-ANIR-Timer to have any effect.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: R1-ANIR-Delay, R1-First-Digit-Timer, R1-Modified, R1-Use-ANIR, Signaling-Mode

R1-First-Digit-Timer

Description: Specifies the time in milliseconds that the unit waits for the first digit from the switch after sending the KP pulse.

Usage: Specify a number from 0 to 1000. The default is 340.

Example: `set r1-first-digit-timer = 300`

Dependencies: You must set Signaling-Mode to R1-Inband for R1-First-Digit-Timer to have any effect.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: R1-ANIR-Delay, R1-ANIR-Timer, R1-Modified, R1-Use-ANIR, Signaling-Mode

R1-Modified

Description: Enables or disables a modified version R1 signaling required in Taiwan.

Usage: TAOS units located in Taiwan should set R1-Modified to Yes. It is set to No by default, which indicates regular R1 signaling (described in the ITU recommendation Q.310-332).

Example: `set r1-modified = yes`

Dependencies: You must set Signaling-Mode to R1-Inband for R1-Modified to have any effect.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: R1-ANIR-Delay, R1-ANIR-Timer, R1-First-Digit-Timer, R1-Use-ANIR, Signaling-Mode

R1-Use-ANIR

Description: Enables and disables Automatic Number Identification (ANI) processing.

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

- Yes specifies that the system performs ANI processing on incoming calls.
- No specifies that the system does not perform ANI processing on incoming calls.

Example: `set r1-use-anir = yes`

Dependencies: You must set Signaling-Mode to R1-Inband for R1-Use-ANIR to have any effect.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: R1-ANIR-Delay, R1-ANIR-Timer, R1-First-Digit-Timer, R1-Modified, Signaling-Mode

R2-Signaling-Enabled

Description: Indicates whether R2 signaling is enabled.

Usage: The R2-Signaling-Enabled setting is read only. Yes indicates that R2 signaling is enabled. No indicates that R2 signaling is not enabled.

Example: `r2-signaling-enabled = no`

Location: Base

See Also: AIM-Enabled, Countries-Enabled, Data-Call-Enabled, D-Channel-Enabled, Frame-Relay-Enabled, MAXLink-Client-Enabled, Modem-Dialout-Enabled, Multi-Rate-Enabled, Switched-Enabled

Rad-Acct-Client

Description: A subprofile that enables you to define how the TAOS unit interacts as a client to Remote Authentication Dial-In User Service (RADIUS) accounting servers.

Usage: With External-Auth as the working profile, list the Rad-Acct-Client subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Rad-Acct-Client subprofile:

```
admin> list rad-acct-client
[in EXTERNAL-AUTH:rad-acct-client]
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 = 0
acct-sess-interval = 0
acct-id-base = acct-base-10
acct-limit-retry = 0
acct-drop-stop-on-auth-fail = no
acct-stop-only = yes
acct-radius-compat = old-ascend
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: External-Auth

See Also: Acct-Drop-Stop-On-Auth-Fail, Acct-ID-Base, Acct-Key, Acct-Limit-Retry, Acct-Port, Acct-RADIUS-Compat, Acct-Server-N, Acct-Sess-Interval, Acct-Src-Port, Acct-Stop-Only, Acct-Timeout

Rad-Auth-Client

Description: A subprofile that enables you to define how the TAOS unit interacts as a client to Remote Authentication Dial-In User Service (RADIUS) authentication servers.

Usage: With External-Auth as the working profile, list the Rad-Auth-Client subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Rad-Auth-Client subprofile:

```
admin> list rad-auth-client
[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-pool = no
auth-timeout = 0
auth-rsp-required = no
auth-sess-interval = 0
auth-ts-secure = yes
auth-Send67 = yes
auth-frm-adr-start = no
auth-boot-host = 0.0.0.0
auth-boot-host-2 = 0.0.0.0
auth-boot-port = 0
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 = "@/\%"
auth-req-delim-count = 0
auth-req-strip-side = none
id-auth-prefix = ""
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: External-Auth

See Also: Auth-Boot-Host, Auth-Boot-Host-2, Auth-Boot-Port, Auth-Frm-Adr-Start, Auth-ID-Fail-Return-Busy, Auth-ID-Timeout-Return-Busy, Auth-Keep-User-Name, Auth-Key, Auth-Pool, Auth-Port, Auth-RADIUS-Compat, Auth-Realm-Delimiters, Auth-Req-Delim-Count, Auth-Req-Strip-Side, Auth-Rsp-Required, Auth-Send67, Auth-Server-N, Auth-Sess-Interval, Auth-Src-Port, Auth-Timeout, Auth-TS-Secure, ID-Auth-Prefix

Rad-Auth-Server

Description: A subprofile that enables you to define how Remote Authentication Dial-In User Service (RADIUS) clients interact with the TAOS unit. With the appropriate software, clients can issue RADIUS commands for session termination and filter changes.

Usage: With External-Auth as the working profile, list the Rad-Auth-Server subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Rad-Auth-Server subprofile:

```
admin> list rad-auth-server
[in EXTERNAL-AUTH:rad-auth-server]
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 +
auth-netmask = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0+
auth-key = " "
radius-server-compat = old-ascend
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: External-Auth

See Also: Auth-Attribute-Type, Auth-Client N, Auth-Key,
Auth-Netmask N (N = 1–9), Auth-Port, Auth-Session-Key, RADIUS-Server-Compat

RADIUS-Change-Enabled

Description: Specifies whether the system generates a trap when a new Remote Authentication Dial-In User Service (RADIUS) server is being accessed. This trap returns the objectID and IP address of the new server.

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

- Yes specifies that the system generates a trap when a new RADIUS server is being accessed.
- 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

RADIUS-Server-Compat

Description: Enables or disables Vendor-Specific Attribute (VSA) compatibility mode when the unit is acting as a Remote Authentication Dial-In User Service (RADIUS) server that is able to accept requests for certain limited purposes, such as changing a filter or disconnecting a user.

Usage: Specify one of the following settings:

- Old-Ascend (the default) specifies that the 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. All attributes are sent in standard RFC format.
- 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: At this time, only NavisRadius supports 16-bit VSAs.

Example: `set radius-server-compat = vendor-specific`

Location: External-Auth > Rad-Auth-Server

See Also: Acct-RADIUS-Compat, Auth-RADIUS-Compat, Call-Log-RADIUS-Compat

Rad-Serv-Enable

Description: Specifies whether Remote Authentication Dial-In User Service (RADIUS) clients can send RADIUS commands for session termination and filter changes to the TAOS unit.

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

- Yes specifies that RADIUS clients can send RADIUS commands to the TAOS unit.
- No specifies that RADIUS clients cannot send RADIUS commands to the TAOS unit.

Example: `set rad-server-enable = no`

Location: External-Auth

See Also: Auth-Attribute-Type, Auth-Client N, Auth-Key, Auth-Netmask N (N = 1–9), Auth-Port, Auth-Session-Key, Rad-Auth-Server

RARP-Enabled

Description: Enables the TAOS unit to use the Reverse Address Resolution Protocol (RARP) to obtain its IP address from a RARP server.

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

- Yes enables the TAOS unit to use RARP to obtain its IP address from a RARP server.
- No disables the TAOS unit's ability to use RARP.

Example: `set rarp-enabled = yes`

Location: IP-Global

See Also: Atalk-Peer-Mode, Proxy-Mode

Read-Access-Hosts

Description: An array containing up to eight IP addresses of SNMP managers that have Read permission. If Enforce-Address-Security is set to Yes, the TAOS unit responds to SNMP Get and Get-Next commands only from the SNMP managers you specify in the array.

Usage: Each element in the array can specify an IP address. When SNMP is the working profile, you can use the List command to display the array elements. You can then set the Read-Access-Hosts parameter to the numeric index of one of the array elements and the value for that element. Or, you can specify an array element without listing the array.

Example: To list the array elements and specify the Read-Access-Hosts [1] value:

```
admin> list read-access-hosts
[in SNMP:read-access-hosts]
read-access-hosts[1] = 0.0.0.0
read-access-hosts[2] = 0.0.0.0
read-access-hosts[3] = 0.0.0.0
read-access-hosts[4] = 0.0.0.0
read-access-hosts[5] = 0.0.0.0
read-access-hosts[6] = 0.0.0.0
read-access-hosts[7] = 0.0.0.0
read-access-hosts[8] = 0.0.0.0
admin> set 1 10.2.3.4/24
```

To specify the Read-Access Hosts [1] value without listing the array:

```
admin> set read-access-hosts 1 10.2.3.4/24
```

Dependencies: You must set the Enforce-Address-Security parameter to Yes in the SNMP profile for the Read-Access-Hosts setting to have any effect.

Location: SNMP

See Also: Enforce-Address-Security, Read-Community, Read-Write-Community, Write-Access-Hosts

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.

Example: `set read-community = unit0`

Location: SNMP

See Also: Enforce-Address-Security, Read-Access-Hosts, Read-Write-Community, Write-Access-Hosts

Read-Write-Access

Description: Specifies whether the TAOS unit grants the SNMPv3 User-based Security Model (USM) user read and write access to its Management Information Base (MIB) settings.

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

- Yes specifies that the TAOS unit grants the SNMPv3 USM user read and write access to its MIB settings.
- No specifies that the TAOS unit does not grant the SNMPv3 USM user read and write access to its MIB settings. The user has read access only, which enables viewing but not modification of the MIBs.

Example: `set read-write-access = no`

Location: SNMPv3-USM-User *name*

See Also: Active-Enabled, Auth-Protocol, Name, Password, Priv-Protocol

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

See Also: Enforce-Address-Security, Read-Access-Hosts, Read-Community, Write-Access-Hosts

Read-Write-Enabled

Description: Enables or disables read-write access to the unit's MIB.

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

- Yes specifies that if the management station provides the correct read-write community string, the unit allows the MIB to be modified by means of Set requests.
- No specifies that the unit responds only to Get and Get Next requests.

Example: `set read-write-enabled = yes`

Dependencies: Read-Write-Enabled does not apply to SNMPv3 messages.

Location: SNMP

See Also: Read-Write-Community

Receive-Auth-Mode

Description: Specifies the authentication protocol to use for incoming Point-to-Point Protocol (PPP), Multilink Protocol (MP), and Multilink Protocol Plus (MP+) calls.

Usage: Specify one of the following settings:

Setting	Description
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, 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. When you specify this setting, 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.

Example: `set receive-auth-mode = both-ppp-auth`

Dependencies: Consider the following:

- When Calling-Line ID (CLID) authentication is in use, the Receive-Auth-Mode value is superseded by the Send-Auth-Mode setting in the local Connection profile.
- You must specify a password for each PPP call if Receive-Auth-Mode is set to any value other than No-PPP-Auth.

Location: Answer-Defaults > PPP-Answer

See Also: PPP-Answer, Recv-Password, Send-Auth-Mode

Recv-AH

Description: A subprofile that enables you to configure IP Security (IPSec) Authentication Header (AH) processing for packets received through the tunnel.

Usage: With IPSec as the working profile, list the Recv-AH subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Recv-AH subprofile:

```
admin> list
[ in IPSEC/greg:recv-ah ]
active = no
spi = 1
ah-type = none
key =
replay-protection = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IPSec *name*

See Also: Active, AH-Type, Key, Replay-Protection, Send-AH, SPI

Recv-ESP

Description: A subprofile that enables you to configure IP Security (IPSec) Encapsulating Security Payload (ESP) settings for packets received through the tunnel.

Usage: With IPSec as the working profile, list the Recv-ESP subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Recv-ESP subprofile:

```
admin> list
[ in IPSEC/greg:recv-esp ]
active = no
spi = 1
version = 0
esp-type = none
iv-len = 32
key =
key2 =
key3 =
auth-type = none
auth-key =
replay-protection = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IPsec *name*

See Also: Active, Auth-Key, Auth-Type, ESP-Type, IV-Len, Key, Key2, Key3, Replay-Protection, Send-ESP, SPI, Version

Recv-Password

Description: Specifies the password that the TAOS unit must receive from the caller.

Usage: Specify a text string of up to 20 characters. The password is case sensitive. If the TAOS unit does not require a password from the remote end, accept the default of null.

Example: `set recv-password = remote`

Dependencies: If Receive-Auth-Mode is set to No-PPP-Auth, Recv-Password does not apply to Point-to-Point Protocol (PPP) calls. You must specify a value for Recv-Password if Receive-Auth-Mode specifies an authentication mode.

Location: Connection *station* > PPP-Options, Connection *station* > ARA-Options

See Also: ARA-Enabled, ARA-Options, PPP-Options, Receive-Auth-Mode, Send-Password

Redirect-Address

Description: Specifies the IP address to which matching packets are redirected.

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

Example: `set redirect-address = 10.10.10.3`

Location: Connection *station* > Port-Redirect-Options

See Also: Port-Number, Protocol

Redundancy

Description: A profile containing configuration settings for redundant controllers.

Usage: Use the Read and List commands to make Redundancy the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make Redundancy the working profile and list its contents:

```
admin> read redundancy
REDUNDANCY read
```

```
admin> list
[in REDUNDANCY]
primary-preference = no-preference
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
REDUNDANCY written
```

Dependencies: Make your settings on the primary controller. Values written on the secondary controller might be overwritten.

See Also: Primary-Preference

Redundancy-Stats

Description: A read-only profile containing statistical information about redundant controllers.

Usage: Use the Read and List command to make Redundancy-Stats the working profile and list its contents.

Example: admin> read redundancy-stats
REDUNDANCY-STATS read

```
admin> list
[in REDUNDANCY-STATS]
context-stats = [ { monitoring secondary defer-to-running +
```

See Also: Context-Stats, Context-Stats N, Fan, Function, Last-Reboot, Prior-Function, Select-Reason, State

Registration-Retries

Description: Specifies the maximum number of registration attempts that a MultiVoice gateway can make during a registration cycle until it registers successfully or all attempts have failed.

Usage: Specify a number from 1 to 200. The default is 5.

Example: set registration-retries = 10

Dependencies: Any change to the value of Registration-Retries becomes effective in the next registration cycle.

Location: VoIP {x y}

See Also: Gatekeeper-Keepalive, Registration-Retry-Timer

Registration-Retry-Timer

Description: Specifies the time interval (in seconds) between each registration attempt with a MultiVoice Access Manager (MVAM).

Usage: Specify a number from 1 to 200. The default is 5.

Example: `set registration-retry-timer = 10`

Dependencies: Any change to the value of Registration-Retry-Timer becomes effective in the next registration cycle.

Location: VoIP {x y}

See Also: Gatekeeper-Keepalive, Registration-Retries

Remote-Address

Description: Specifies the IP address of the remote station. The TAOS unit uses the value you specify to match the address presented by an incoming IP connection.

Usage: Specify an IP address in dotted decimal notation. Separate the optional subnet mask from the address by entering a forward slash. The default is 0.0.0.0.

Example: `set remote-address = 10.77.156.4/24`

Location: Connection *station* > IP-Options

See Also: IP-Options, Local-Address

Remote-Configuration

Description: Specifies whether a Remote Authentication Dial-In User Service (RADIUS) server remotely configures a login banner and a list of Telnet hosts.

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

- Yes enables the TAOS unit to retrieve the login banner and list of Telnet hosts from RADIUS.
- No specifies that you must specify the banner and list of Telnet hosts in a local Terminal-Server profile.

Example: `set remote-configuration = no`

Dependencies: If terminal services are disabled or RADIUS is not in use, Remote-Configuration does not apply.

Location: Terminal-Server > Menu-Mode-Options

See Also: Banner, Host-N, Menu-Mode-Options, Text-N

Replay-Protection

Description: Enables or disables sequence-number processing. The receiving system uses a sequence number to detect arrival of duplicate packets within a constrained window.

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

- Yes enables sequence-number processing. If you specify Yes for Replay-Protection in the Send-AH subprofile, the TAOS unit generates a sequence number for packets it sends through the tunnel. At present, the TAOS unit does not verify the sequence of packets it receives from the L2TP Network Server (LNS), even if Replay-Protection is enabled in the Recv-AH subprofile.
- No disables sequence-number processing.

Example: `set replay-protection = yes`

Location: IPSec *name* > Recv-AH, IPSec *name* > Recv-ESP, IPSec *name* > Send-AH, IPSec *name* > Send-ESP

See Also: Active, AH-Type, Auth-Key, Auth-Type, ESP-Type, IV-Len, Key, Key2, Key3, SPI, Version

Reply-Enabled

Description: Enables or disables the system's response to Dynamic Host Configuration Protocol (DHCP) requests from the client using the Connection profile.

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

- Yes enables DHCP responses on the interface.
- No disables DHCP responses on the interface.

Example: `set reply-enabled = yes`

Location: Connection *station* > DHCP-Options

See Also: Maximum-Leases, Pool-Number

Reqd-State

Description: Specifies the required operational state of a slot or device.

Changing the value of Reqd-State initiates a state change. The state change is complete when the Reqd-State value is equal to the Device-State or Current-State value.

Usage: In a Device-State profile, specify one of the following values:

- Down-Reqd-State requires the device to be in a nonoperational state.
- Up-Reqd-State requires the device to be in normal operations mode.

In a Slot-State profile, specify one of the following values:

- Reqd-State-Down requires the slot to be in a nonoperational state.
- Reqd-State-Up requires the slot to be in normal operations mode.

Example: `set reqd-state = down-req-state`

Dependencies: You can also set Req-State by using the Device or Slot command. In a Slot-State profile, setting Req-State to Down-Req-State does not persist across system resets.

Location: Device-State { {shelf-*N* slot-*N* *N*} *N*}, Slot-State {shelf-*N* slot-*N* *N*}

See Also: Current-State, Device-State

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 { {shelf-*N* slot-*N* *N*} *N*} > OSPF,
Connection *station* > IP-Options > OSPF-Options

See Also: IP-Options, OSPF, OSPF-Options, Transit-Delay

Retry-Count

Description: Specifies the maximum number of times that the TAOS unit attempts to establish a tunnel. Any change you make to this value takes effect when the previous timer expires.

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

Example: `set retry-count = 10`

Dependencies: Retry-Count applies only if you have set L2TP-Mode to LAC.

Location: L2-Tunnel-Global > L2TP-Config

See Also: Control-Connect-Establish-Timer, First-Retry-Timer, Hello-Timer,
LAC-Incoming-Call-Timer

Retry-Limit

Description: Controls the maximum number of attempts that the TAOS unit makes to establish an Ascend Tunnel Management Protocol (ATMP) tunnel before switching to an alternative Home Agent.

Usage: Specify an integer from 1 to 100. The default is 10.

Example: `set retry-limit = 25`

Location: ATMP

See Also: Agent-Mode, Agent-Type, Password, Retry-Timeout, UDP-Port

Retry-Timeout

Description: Controls the time (in seconds) that the unit must wait between retries when attempting to establish an Ascend Tunnel Management Protocol (ATMP) tunnel.

Usage: Specify the number of seconds. The default is 3, which is appropriate for most sites.

Example: `set retry-timeout = 5`

Location: ATMP

See Also: Agent-Mode, Agent-Type, Password, Retry-Timeout, UDP-Port

RIP

Description: Specifies Routing Information Protocol (RIP) behavior for a Connection profile:

- In the IP-Options subprofile, the RIP setting specifies whether the link runs RIP version 1 (RIP-v1) or RIP version 2 (RIP-v2), and whether it sends updates, receives them, or both.
- In the IPX-Options subprofile, the RIP setting specifies whether the link runs IPX RIP when the peer is a router.

Note: The 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: In the IP-Options subprofile, specify one of the following settings:

Setting	Description
Routing-Off (the default)	The TAOS unit does not send routing updates, and ignores any routing updates it receives for the connection.
Routing-Send-Only	The TAOS unit sends RIP-v1 routing updates, but ignores any it receives for the connection.
Routing-Recv-Only	The TAOS unit does not send RIP-v1 routing updates, but accepts any routing updates it receives for the connection.
Routing-Send-And-Recv	The TAOS unit both sends RIP-v1 routing updates and accepts any it receives for the connection.
Routing-Send-Only-V2	The TAOS unit sends RIP-v2 routing updates, but ignores any it receives for the connection.
Routing-Recv-Only-V2	The TAOS unit does not send RIP-v2 routing updates, but accepts any routing updates it receives for the connection.
Routing-Send-And-Recv-V2	The TAOS unit both sends RIP-v2 routing updates and accepts any it receives for the connection.

In the IPX-Options subprofile, specify one of the following settings:

Setting	Description
Off (the default)	IPX RIP is turned off for the connection.
Send	The TAOS unit sends IPX RIP packets, but does not accept any on the connection.
Recv	The TAOS unit accepts IPX RIP packets, but does not send any on the connection.
Both	The TAOS unit both sends and accepts IPX RIP packets on the connection.

Example: `set rip = routing-send-only-v2`

Dependencies: If the TAOS unit does not route either IP or IPX for the connection, or if both IP routing and IPX routing are globally disabled, RIP does not apply.

Location: Connection *station* > IP-Options, Connection *station* > IPX-Options

See Also: Dial-Query, IP-Options, IPX-Header-Compression, IPX-Options, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Alias, Net-Number, Peer-Mode, RIP, RIP2-Use-Multicast, RIP-ASE-Type, RIP-Mode, RIP-Policy, RIP-Pref, RIP-Tag, SAP, SAP-Filter, Summarize-RIP-Routes

RIP2-Use-Multicast

Description: Enables or disables the default Routing Information Protocol version 2 (RIP-v2) behavior of using the multicast address (224.0.0.9) to send and receive updates.

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

- Yes enables RIP-v2 to use the multicast address (224.0.0.9) instead of the broadcast address for its updates.
- No disables the use of the multicast address for RIP updates. The updates revert to the use of the broadcast address. Use this setting if you must use the broadcast address for backward compatibility with other systems.

Example: `set rip2-use-multicast = yes`

Dependencies: The RIP2-Use-Multicast setting does not apply to RIP-v1.

Location: IP-Interface

See Also: RIP, RIP-ASE-Type, RIP-Mode, RIP-Policy, RIP-Pref, RIP-Tag, Summarize-RIP-Routes

RIP-ASE-Type

Description: Specifies the Open Shortest Path First (OSPF) Autonomous System External (ASE) type associated with Routing Information Protocol (RIP) routes.

Usage: Specify one of the following values:

- A value of 1 indicates Type-1 metrics. A Type-1 external metric is expressed in the same units as the link-state metric (interface cost). Type-1 is the default.
- A value of 2 indicates Type-2 metrics. A Type-2 external metric is considered larger than any link-state path. Use of Type-2 external metrics assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.

Example: `set rip-ase-type = 1`

Location: IP-Global

See Also: ASE-Type

RIP-Mode

Description: Specifies whether the interface should run Routing Information Protocol version 1 (RIP-v1) or version 2 (RIP-v2), and whether it sends updates, receives them, or both.

The 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: Specify one of the following settings:

Setting	Description
Routing-Off (the default)	The TAOS unit does not send routing updates, and ignores any routing updates it receives for the connection.
Routing-Send-Only	The TAOS unit sends RIP-v1 routing updates, but ignores any it receives for the connection.
Routing-Recv-Only	The TAOS unit does not send RIP-v1 routing updates, but accepts any routing updates it receives for the connection.
Routing-Send-And-Recv	The TAOS unit both sends RIP-v1 routing updates and accepts any it receives for the connection.
Routing-Send-Only-V2	The TAOS unit sends RIP-v2 routing updates, but ignores any it receives for the connection.
Routing-Recv-Only-V2	The TAOS unit does not send RIP-v2 routing updates, but accepts any routing updates it receives for the connection.
Routing-Send-And-Recv-V2	The TAOS unit both sends RIP-v2 routing updates and accepts any it receives for the connection.

Example: `set rip-mode = routing-send-only-v2`

Location: IP-Interface { {shelf-*N* slot-*N* *N*} *N*}

See Also: RIP, RIP2-Use-Multicast, RIP-ASE-Type, RIP-Policy, RIP-Pref, RIP-Tag, Summarize-RIP-Routes

RIP-Policy

Description: Specifies whether the TAOS unit propagates routes back to the subnet from which they were received. If the router is running Routing Information Protocol (RIP), the RIP-Policy setting must specify a policy for outgoing update packets that include routes received on the same interface as the one that sent the update.

Usage: Specify one of the following values:

- `Poison-Rvrs` (the default) specifies that the TAOS unit propagates routes back to the subnet from which they were received, but with a metric of 16 (infinite metric).
- `Split-Horzn` specifies that the TAOS unit does not propagate routes back to the subnet from which they were received.

Dependencies: Consider the following:

- All the default RIP-related settings in a VRouter profile are the values recommended for most sites.
- Unless the system supports RIP-v1, the RIP-Policy setting does not apply.

Example: `set rip-policy = split-horzn`

Location: IP-Global, VRouter

See Also: RIP, RIP2-Use-Multicast, RIP-ASE-Type, RIP-Mode, RIP-Pref, RIP-Tag, Summarize-RIP-Routes

RIP-Pref

Description: Specifies the default preference for routes that the TAOS unit learns from the Routing Information Protocol (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—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 rip-pref = 50`

Location: IP-Global

See Also: Down-Preference, OSPF-ASE-Pref, OSPF-Pref, Preference, Static-Pref

RIP-Queue-Depth

Description: Specifies the maximum size of the queue for RIP packets.

Usage: Specify the maximum number of packets from 0 to 1024. The default is 0 (zero), which prevents the TAOS unit from dropping packets, no matter what the state of the routing subsystem or system memory. If a queue grows too large in a heavily loaded routing environment, the system can ultimately run out of memory.

Example: `set rip-queue-depth = 128`

Location: IP-Global

See Also: Queue-Depth

RIP-Tag

Description: Specifies a tag to associate with RIP routes. A tag is a 32-bit hexadecimal number. Open Shortest Path First (OSPF) border routers can use the tag to filter a record.

Usage: Specify a 32-bit hexadecimal number. The default is c8:00:00:00.

Example: `set rip-tag = cfc80000`

Location: IP-Global

See Also: ASE-Tag

RIP-Trigger

Description: Specifies whether the IP router or Virtual Router (VRouter) tags routes that have been updated in the routing table and sends updates that include only the changed routes.

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

- Yes specifies that the router tags changes to its routing table and includes only the tagged routes in its next update. Changes occur when a call arrives or disconnects, RIP or Open Shortest Path First (OSPF) learns a route from another router, or the administrator modifies a route-related profile. The router broadcasts updates 5 to 8 seconds after the first change in the routing table is detected. The delay helps to prevent constant updates during peak traffic conditions. The result is reduced processing overhead in the router as well as its neighbors.
- No specifies that the router sends full table updates every 20 to 40 seconds. The full table update is no longer broadcasted at fixed 30-second intervals, to prevent RIP routers on a network from synchronizing and sending large updates in unison.

Example: `set rip-trigger = no`

Location: IP-Global, VRouter

See Also: RIP, RIP-Policy, Summarize-RIP-Routes

Rlogin

Description: Enables or disables the use of the Rlogin command from the terminal-server interface.

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

- Yes enables the use of the Rlogin command.
- No disables the use of the Rlogin command. If Rlogin is set to No and a user attempts to initiate an Rlogin session in the terminal-server interface, the following message appears:

```
rlogin: not enabled
```

Example: `set rlogin = yes`

Dependencies: If terminal services are disabled, Rlogin does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration > Rlogin-Options

See Also: Max-Source-Port, Min-Source-Port

Rlogin-Options

Description: A subprofile containing options for configuring Rlogin connections.

Usage: With Terminal-Mode-Configuration subprofile as the working profile, list the Rlogin-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Rlogin-Options subprofile:

```
admin> list rlogin-options
[ in TERMINAL-SERVER:terminal-mode-configuration:rlogin-options ]
rlogin = no
max-source-port = 1023
min-source-port = 128
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Max-Source-Port, Min-Source-Port, Rlogin

Robbed-Bit-Mode

Description: Specifies the call-control mechanism for robbed-bit signaling. The mechanisms you can specify are based on the AT&T Special Access Connections specification for ACCUNET T1.5 services (AT&T TR 41458).

Usage: Specify one of the following values:

- Wink-Start (the default) specifies that the switch can seize the trunk by going off hook. The local unit requires the switch to wait for a 200msec wink when it seizes a trunk.
- Idle-Start specifies that both ends seize a trunk by simply going off hook.
- Inc-W-200 specifies wink-wink signaling with a 200msec wink time.
- Inc-W-400 specifies wink-wink signaling with a 400msec wink time. Some switches that miss a wink might require the Inc-W-400 setting.
- Loop-Start specifies that the TAOS unit uses loop-start signaling instead of wink signaling. If you specify this setting, only Multilink Protocol Plus (MP+) and Point-to-Point Protocol (PPP) provide an indication of call establishment or call termination. Using this setting for other types of calls is strongly discouraged. Specify it only if you cannot get wink signaling on your T1 access line.
- Ground-Start specifies that the TAOS unit uses ground-start signaling.

Example: `set robbed-bit-mode = wink-start`

Dependencies: Consider the following:

- Robbed-Bit-Mode applies only when Signaling-Mode is set to Inband.
- Regardless of the type of call-control mechanism you choose, the switch must not forward dialed digits to the TAOS unit. Doing so disrupts the handshaking process during multichannel calls.

Location: T1 {shelf-*N* slot-*N N*} > Line-Interface

See Also: Line-Interface, Signaling-Mode

Route-Address

Description: Specifies a route address that the TAOS unit compares to a packet's route address (after applying the mask specified by Route-Mask).

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0, which matches all route addresses in all packets.

Example: `set route-address = 10.62.201.56`

Location: Filter *filter-name* > Input-Filters > Route-Filter,
Filter *filter-name* > Output-Filters > Route-Filter

Dependencies: Route-Address applies only if Type is set to Route-Filter.

See Also: Action, Add-Persistence, Input-Filters, Output-Filters, Route-Filter, Route-Filter (subprofile), Route-Mask, Source-Address, Source-Address-Mask, Type

Route-Description-List

Description: A subprofile that contains a series of private routing table configurations.

Usage: With a Private-Route-Table profile as the working profile, use the List command to display the contents of the Route-Description-List subprofile. To return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Route-Description-List subprofile:

```
admin> list route-description-list
[in PRIVATE-ROUTE-TABLE/robin:route-description-list]
route-description-list[1] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[2] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[3] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
.....
route-description-list[24] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Private-Route-Table *name*

See Also: Route-Description-List N

Route-Description-List N

Description: A subprofile that enables you to define a private routing table.

Usage: With a Private-Route-Table profile as the working profile, use the List command to display the configuration for one of the Route-Description-List subprofiles. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Route-Description-List[1] subprofile:

```
admin> list route-description-list 1
[in PRIVATE-ROUTE-TABLE/robin: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
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Private-Route-Table *name* > Route-Description-List

See Also: Dest-Address, Enabled, Gateway-Address, Metric, Netmask

Route-Filter

Description: Specifies the route filter to apply to a LAN interface (in an IP-Interface profile) or a WAN interface (in a Connection profile).

Usage: Specify the name of the Filter profile that contains the route-filter definition. The default is null.

Example: `set route-filter = route-test`

Dependencies: The Route-Filter setting applies only if you have defined a route filter in the Route-Filter subprofile.

Location: Connection *station* > IP-Options, IP-Interface { { shelf-*N* slot-*N* *N* } *N* }

See Also: Action, Add-Persistence, Route-Address, Route-Filter (subprofile), Route-Mask, Source-Address, Source-Address-Mask, Type

Route-Filter (subprofile)

Description: A subprofile containing a route-filter specification.

Usage: With a Filter profile as the working profile, list the Route-Filter subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Route-Filter subprofile:

```
admin> list input-filters 1 route-filter
[in FILTER/test:input-filters[1]:route-filter]
source-address-mask = 255.255.255.192
source-address = 200.100.50.128
route-mask = 0.0.0.0
route-address = 0.0.0.0
add-metric = 0
action = none
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name* > Input-Filters, Filter *filter-name* > Output-Filters

See Also: Action, Add-Persistence, Input-Filters, Output-Filters, Route-Address, Route-Filter, Route-Mask, Source-Address, Source-Address-Mask, Type

Route-Mask

Description: Specifies a mask that the unit applies to the Route-Address before comparing the resulting value to the route address in a packet. You can use Route-Mask to hide the host portion of a route, or the host and subnet portion.

After translating the Mask and Route-Address into binary format, the TAOS unit applies the mask to the specified Route-Address by performing a logical AND. The mask hides the bits that appear behind each binary 0 (zero) in the mask.

Usage: Specify a mask in dotted decimal notation. A mask of all 1s (FF:FF:FF:FF:FF:FF:FF:FF) masks no bits, so the Route-Address value must match the full route address for a single host. The default is 0.0.0.0, which matches all route addresses.

Example: `set route-mask = 255.255.255.0`

Dependencies: Route-Mask applies only if Type is set to Route-Filter.

Location: Filter *filter-name* > Input-Filters > Route-Filter,
Filter *filter-name* > Output-Filters > Route-Filter

See Also: Action, Add-Persistence, Input-Filters, Output-Filters, Route-Address, Route-Filter, Route-Filter (subprofile), Source-Address, Source-Address-Mask, Type

Routing-Metric

Description: Assigns a RIP-style metric to a route.

Usage: Specify an integer from 1 to 15. The default is 7.

Example: `set routing-metric = 1`

Location: Answer-Defaults > IP-Answer, Connection *station* > IP-Options

See Also: IP-Answer, IP-Options, Private-Route, RIP

RT-Fax-Enable

Description: Enables or disables T.38 fax call processing.

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

- Yes specifies that the unit switches over from a voice session to fax when it detects a Caller-Entered Digits (CED) tone or V.21 High-Level Data Link Control (HDLC) flag. The TAOS unit detects a fax tone if RT-Fax-Enable is set to Yes in the default VoIP profile or if it receives the relevant Internet Protocol Device Control (IPDC) message from the signaling gateway.
- No specifies that the unit passes fax tones as though they were normal voice samples.

Example: `set rt-fax-enable = yes`

Dependencies: For the other settings in the RT-Fax-Options subprofile to apply, you must set RT-Fax-Enable to Yes.

Location: VoIP { *x y* } > RT-Fax-Options

See Also: Command-Spoof, ECM-Enable, Local-Retransmit-LSF, Low-Latency-Mode

RT-Fax-Options

Description: A subprofile that enables you to finetune the performance of real-time fax processing.

Usage: With a VoIP profile as the working profile, list the RT-Fax-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the RT-Fax-Options subprofile:

```
admin> list rt-fax-options
[In VOIP/{ 0 0 }:rt-fax-options]
rt-fax-enable = no
ecm-enable = yes
low-latency-mode = yes
command-spoof = yes
local-retransmit-lsf = yes
packet-redundancy = 0
fixed-packets = yes
max-rate = 14400
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: VoIP { x y }

See Also: Command-Spoof, ECM-Enable, Fixed-Packets, Local-Retransmit-LSF, Low-Latency-Mode, Max-Rate, Packet-Redundancy, RT-Fax-Enable

RX-Cell-Payload-Descramble-Disabled

Description: Enables or disables descrambling of the 48-byte Asynchronous Transfer Mode (ATM) cell payload in received cells.

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

- Yes disables descrambling of the 48-byte ATM cell payload in received cells.
- No enables descrambling of the 48-byte ATM cell payload in received cells.

Example: `set rx-cell-payload-descramble-disabled = yes`

Dependencies: Set RX-Cell-Payload-Descramble-Disabled to Yes only if the transmitting switch has disabled the corresponding scramble function.

Location: OC3-ATM {shelf-N slot-N N} > Line Config

See Also: RX-Descramble-Disabled

RX-Data-Rate-Limit

Description: Specifies the maximum data rate (in kilobits per second) to be received across the connection. You can use this setting to limit bandwidth for a connection according to the rate charged for the account.

Usage: Specify a number from 0 to 64000. The default is 0 (zero), which disables the data-rate limit feature. If the value you specify is larger than the actual bandwidth provided by the line, the connection behaves as though the data-rate limit were disabled, except that additional computations are performed unnecessarily.

Example: `set rx-data-rate-limit = 32000`

Dependencies: The system activates configurable receive data-rate limits only for connections that use unchannelized DS3 cards. If you specify a value for a connection that does not use these cards, the system ignores the settings.

Location: Connection > Session-Options

See Also: TX-Data-Rate-Limit

RX-Descramble-Disabled

Description: Enables or disables descrambling of the entire Asynchronous Transfer Mode (ATM) receive stream.

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

- Yes disables descrambling of the entire ATM receive stream.
- No enables descrambling of the entire ATM receive stream.

Dependencies: Set RX-Descramble-Disabled to Yes only if the transmitting switch has disabled the corresponding scramble function.

Location: OC3-ATM {shelf-*N* slot-*N* *N*} > Line Config

See Also: RX-Cell-Payload-Descramble-Disabled

S

SAP

Description: Specifies IPX Service Advertising Protocol (SAP) behavior for the connection when the peer is a router.

Usage: Specify one of the following values:

- Off (the default) specifies that SAP is turned off for the connection.
- Send specifies that the TAOS unit sends SAP packets, but does not accept any on the connection.
- Recv specifies that the TAOS unit accepts SAP packets, but does not send any on the connection.
- Both specifies that the TAOS unit both sends and accepts SAP packets on the connection.

Example: `set sap = both`

Dependencies: If the TAOS unit does not route IPX for the connection, or if IPX routing is globally disabled, SAP does not apply.

See Also: Dial-Query, IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Alias, Net-Number, Peer-Mode, RIP, SAP-Filter

SAP-Filter

Description: Specifies the Service Advertising Protocol (SAP) filter to apply to the connection.

A SAP filter includes or excludes specific servers or services from the TAOS unit's SAP table. If the directory services feature is not supported, servers or services that are not in the table are inaccessible to clients across the WAN.

Usage: Specify the name of a SAP filter defined in the IPX-SAP-Filter profile. The default is null.

Example: `set sap-filter = Alameda`

Dependencies: If the TAOS unit does not route IPX for the connection, or if IPX routing is globally disabled, SAP-Filter does not apply.

Location: Connection *station* > IPX-Options

See Also: Dial-Query, IPX-Header-Compression, IPX-Routing-Enabled, IPX-SAP-HS-Proxy, IPX-SAP-HS-Proxy-Net, Net-Alias, Net-Number, Peer-Mode, RIP, SAP

Save-Level

Description: Indicates the lowest level of log messages that the TAOS unit displays in the log status window when you use the Log command.

Usage: Specify one of the following settings:

Setting	Lowest-level message indicates
None (the default)	The TAOS 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	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	State and status changes that are commonly not of general interest have occurred.
Debug	Helpful debugging information.

Example: `set save-level = error`

Dependencies: Log levels are also configurable on a per-user basis in User profiles.

Location: Log

See Also: Facility, Host, Log-Display-Level, Save-Number, Syslog-Enabled

Save-Number

Description: Specifies the maximum number of log messages that the TAOS unit saves for display in the status windows.

Usage: Specify an integer. The default is 100.

Example: `set save-number = 150`

Location: Log

See Also: Facility, Host, Log-Display-Level, Save-Level, Syslog-Enabled

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 between 24 and 999. The default is 24 lines.

Example: `set screen-length = 68`

Location: User

See Also: Screen-Width

Screen-Width

Description: Specifies the number of characters allowed on a command line or terminal-server banner.

Usage: Specify an integer from 80 to 255. The default is 80.

Example: `set screen-width = 100`

Location: User

See Also: Screen-Length

SDTN-Packets-Server

Description: Specifies whether Quick Transaction Protocol (QTP) forwards packets to a transaction server for High-Level Data Link Control-Normal Response Mode (HDLC-NRM) or Visa terminal connections.

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

- Yes specifies that the unit establishes HDLC-NRM or Visa terminal connections.
- No specifies that the unit establishes HDLC-NRM or Visa terminal connections but drops the data.

Example: `set sdtm-packets-server = yes`

Location: Connection *station*

See Also: HDLC-NRM-Options

Sec-Domain-Name

Description: Specifies a secondary domain name that the TAOS unit searches by means of the Domain Name System (DNS).

Usage: Specify a secondary domain name. The default is null.

Example: `set sec-domain-name = xyz.com`

Location: IP-Global, VRouter *name*

See Also: Domain-Name, DNS-Primary-Server, DNS-Secondary-Server

Secondary-Controller-State-Change-Enabled

Description: Specifies whether a trap is sent to NavisAccess whenever the secondary controller goes in or out of service.

Usage: Specify one of the following values:

- Yes (the default) specifies that a trap is sent to NavisAccess when the secondary controller goes in or out of service.
- No specifies that a trap is not sent to NavisAccess when the secondary controller goes in or out of service.

Example: `set secondary-controller-state-change-enabled = no`

Location: Trap *host-name*

See Also: Trap

Secondary-IP-Address

Description: Specifies the IP address to use for communicating with a secondary signaling gateway.

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

Example: `set secondary-ip-address = 10.1.2.3`

Dependencies: Consider the following:

- If Enabled is set to No in the SS7-Gateway profile, Secondary-IP-Address does not apply.
- If you specify values for Secondary-IP-Address and Secondary-TCP-Port, the TAOS unit uses the secondary signaling gateway only when the primary gateway is unavailable.
- The primary and secondary IP address and TCP port values can specify two Ethernet interfaces of the same signaling gateway.

Location: SS7-Gateway

See Also: Primary-IP-Address, Primary-TCP-Port, Secondary-TCP-Port

Secondary-TCP-Port

See Also: Specifies the TCP port to use for communicating with a secondary signaling gateway.

Usage: Specify a port number. The default is 0 (zero).

Example: `set secondary-tcp-port = 5000`

Dependencies: Consider the following:

- If Enabled is set to No in the SS7-Gateway profile, Secondary-TCP-Port does not apply.
- If you specify values for Secondary-IP-Address and Secondary-TCP-Port, the TAOS unit uses the secondary signaling gateway only when the primary gateway is unavailable.
- The primary and secondary IP address and TCP port values can specify two Ethernet interfaces of the same signaling gateway.

Location: SS7-Gateway

See Also: Primary-TCP-Port, Secondary-IP-Address

Secondary-Tunnel-Server

Description: Specifies the IP address or hostname of the Ascend Tunnel Management Protocol (ATMP) secondary Home Agent, or of the secondary tunnel server for a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnel. The TAOS unit initiates a connection to the host after a connection attempt to Primary-Tunnel-Server times out or the Foreign Agent receives an error code in an ATMP Register-Reply or Challenge-Request message.

Usage: Specify an IP address in dotted decimal notation, or a symbolic hostname containing up to 31 characters. The default is 0.0.0.0.

If you specify a hostname, the TAOS unit 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. The IP address must be the system address, not the IP address of the interface on which the unit receives tunneled data.

Example: The following setting specifies an IP address and UDP port number:

```
admin> set secondary-tunnel-server = 10.11.22.33:8877
```

The following setting specifies a hostname and UDP port number:

```
admin> set secondary-tunnel-server = tunnel.company.com:6969
```

Dependencies: You must set Profile-Type to Mobile-Client for the Secondary-Tunnel-Server setting to apply.

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: Connection *station* > Tunnel-Options

See Also: Home-Network-Name, Max-Tunnels, Password, Primary-Tunnel-Server, Profile-Type, UDP-Port

Second-Data-Forward-Character

Description: Specifies the hexadecimal value of the second character to be used as a trigger to forward data.

Usage: Specify a hexadecimal value. The default is 06.

Example: `set second-data-forward-character = 07`

Location: Connection *station* > Visa2-Options

See Also: First-Data-Forward-Character, Fourth-Data-Forward-Character, Third-Data-Forward-Character

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 TAOS unit adds or subtracts bandwidth.

Usage: Specify an integer from 1 to 300. The default is 15 seconds.

Example: `set seconds-history = 60`

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 TAOS 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.

Location: Answer-Defaults > MPP-Answer, Connection *station* > MPP-Options

See Also: Add-Persistence, Aux-Send-Password, Bandwidth-Monitor-Direction, Decrement-Channel-Count, Dynamic-Algorithm, Enabled, Increment-Channel-Count, MPP-Answer, MPP-Options, Sub-Persistence, Target-Utilization

Security-Enabled

Description: Specifies whether the TAOS unit traps security events and sends a trap Protocol Data Unit (PDU) to the Simple Network Management Protocol (SNMP) manager when one of the following events occurs:

- Authentication
- Console
- UseExceeded
- Password
- RadiusChange
- CallLogServChange
- VoipGkChange

Security events notify users of security problems and track access to the unit.

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

- Yes specifies that the TAOS unit sends security-event traps to the host specified by Host-Address.
- No specifies that the TAOS unit does not send security-event traps.

Example: `set security-enabled = yes`

Location: Trap *host-name*

See Also: Alarm-Enabled, Community-Name, Host-Address, Host-Name, Port-Enabled

Security-For-Direct-Access

Description: Specifies the type of security required for the direct-access dial-out service.

Usage: Specify one of the following values:

- None (the default) specifies that no password is required for the direct-access dial-out service.
- User specifies that a local Connection profile or remote Remote Authentication Dial-In User Service (RADIUS) profile must be configured to allow dial-out.
- Global specifies that a user must specify the password indicated by the Password-For-Direct-Access setting.

Example: `set security-for-direct-access = global`

Dependencies: If Direct-Access is set to No, Security-For-Direct-Access does not apply.

Location: Terminal-Server > Dialout-Configuration

See Also: Direct-Access, Password-For-Direct-Access, Port-For-Direct-Access

Security-Level

Description: Specifies the level of security to use when generating messages.

Usage: Specify one of the following values:

- None (the default) specifies no authentication and no privacy. No security level checking is required for incoming messages.
- Auth-Priv specifies authentication and privacy. All user transmissions with a security level of None or Auth-NoPriv are rejected with the error message `Unsupported Security Level`. For SNMPv3 USM privacy support, specify Auth-Priv.
- Auth-NoPriv specifies authentication and no privacy. The SNMPv3-USM-User profile for the user sending a message must have Auth-Protocol set to a value other than No-Auth.

Example: `set security-level = auth-nopriv`

Dependencies: Consider the following:

- Security-Level does not apply to SNMPv1 messages.
- For the Auth-Priv setting to apply, you must set the Priv-Protocol and Priv-Password parameters in the SNMPv3-USM-User profile.

Location: SNMP, SNMPv3-Target-Param *name*

See Also: Active-Enabled, Host-Port, Msg-Proc-Model, Notify-Tag-List, Security-Model, Security-Name, SNMP-Message-Type, Tag, Target-Params-Name

Security-Mode

Description: Specifies the type of terminal-server security in use.

Usage: Specify one of the following values:

- None (the default) specifies that a username and password are not required for terminal-server access.
- Partial specifies that a username, password, or both are required in command mode, but not in menu mode. If an interactive user toggles between menu mode and command mode, a password and username are required only upon entry to command mode.
- Full specifies that a username, password, or both are required in order to enter the terminal server in both command mode and menu mode.

Example: `set security-mode = full`

Location: Terminal-Server

See Also: Menu-Mode-Options, System-Password

Security-Model

Description: Specifies the security model to use when generating SNMP messages.

Usage: Specify one of the following values:

- V1 (the default) specifies the SNMP version 1 security model.
- V3-USM specifies the SNMP version 3 User-Based Security Model (USM). For SNMPv3 Notifications support, specify V3-USM.

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 *name*

See Also: Active-Enabled, Host-Port, Msg-Proc-Model, Notify-Tag-List, Security-Level, Security-Name, Tag, Target-Params-Name

Security-Name

Description: Specifies a security name that 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 *name*

See Also: Active-Enabled, Host-Port, Msg-Proc-Model, Notify-Tag-List, Security-Level, Security-Model, Tag, Target-Params-Name

SEL

Description: Specifies the Selector field of the Domain-Specific Part (DSP) of an ATM End System Address (AESAs)—a hexadecimal number that is not used for Asynchronous Transfer Mode (ATM) routing, but can be used by the end system.

Usage: Specify a value 1 byte long (2 hexadecimal digits).

Example: `set sel = 82`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > ATM-Address > AESA-Address > DSP-Portion,
Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr > AESA-Address > DSP-Portion,
Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr > AESA-Address > DSP-Portion

See Also: ESI, HO-DSP

Selection-Timeout

Description: Specifies the number of milliseconds that must elapse before the TAOS unit's attempt to establish a Quick Transaction Protocol (QTP) connection with a transaction server times out.

Usage: Specify a number from 0 to 65000. The default is 10000.

Example: `set selection-timeout = 5000`

Location: Transaction-Server

See Also: Hunting-Mechanism

Selectools-Enabled

Description: Indicates whether Selectools™ software is enabled.

Usage: The Selectools-Enabled setting is read only. Yes indicates that Selectools are enabled. No indicates that Selectools are disabled.

Location: Base

See Also: MAXLink-Client-Enabled, PHS-Support

Select-Reason

Description: Specifies the basis on which this controller was assigned the current function.

Usage: The Select-Reason setting is read only. It can have one of the following values:

- No-Reason
- 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-Fans
- Remote-Matches-Fans
- 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
- Communication-Loss

Example: select-reason = prior-local-primary

Location: Redundancy-Stats > Context-Stats > Context-Stats *N*

See Also: Prior-Function

Send-AH

Description: A subprofile that enables you to configure IP Security (IPSec) Authentication Header (AH) processing for packets sent through the tunnel.

Usage: With IPSec as the working profile, list the Send-AH subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Send-AH subprofile:

```
admin> list
[In IPSEC/greg:send-ah]
active = no
spi = 1
ah-type = none
key =
replay-protection = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IPSec *name*

See Also: Active, AH-Type, Key, Recv-AH, Replay-Protection, SPI

Send-Auth-Mode

Description: Specifies the authentication protocol that the TAOS unit requests when initiating an outgoing call with Point-to-Point Protocol (PPP), Multilink Protocol (MP), or Multilink Protocol Plus (MP+) encapsulation. The answering side of the connection determines which authentication protocol the connection uses (if any). If Calling-Line ID (CLID) authentication is in use, the Send-Auth-Mode setting also defines the authentication protocol to use for incoming calls.

Usage: Specify one of the following settings:

Setting	Description
No-PPP-Auth (the default)	No authentication is requested.
PAP-PPP-Auth	The connection requests Password Authentication Protocol (PAP). The remote end sends its password in the clear. The password is not encrypted. The remote device must support PAP, and you must specify a password by means of the Send-Password setting.

Setting	Description
CHAP-PPP-Auth	The connection requests 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.
MS-CHAP-PPP-Auth	The connection requests MS-CHAP, designed mostly for Windows NT or LAN Manager platforms.

Example: `set send-auth-mode = any-ppp-auth`

Dependencies: Consider the following:

- For most incoming calls, the Send-Auth-Mode setting has no effect. It is superseded by the Answer-Default profile's Receive-Auth-Mode setting, which specifies the authentication method for incoming PPP calls. However, if CLID authentication is in use, the Send-Auth-Mode setting defines the authentication protocol to use for incoming calls, and the Receive-Auth-Mode setting is ignored.
- If you specify PAP-PPP-Auth, the remote device must support PAP, and you must enter a password for Send-Password.
- If you specify CHAP-PPP-Auth, the remote device must support CHAP, and you must enter a password for Send-Password.

Location: Connection *station* > PPP-Options

See Also: PPP-Options, Receive-Auth-Mode, Send-Password

SendDisc-Val

Description: Specifies the number of seconds the TAOS unit waits before sending an ISDN disconnect to the switch.

Usage: Specify an integer. The default is 0 (zero).

Example: `set sendDisc-val = 10`

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Line-Interface

Send-ESP

Description: A subprofile that enables you to configure IP Security (IPSec) Encapsulating Security Payload (ESP) settings for packets sent through the tunnel.

Usage: With IPSec as the working profile, list the Send-ESP subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Send-ESP subprofile:

```
admin> list
[ in IPSEC/greg:send-esp ]
active = no
spi = 1
version = 0
esp-type = none
iv-len = 32
key =
key2 =
key3 =
auth-type = none
auth-key =
replay-protection = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IPsec *name*

See Also: Active, Auth-Key, Auth-Type, ESP-Type, IV-Len, Key, Key2, Key3, Recv-ESP, Replay-Protection, SPI, Version

Send-ICMP-Dest-Unreachable

Description: Specifies whether the unit sends Internet Control Message Protocol (ICMP) destination-unreachable packets.

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

- Yes specifies that the unit sends ICMP destination-unreachable packets.
- No specifies that the unit does not send ICMP destination-unreachable packets.

Example: `set send-icmp-dest-unreachable = no`

Dependencies: Consider the following:

- Set Send-ICMP-Dest-Unreachable to No only in VoIP environments. Doing so in a non-VoIP environment can break required behavior for IPv4 routers, such as Path MTU Discovery.
- When operating under heavy call volumes, enabling this parameter reduces the load placed on the shelf controller.
- For Voice over IP (VoIP) applications, UDP for-me packets can arrive at a rate of 200 packets per second for each direction of the call. If the TAOS unit is not listening on a port for the for-me packets while setting up or tearing down a call, the unit returns ICMP destination-unreachable packets at the same rate as the call. To prevent the performance penalty caused by this situation, set Send-ICMP-Dest-Unreachable to No.
- For H.323 VoIP, the value of Send-ICMP-Dest-Unreachable must be set to Yes for MultiVoice operations. Doing so allows the TAOS unit to detect and respond to misdirected ICMP packets by responding with an ICMP unreachable packet, rather than by redirecting the packet to the shelf controller.

Location: IP-Global

See Also: VoIP-Enabled

Send-Password

Description: Specifies the password that the TAOS unit sends to the remote end during authentication of an outgoing Point-to-Point Protocol (PPP) connection.

Usage: Specify up to 20 characters. The password is case sensitive. If the remote end does not require a password, accept the default of null.

Example: `set send-password = unit0`

Dependencies: You must specify a value for Send-Password when Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Cache-Token authentication is in use. If the Connection profile does not make outgoing calls, do not enter a value for Send-Password.

Location: Connection *station* > PPP-Options

See Also: PPP-Options, Recv-Password, Send-Auth-Mode

Sequential-Calls-Enable

Description: Specifies whether callers who must enter a PIN to authenticate MultiVoice calls can dial subsequent Voice over IP (VoIP) calls without reentering the PIN.

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

- Yes specifies that each user need only enter his or her PIN for the initial VoIP call. Each user can place additional calls without subsequent authentication.
- No specifies that each user must enter his or her PIN for each additional call.

Example: `set sequential-calls-enable = no`

Dependencies: Consider the following:

- The unit must be configured for two-stage dialing and PIN collection. That is, VPN-Mode must be set to No.
- If the original call was operator-assisted, the caller is automatically disconnected.
- If the original call used single-stage dialing, the caller is automatically disconnected.

Location: VoIP { *x y* }

See Also: VPN-Mode

Serial

Description: A profile that specifies physical interface settings for a system serial interface.

Usage: Use the Read and List commands to make Serial the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: On a MAX TNT unit:

```
admin> read serial { 1 c 2 }
SERIAL/{ shelf-1 controller 2 } read
admin> list
[in SERIAL/{ shelf-1 controller 2 }]
physical-address* = { shelf-1 controller 2 }
term-rate = 9600-bps
flow-control = none
user-profile = admin
auto-logout = no
admin> set auto-logout = yes
admin> write
SERIAL/{ shelf-1 controller 2 } written
```

On an APX 8000 unit:

```
admin> read serial { 1 first 2 }
SERIAL/{ shelf-1 left-controller 2 } read
admin> list
[in SERIAL/{ shelf-1 left-controller 2 }]
physical-address* = { shelf-1 left-controller 2 }
term-rate = 9600-bps
flow-control = none
user-profile = admin
auto-logout = no
admin> set auto-logout = yes
admin> write
SERIAL/{ shelf-1 left-controller 2 } written
```

See Also: Auto-Logout, Flow-Control, Physical-Address, Term-Rate, User-Profile

Serial-Number

Description: Displays the TAOS unit's serial number.

Usage: The Serial-Number setting is read only.

Example: serial-number = 6201732

Location: Base, Slot-Info {shelf-*N* slot-*NN*}

See Also: Software-Level, Software-Revision, Software-Version

Server-Address

Description: Specifies the IP address of the default router for client connections.

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

Example: `set server-address = 10.10.10.2`

Location: IP-Global > DHCP-Server

See Also: Active, Boot-File-Path, Default-Lease-Duration, Default-Max-Lease, Default-Pool, Lease-Duration, Static-Address, TFTP-Host-Name

Server-Auth-ID

Description: Specifies the name sent from the Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnel server, during the tunnel authentication phase, to the system initiating the tunnel.

Usage: Specify up to 31 characters. The default is null.

Example: `set server-auth-id = nyserver`

Dependencies: L2F does not support the Server-Auth-ID setting in a Tunnel-Server profile. Also, this setting is currently ignored if specified in a Connection profile.

Location: Connection *station* > Tunnel-Options, Tunnel-Server *name*

See Also: Client-Auth-ID

Server-Endpoint

Description: Specifies the Domain Name System (DNS) hostname or dotted IP address of the L2TP Network Server (LNS), PPTP Network Server (PNS) endpoint, or Layer 2 Forwarding (L2F) endpoint.

Usage: Specify a symbolic hostname or IP address in dotted decimal notation. The default is null.

Example: `set server-endpoint = 200.40.50.2`

Dependencies: To be applied to an IP Security (IPSec) configuration, the Server-Endpoint value must specify the same host as the Tunnel-Address value in the IPSec profile.

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: Tunnel-Server *name*

See Also: Enabled, PPTP-Enabled, Server-Profile-Required, Shared-Secret, Tunnel-Address

Server-Login

Description: Specifies the login name used to authenticate the fax server as part of an outgoing fax session.

Usage: Specify a login name. The default is null.

Example: `set server-login = john`

Dependencies: When the fax server receives a fax from the Internet, it connects to the TAOS unit and sends a name and password. The TAOS unit compares the values to the Server-Login and Server-Password settings.

Location: IP-Fax

See Also: Server-Password

Server-Name

Description: Specifies a local or remote NetWare server. If the server is on the local network and you are specifying a Service Advertising Protocol (SAP) output filter, the Server-Type setting specifies whether to include or exclude advertisements for the server in SAP response packets. If the server is on the remote IPX network and you are specifying a SAP input filter, Server-Type specifies whether to include or exclude the server in the SAP table.

Usage: Specify the name of a NetWare server. You can use the wildcard characters * and ? for partial name matches. The default is null.

Example: `set server-name = server_1`

Location: IPX-SAP-Filter > Input-IPX-SAP-Filters,
IPX-SAP-Filter > Output-IPX-SAP-Filters

See Also: Server-Type, Type-Filter, Valid-Filter

Server-Node

Description: Specifies the node number for the NetWare server.

Usage: Specify a hexadecimal number of up to 12 digits. The default is 00:00:00:00:00:01 (the typical node number for a NetWare file server).

Example: `set server-node = 00:00:00:00:00:01`

Location: IPX-Route *name*

See Also: Active-Route, Dest-Network, Hops, Name, Profile-Name, Server-Socket, Server-Type, Ticks

Server-Password

Description: Specifies the password used to authenticate the fax server as part of an outgoing fax session.

Usage: Specify a password. The default is null.

Example: `set server-password = mypw12!`

Dependencies: When the fax server receives a fax from the Internet, it connects to the TAOS unit and sends a name and password. The TAOS unit compares the values to the Server-Login and Server-Password settings.

Location: IP-Fax

See Also: Server-Login

Server-Profile-Required

Description: Specifies whether Point-to-Point Tunneling Protocol (PPTP) requires a Tunnel-Server profile that matches the PPTP Network Server (PNS) specification in a Connection profile before it creates a tunnel.

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

- Yes specifies that PPTP requires a Tunnel-Server profile that matches the PNS specification in a Connection profile before it creates a tunnel to the server.
- No specifies that PPTP first looks for a matching Tunnel-Server profile, and if it finds one, uses the settings in that profile to create (or refuse) the tunnel. However, if PPTP does not find a matching Tunnel-Server profile, it attempts to create a tunnel anyway.

Example: `set server-profile-required = yes`

Location: L2-Tunnel-Global

See Also: PPTP-Enabled, Tunnel-Server

Server-Socket

Description: Specifies the socket number for the NetWare server.

Usage: Enter a hexadecimal number of up to four digits. Typically, the NetWare file server uses socket 0451. The default is 0000.

Example: `set server-socket = 04:51`

Dependencies: The number you specify must be a well-known socket number. Services that use dynamic socket numbers might use a different socket each time they load and will not work with IPX-Route profiles. To bring up a connection to a remote service that uses a dynamic socket number, specify a master server that uses a well-known socket number on the remote network.

Location: IPX-Route *name*

See Also: Active-Route, Dest-Network, Hops, Name, Profile-Name, Server-Node, Server-Type, Ticks

Server-Type

Description: Specifies the Service Advertising Protocol (SAP) service type of the NetWare server.

Usage: Specify a hexadecimal number of up to four digits. A NetWare file server has SAP service type 0004. You can use the wildcard characters * and ? for partial type matches. FFFF is a wildcard setting that matches all server types. The default is 0000.

Example: `set server-type = 0004`

Dependencies: In a SAP output filter, Server-Type specifies whether to include or exclude advertisements for the service type in SAP response packets. In a SAP input filter, Server-Type specifies whether to include or exclude services of this type in the SAP table. For complete information on SAP service types, refer to your NetWare documentation.

Location: IPX-Route *name*, IPX-SAP-Filter > Input-IPX-SAP Filters, IPX-SAP-Filter > Output-IPX-SAP-Filters

See Also: Active-Route, Dest-Network, Hops, Name, Profile-Name, Server-Name, Server-Node, Server-Socket, Ticks, Type-Filter, Valid-Filter

Service

Description: In the Terminal-Server > Immediate-Mode-Options subprofile, enables or disables immediate mode, and specifies the immediate service type if immediate mode is enabled. In immediate mode, an interactive user immediately connects to a host by means of a specified service.

In the Ext-Tsrv > Hosts-Info *N* subprofile, indicates the type of service to use for the host.

Usage: In the Immediate-Mode-Options subprofile, specify one of the following values:

- None (the default) specifies no immediate service.
- Telnet specifies immediate Telnet service.
- Raw-TCP specifies an immediate TCP connection.
- Rlogin specifies immediate Rlogin service.

In the Hosts-Info *N* subprofile, the Service value is read only. It can be one of the following:

- Telnet indicates Telnet service.
- RawTCP indicates raw TCP service.
- Rlogin indicates Rlogin service.
- PPP indicates PPP service.

Example: `set service = rlogin`

Dependencies: If terminal services are disabled, Service does not apply.

Location: Ext-Tsrv > Hosts-Info *N*, Terminal-Server > Immediate-Mode-Options

See Also: Host, Immediate-Mode-Options, Port, Service, Telnet-Host-Auth

Service-N

Description: Specifies the type of service to use for the host specified by Host-N.

Usage: Specify one of the following values:

- Telnet (the default) specifies Telnet service.
- RawTCP specifies raw TCP service.
- Rlogin specifies Rlogin service.
- PPP specifies PPP service.

Example: `set service-1 = rlogin`

Location: Terminal-Server > Menu-Mode-Options

See Also: Host-N

SessionID-Base

Description: Specifies the base number that the TAOS unit uses for generating a unique ID for each session.

The TAOS unit can pass a session ID to Simple Network Management Protocol (SNMP), Remote Authentication Dial-In User Service (RADIUS), or other external entities. If the value of SessionID-Base is nonzero, the TAOS 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 TAOS unit sets the initial base for session IDs to the absolute clock.

Usage: Specify an integer from 1 to 2147483647. The default is 0 (zero), which causes the TAOS unit to generate a session ID base using the absolute clock.

Example: If SessionID-Base is set to 0 (zero) and 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.

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

See Also: Analog-Encoding, Call-Routing-Sort-Method, Idle-Logout, Name, Parallel-Dialing, Single-File-Incoming, System-Rmt-Mgmt, Use-Trunk-Groups

Session-Info

Description: A subprofile containing default settings for incoming connections. The settings in the Session-Info subprofile are not specific to any encapsulation method or network protocol.

Usage: With Answer-Defaults as the working profile, list the Session-Info subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Session-Info subprofile:

```
admin> list session-info
[ in ANSWER-DEFAULTS:session-info ]
call-filter = ""
data-filter = ""
filter-persistence = no
idle-timer = 120
ts-idle-mode = no-idle
ts-idle-timer = 120
max-call-duration = 0
filter-required = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Call-Filter, Data-Filter, Filter-Persistence, Filter-Required, Idle-Timer, Max-Call-Duration, TS-Idle-Mode, TS-Idle-Timer

Session-Options

Description: A subprofile that specifies session settings not specific to any encapsulation method or network protocol.

Usage: With a Connection profile as the working profile, list the Session-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Session-Options subprofile:

```
admin> list session-options
[ in CONNECTION/tim:session-options ]
call-filter = ""
data-filter = ""
filter-persistence = no
idle-timer = 120
ts-idle-mode = no-idle
ts-idle-timer = 120
backup = ""
max-call-duration = 0
```

```
rx-data-rate-limit = 0
tx-data-rate-limit = 0
filter-required = no
traffic-shaper = 16
cir-timer = 5000
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: Backup, Call-Filter, CIR-Timer, Data-Filter, Filter-Persistence, Filter-Required, Idle-Timer, Max-Call-Duration, RX-Data-Rate-Limit, Traffic-Shaper, TS-Idle-Mode, TS-Idle-Timer, TX-Data-Rate-Limit

Shared-Prof

Description: Specifies whether multiple incoming calls can share a Connection profile.

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

- Yes specifies that the TAOS unit allows more than one caller to share the same profile, provided that no IP address conflicts result.
- No specifies that the TAOS unit does not allow shared profiles.

Example: `set shared-prof = no`

Dependencies: Consider the following:

- Use the Shared-Prof setting only when the TAOS unit dynamically assigns each caller an IP address. A shared profile must not contain a hard-coded remote IP address.
- If you set Shared-Prof to Yes in the IP-Global profile, the Shared-Prof setting in a Connection profile has no effect.
- If you set Shared Prof to No in a Connection profile, the Shared-Prof setting in the IP-Global profile allows or disallows shared profiles systemwide.
- If you set Share-Prof to No in the IP-Global profile, and you specify Yes for Shared-Prof in the Connection profile, the setting in the Connection profile takes precedence.

Location: IP-Global

See Also: Address-Pool, Assign-Count, Must-Accept-Address-Assign, Pool-Base-Address

Shared-Secret

Description: Specifies the shared secret required to bring up a Layer 2 Forwarding (L2F) or Layer 2 Tunneling Protocol (L2TP) tunnel with the specified Server-Endpoint.

Usage: Specify the text of the shared secret. The default is null.

Example: `set shared-secret = 3f4tr`

Dependencies: An L2F tunnel can be authenticated with the same shared secret at both ends.

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: Tunnel-Server *name*

See Also: Enabled, Server-Endpoint

Shelf

Description: Specifies the shelf in which an item resides.

Usage: The Shelf setting is always 1.

Example: `shelf = 1`

Location: Call-Route-Info, Device-Address, Error, Physical-Address

See Also: Call-Route-Info, Device-Address, Item-Number, Physical-Address, Slot

Shelf-Number

Description: Indicates the shelf number of the TAOS unit.

Usage: The Shelf-Number setting is read only and is always 1.

Example: `shelf-number = 1`

Location: Base

See Also: Shelf

Shutdown-Metric

Description: Specifies a number from 0 to 255 to use as a transaction server's current metric if it sends a Quick Transaction Protocol (QTP) status message with a Flow Control Attribute set to Shutdown.

Usage: Specify a number from 0 to 255. The default is 14.

Example: `set shutdown-metric = 15`

Location: Transaction-Server

See Also: Available-Metric, Congested-Metric, Partly-Congested-Metric

Signaling-Heartbeat

Description: A subprofile that enables you to configure signaling heartbeat messages for an SS7 configuration.

Usage: With SS7-Gateway as the working profile, list the Signaling-Heartbeat subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Signaling-Heartbeat subprofile:

```
admin> list signaling-heartbeat
[ in SS7-GATEWAY:signaling-heartbeat ]
enabled = no
interval = 3
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: SS7-Gateway

See Also: Enabled, Interval

Signaling-Mode

Description: Specifies the type of signaling used on a T1 or E1 line.

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

- Inband (the default) specifies inband, robbed-bit signaling. When you specify Inband, the TAOS unit reads Robbed-Bit-Mode for the call-control mechanism.
- ISDN specifies ISDN signaling on the D channel.
- ISDN-NFAS specifies Non-Facility Associated Signaling (NFAS). NFAS enables a group of T1 lines on the same card to share a D channel. All NFAS lines that share a D channel must use the same NFAS group ID. You must configure one of the lines to provide the primary D channel and secondary (backup) D channel.
- R1-Inband specifies R1 inband signaling.
- SS7-Data-Trunk causes the unit to provide clear 64Kbps Signaling System 7 (SS7) data trunk support. If any of the Public Switched Telephone Network (PSTN) switches you are using is a 1AESS switch, which uses robbed-bit signaling, this setting can sometimes cause that switch to receive fluctuating A/B bit status. This condition might ultimately force the line out of service, unless you disable robbed-bit signaling on the 1AESS switch.
- SS7-Robbed-Bit causes the TAOS unit to send a steady A/B bit status on the SS7 data trunk, eliminating the need to disable robbed-bit signaling on the 1AESS switch.
- Tunneler-PRI-Signaling enables the TAOS unit to recognize and respond to ISDN signaling with local B channels controlled by an external Media Gateway Controller. Once selected, PRI tunneling is enabled with the next VoIP call. ISDN Layer 3 signaling is tunneled to an external signaling gateway. All Layer-3 Q.931 messages are tunneled to the gateway configured in the SS7-Gateway profile.

- FGD-In-FGD-Out-Inband specifies that a MultiVoice gateway can receive call-signaling data in Feature Group D (FGD) format and connect VoIP calls to the egress switched telephone network by sending call-signaling data in FGD format.
- FGD-In-FGC-Out-Inband specifies that a MultiVoice gateway can receive call-signaling data in FGD format and connect VoIP calls to the egress switched telephone network by sending call signaling data in FGC (Feature Group C) traditional toll service format.
- FGC-In-FGC-Out-Inband specifies that a MultiVoice gateway can receive call-signaling data in FGC format and connect VoIP calls to the egress switched telephone network by sending call signaling data in FGC (traditional toll service) format.
- FGC-In-FGD-Out-Inband specifies that a MultiVoice gateway can receive call-signaling data in FGC format and connect VoIP calls to the egress switched telephone network by sending call-signaling data in FGD format.

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

- ISDN specifies ISDN signaling on the D channel.
- DTMF-R2-signaling specifies DTMF R2 signaling detection and processing.
- E1-R2-Signaling specifies R2 signaling.
- R1-Inband specifies R1 inband signaling.
- E1-Korean-Signaling specifies a version of the R2 signaling protocol for use in Korea.
- E1-P7-Signaling specifies P7 signaling.
- E1-Chinese-Signaling specifies a version of the R2 signaling protocol for use in China.
- E1-Metered-Signaling specifies the metered R2 signaling protocol, used in Brazil and South Africa.
- E1-No-Signaling specifies a nailed-up line.
- E1-DPNSS-Signaling specifies Digital Private Network Signaling System (DPNSS) or DASS 2 signaling.
- E1-Czech-Signaling specifies KR2 processing, a variation of R2 signaling for the Czech Republic.
- E1-Indian-Signaling specifies R2 signaling for India.
- E1-Argentina-Signaling specifies R2 signaling for Argentina.
- E1-Philippine-Signaling specifies R2 Calling-Line ID (CLID) signaling for the Philippines.
- E1-Brazil-Signaling specifies R2 CLID processing for Brazil.
- E1-Malaysia-Signaling specifies R2 CLID processing for Malaysia.
- E1-New-Zealand-Signaling specifies R2 CLID processing for New Zealand.
- E1-Thailand-Signaling specifies R2 CLID processing for Thailand.
- E1-Israel-Signaling specifies R2 CLID processing for Israel.
- E1-Mexico-Signaling specifies R2 CLID processing for Mexico.
- E1-Kuwait-Signaling specifies R2 CLID processing for Kuwait.

Example: `set signaling-mode = isdn`

Dependencies: Consider the following:

- Signaling-Mode must be set to ISDN (or ISDN-NFAS, for T1) if you are using overlap receiving (Overlap-Receiving is set to Yes). If it is set to any other value, overlap receiving does not apply.
- R1 signaling can optionally be used with Automatic Number Identification (ANI), which is similar to CLID. When ANI is in use, you can specify whether to send an Automatic Number Id Request (ANIR) to the switch. If you specify that the unit must send an ANIR to the switch, you can also specify how long the unit waits before sending the request, and how long the ANIR signal lasts.
- An SS7 data trunk carries no signaling. The SS7-Data-Trunk and SS7-Robbed-Bit values register the line with the signaling gateway and allow the gateway to take control of the line and its calls.
- When you specify Tunneled-PRI-Signaling, PRI tunneling for SS7 VoIP calls is supported only when IPDC signal processing is enabled for the TAOS unit. The Base profile should contain the entry `xcom-ss7=enabled`.

When Signaling-Mode is set to DTMF-R2-Signaling, keep the following information in mind:

- Collect-Incoming-Digits must be set to Yes.
- Assigning a lower value (600 to 3000) for the T1-Inter-Digit-Timeout setting improves call setup times. Assigning a higher value (3001 to 6000) improves DTMF detection.
- DTMF R2 detection is supported only when R2 signal processing is enabled for a TAOS unit.

Location: T1 {shelf-*N* slot-*N N*} > Line-Interface, E1 {shelf-*N* slot-*N N*} > Line-Interface

See Also: Call-By-Call, Caller-ID, Channel-Usage, Data-Service, D-Channel-Enabled, Encoding, FDL, Frame-Type, Line-Interface, NFAS-ID, Number-Complete, Overlap-Receiving, R1-ANIR-Delay, R1-ANIR-Timer, R1-First-Digit-Timer, R1-Modified, R1-Use-ANIR, R2-Signaling-Enabled, Robbed-Bit-Mode, Switch-Type

Silence-Det-Cng

Description: Enables or disables silence detection and suppression, and noise generation.

Usage: Specify one of the following values:

- Yes specifies that silence frames are not passed across the IP network by the TAOS unit. During silent periods, while the call is still connected, the local TAOS unit generates background (comfort) noise to assure the caller that the call is still connected.
- No (the default) specifies that silence is processed as part of the audio stream and that comfort noise is not locally generated.
- Cng-Only enables comfort noise generation when the unit is using a G.723.1 codec running at the 5.3Kbps resampling rate.

Example: `set silence-det-cng = yes`

Dependencies: Consider the following:

- Changes to Silence-Det-Cng become effective with the next Voice over IP (VoIP) call.
- The silence suppression and comfort noise generation features must be enabled on both the local unit and the remote unit involved in a call.
- When you set Silence-Det-Cng to Yes or Cng-Only, the dynamic jitter buffer is not used.
- The Silence-Det-Cng setting is ignored when the TAOS unit uses a G.711 U-Law or G.711 A-Law audio codec.

When a G.723.1 codec is selected:

- Voice announcements do not work if silence suppression is enabled. Internet Protocol Device Control (IPDC) voice announcement Stored Telephone Number (STN) messages are rejected with an MRJ (0xFF) if Packet-Audio-Mode is set to G723 or G723-6.4kps.
- Comfort noise generation can be enabled or disabled for 5.3Kbps processing. With comfort noise enabled, the 5.3 kbps codec can decode silence detection and suppression packets.
- Comfort noise generation cannot be enabled for 5.3Kbps processing unless the adaptive jitter buffer is disabled.
- Silence detection and suppression cannot be enabled for 6.4Kbps processing unless the adaptive jitter buffer is disabled.

Location: VoIP {x y}

See Also: Ena-Adap-Jitter-Buffer, Initial-Jitter-Buffer-Size, Max-Jitter-Buffer-Size, Packet-Audio-Mode, Silence-Threshold

Silence-Threshold

Description: Specifies the relative threshold for silence suppression.

Usage: Specify a number in decibels. The default is 0 (zero).

Example: `set silence-threshold = 3`

Dependencies: Silence-Threshold does not apply if Silence-Det-Cng is set to No.

Location: VoIP {x y}

See Also: Silence-Det-Cng

Silent-Mode

Description: Specifies whether the TAOS unit suppresses status messages when an interactive terminal-server connection is established.

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

- Yes specifies that the TAOS unit suppresses status messages when an interactive terminal-server connection is established.
- No specifies that the TAOS unit sends all status messages when an interactive terminal-server connection is established.

Example: `set silent-mode = yes`

Dependencies: If terminal services are disabled, Silent-Mode does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Terminal-Mode-Configuration

Single-Dial-Enable

Description: Enables or disables single-stage dialing of Voice over IP (VoIP) calls when MultiVoice is configured to perform H.323 call processing.

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

- Yes specifies that the unit extracts the Dialed Number Information Service (DNIS) number from a single dialed entry. The destination number is passed to the remote MultiVoice gateway during call setup.
- No specifies that callers are required to dial into the unit, and then wait for a dial tone before dialing the destination number.

Example: `set single-dial-enable = yes`

Dependencies: Single-stage dialing works with MultiVoice gateways under the following conditions:

- You are using T1 inband trunks and the switch or PBX can relay Dual Tone Multifrequency (DTMF) signals to the MultiVoice gateway.
- You are using T1 PRI trunks.
- You have enabled DNIS on the TAOS unit.

Location: VoIP {x y}

See Also: T1-Inter-Digit-Timeout

Single-File-Incoming

Description: Specifies whether the TAOS unit treats incoming calls as a single-file list, or handles them in parallel.

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

- Yes specifies that the TAOS unit answers and routes one call before answering and routing the next call.
- No specifies that the TAOS unit answers and routes an incoming call immediately.

Example: `set single-file-incoming = yes`

Location: System

See Also: Parallel-Dialing

SLIP

Description: Enables or disables the use of the terminal-server SLIP command.

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

- Yes enables a user to begin Serial Line Internet Protocol (SLIP) sessions from the terminal-server interface.
- No disables a user from beginning SLIP from the terminal-server interface.

Example: `set slip = yes`

Dependencies: If terminal services are disabled, SLIP does not apply.

Location: Terminal-Server > SLIP-Mode-Configuration

See Also: Ping, PPP, Rlogin, SLIP-Mode-Configuration, TCP, Telnet, Traceroute

SLIP-BOOTP

Description: Specifies whether the TAOS unit responds to BOOTP within Serial Line Internet Protocol (SLIP) sessions.

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

- Yes enables the TAOS unit to respond to a BOOTP request from the calling unit during a SLIP session. An interactive user who initiates a SLIP session can use BOOTP to get an IP address from the designated IP address pool.
- No disables BOOTP for a SLIP session. The user is prompted to accept an IP address at the start of the SLIP session.

Example: `set slip-bootp = yes`

Dependencies: If terminal services are disabled, SLIP-BOOTP does not apply.

Location: Terminal-Server > SLIP-Mode-Configuration

See Also: Address-Pool, Assign-Count, Pool-Base-Address, SLIP, SLIP-Mode-Configuration

SLIP-Mode-Configuration

Description: A subprofile with terminal-server configuration options for asynchronous Serial Line Internet Protocol (SLIP) users.

Usage: With Terminal-Server as the working profile, list the SLIP-Mode-Configuration subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the SLIP-Mode-Configuration subprofile:

```
admin> list slip-mode-configuration
[in TERMINAL-SERVER:slip-mode-configuration]
info
slip = no
slip-bootp = no
info = mode-ppp
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server

See Also: SLIP, SLIP-BOOTP

Slot

Description: Specifies the number of the item's expansion slot. For call-routing purposes, a value of 0 (zero) or `any-slot` specifies that the item can use any slot.

Usage: For a Device-Address, Physical-Address, or Call-Route-Info setting, specify an integer. In an Error profile, the Slot setting is read only.

Example: `set slot = 10`

Location: Call-Route-Info, Device-Address, Error, Physical-Address

See Also: Call-Route-Info, Device-Address, Item-Number, Physical-Address, Shelf

Slot-Address

Description: Indicates the physical address of the slot.

Usage: 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. To modify the value after reading a Slot-Info, Slot-State, or Slot-Type profile, use the List and Set commands.

Example: To modify the Slot-Address value, you can list the contents of the subprofile and then specify a slot number:

```
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 slot = slot-8
```

As an alternative, you can simply use the Set command:

```
admin> set slot-address slot = slot-8
```

Location: Slot-Info {shelf-*N* slot-*N* *N*}, Slot-State {shelf-*N* slot-*N* *N*}, Slot-Type {shelf-*N* slot-*N* *N*}

See Also: Physical-Address

Slot-Enabled

Description: Specifies whether the TAOS unit traps slot events and sends a trap Protocol Data Unit (PDU) to the Simple Network Management Protocol (SNMP) manager when the SlotProfileChange event occurs.

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

- Yes specifies that the TAOS unit sends slot-event traps to the host specified by Host-Address.
- No specifies that the TAOS unit does not send slot-event traps.

Example: `set security-enabled = yes`

Location: Trap *host-name*

See Also: Port-Enabled

Slot-Info

Description: A profile that displays the software version, serial number, and other system information about the TAOS unit.

Usage: The Slot-Info profile is read only. Use the Get command to display its contents.

Example: `admin> get slot-info`
[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
hardware-rework-count = 0

See Also: Hardware-Level, Hardware-Rework-Count, Serial-Number, Slot-Address, Software-Level, Software-Release, Software-Revision, Software-Version

Slot-Profile-Change-Enabled

Description: Specifies whether the system generates a trap when a Slot-State profile is created due to slot insertion, or the current-state transitions into Oper-State-Down, Oper-State-Up, Oper-State-Dump, or Oper-State-None.

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

- Yes specifies that the system generates a trap.
- No specifies that the system does not generate a trap.

Example: `set slot-profile-change-enabled = no`

Location: Trap *host-name*

See Also: Current-State, Slot- State

Slot-State

Description: A profile that stores the current state of a slot card. The Slot-State profile does not reside in 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: Use the Read and List commands to make Slot-State the working profile and list its contents.

Example: To make the Slot-State profile with the index { shelf-1 slot-2 0 } the working profile and list its contents:

```
admin> read slot-state {1 2 0}
SLOT-STATE/{ shelf-1 slot-2 0 } read
admin> list
[in SLOT-STATE/{ shelf-1 slot-2 0 }]
slot-address* = { shelf-1 slot-2 0 }
current-state = oper-state-none
reqd-state = reqd-state-up
```

Dependencies: The Slot-State profile is read only.

See Also: Current-State, Reqd-State, Slot-Address

Slot-Type

Description: Specifies the type of device in the slot. If the actual type of device identified by the system at startup differs from the type specified by Slot-Type, the TAOS unit determines that you have changed slot cards. It then deletes the old Simple Network Management Protocol (SNMP) interface numbers.

Usage: Specify one of the following values:

Value	Specifies
none	No card is installed.
unknown	The software does not recognize the card.
shelf-controller	Shelf controller.
router-card	Standalone router card.
8t1-card	T1 card.
8e1-card	E1 card.
4swan-card	Serial WAN (SWAN) card.
10-unchan-t1-card	T1 FrameLine card.
10-unchan-e1-card	E1 FrameLine card.
analog-modem2-card	Analog Modem card.
csmx-card	Series56 II Digital Modem card.
uds3-card	Unchannelized DS3 card.
ds3-atm-card	DS3-ATM card.
4ether2-card	Ethernet2 card.

Value	Specifies
hdlc2-card	Hybrid Access II card.
madd-card	48-port MultiDSP card.
oc3-atm-card	OC3-ATM (fiber) card.
ether3-card	Ethernet3 card.
hdlc2ec-card	Hybrid Access III card.
stm0-card	STM-0 card.
ds3-atm2-card	DS3-ATM2 card.
madd2-card	96-port MultiDSP card.
t3-card	T3 card.

Example: `set slot-type = 8t1-card`

Dependencies: You can also display the slot type for a particular device by using the terminal-server Show command.

Location: Admin-State {shelf-*N* slot-*N* *N*}, Admin-State-Phys-If {shelf-*N* slot-*N* *N*}, Slot-Type {shelf-*N* slot-*N* *N*}

See Also: Slot, Slot-Address, Slot-Info, Slot- State, Slot-Type (profile)

Slot-Type (profile)

Description: A profile that stores the type of slot card installed in each shelf/slot location. The Slot-Type profile resides in NVRAM and persists over system resets. The shelf number is always 1.

Usage: Use the Read and List commands to make Slot-Type the working profile and list its contents.

Example: To make the Slot-Type profile with the index { shelf-1 slot-8 0 } the working profile and list its contents:

```
admin> read slot-type {1 8 0}
SLOT-TYPE/{ shelf-1 slot-8 0 } read

admin> list
[in SLOT-TYPE/{ shelf-1 slot-8 0 }]
slot-address* = { shelf-1 slot-8 0 }
slot-type = 8e1-card
```

Dependencies: The Slot-Type profile is read only.

See Also: Slot, Slot-Address, Slot-Info, Slot- State, Slot-Type

SNMP

Description: A profile containing settings that determine Simple Network Management Protocol (SNMP) security, specify a contact and location, and control which hosts can access the TAOS unit by means of the SNMP manager utilities.

Usage: Use the Read and List commands to make SNMP the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the SNMP profile the working profile and list its contents:

```
admin> read snmp
SNMP read

admin> list
[in SNMP]
enabled = no
read-community = public
read-write-community = write
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 ]
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 = " "
security-level = none
snmp-message-type = v1-and-v3
read-write-enabled = no
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
SNMP written
```

See Also: Contact, Enabled, Enforce-Address-Security, Location, Read-Access-Hosts, Read-Community, Read-Write-Community, Read-Write-Enabled, Security-Level, SNMP-Message-Type, Write-Access-Hosts

SNMP-Interface

Description: Indicates the Simple Network Management Protocol (SNMP) interface number assigned to the device by the system.

Usage: The SNMP-Interface setting is read only.

Example: snmp-interface = 65

Dependencies: At system startup, the TAOS unit reads the Admin-State, 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 system is reset or power cycled, the old device's SNMP interface number is made available for reassignment. Removing a slot card and leaving the slot empty, however, does not free up interface numbers. If you reinstall the slot card, the TAOS unit reassigns the same interface number.

In addition, removing a slot card and replacing it with a slot card of another type does not immediately free up the old interface numbers. New numbers are assigned to the new slot card, and the old numbers become available at the next power cycle or system reset.

Location: Admin-State {shelf-*N* slot-*N* *N*}, Admin-State-Perm-If *station*, Admin-State-Phys-If {shelf-*N* slot-*N* *N*}

See Also: SNMP

SNMP-Message-Type

Description: Specifies the version of Simple Network Management Protocol (SNMP) used by the SNMP agent in the unit.

Usage: Specify one of the following values:

- V1-and-V3 (the default) causes the SNMP agent to use both SNMPv1 and SNMPv3 protocols.
- 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

See Also: Security-Level

SNMPv3-Notification

Description: A profile that enables you to configure SNMPv3 Notifications support.

Usage: Use the Read and List commands to make SNMPv3-Notification the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make SNMPv3-Notification profile *anna* the working profile and list its contents:

```
admin> read snmpv3-notification
[in SNMPV3-NOTIFICATION/anna]
name* = anna
active-enabled = no
tag = ""
type =
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
SNMPV3-NOTIFICATION/anna written
```

See Also: Active-Enabled, Name, Tag

SNMPv3-Target-Param

Description: A profile that enables you to set up security and message-processing features for SNMPv3 Notifications support.

Usage: Use the Read and List commands to make SNMPv3-Target-Param the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the SNMPv3-Target-Param profile sarah the working profile and list its contents:

```
admin> list snmpv3-target-param sarah
[ in SNMPV3-TARGET-PARAM/sarah ]
name* = ""
active-enabled = no
msg-proc-model = v1
security-model = v1
security-name =
security-level = none
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
SNMPV3-TARGET-PARAM/sarah written
```

See Also: Active-Enabled, Msg-Proc-Model, Name, Security-Level, Security-Model, Security-Name

SNMPv3-USM-User

Description: A profile that enables you to configure security features based on the SNMPv3 User-based Security Model (USM) for the specified user.

Usage: Use the Read and List commands to make SNMPv3-USM-User the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the SNMPv3-USM-User profile michael the working profile and list its contents:

```
admin> list snmpv3-usm-user michael
[ in SNMPv3-USM-USER/michael ]
name* = michael
password = *****
active-enabled = no
read-write-access = no
auth-protocol = md5-auth
priv-protocol = no-priv
auth-key = (*)
priv-key = (*)
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
SNMPV3-USM-USER/michael written
```

See Also: Active-Enabled, Auth-Key, Auth-Protocol, Name, Password, Priv-Key, Priv-Protocol, Read-Write-Access

SNRM-Response-Timeout

Description: Specifies the number of milliseconds that the TAOS unit waits for a response to the Set Normal Response Mode (SNRM) packet it sends at the beginning of a High-Level Data Link Control-Normal Response Mode (HDLC-NRM) session.

Usage: Specify a number from 500 to 5000. The default is 2000.

Example: `set snrm-response-timeout = 1000`

Location: Connection *station* > HDLC-NRM-Options

See Also: SNRM-Retry-Counter

SNRM-Retry-Counter

Description: Specifies the number of times that the TAOS unit retries sending a Set Normal Response Mode (SNRM) packet following a response timeout.

Usage: Specify a number from 0 to 255. The default is 2.

Example: `set snrm-retry-counter = 5`

Location: Connection *station* > HDLC-NRM-Options

See Also: SNRM-Response-Timeout

SNTP-Info

Description: A subprofile containing settings required to maintain the system time from a Simple Network Time Protocol (SNTP) server.

Usage: With IP-Global as the working profile, list the contents of the SNTP-Info subprofile.

```
admin> list sntp
enabled = no
GMT-offset = utc+0000
host = [ 0.0.0.0 0.0.0.0 0.0.0.0 ]
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IP-Global

See Also: Enabled, GMT-Offset, Host

Software-Level

Description: Indicates the software-version level of the shelf-controller code.

Usage: The Software-Level setting is read only.

Example: `software-level = H`

Location: Base, Slot-Info {shelf-*N* slot-*N* *N*}

See Also: Hardware-Level, Software-Release, Software-Revision, Software-Version

Software-Release

Description: Displays the engineering or candidate release number of the code image.

Usage: The Software-Release setting is read only.

Example: `software-release = 8.0`

Location: Slot-Info {shelf-*N* slot-*N* *N*}

See Also: Software-Level, Software-Revision, Software-Version

Software-Revision

Description: Indicates the software revision number of the TAOS unit.

Usage: The Software-Revision setting is read only.

Example: `software-revision = 1`

Location: Base, Slot-Info {shelf-*N* slot-*N* *N*}

See Also: Software-Level, Software-Release, Software-Version

Software-Version

Description: Indicates the software version of the TAOS 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 {shelf-*N* slot-*N* *N*}

See Also: Software-Level, Software-Release, Software-Revision

Source-Address

Description: In a Filter profile, specifies a source IP address that the TAOS unit compares to a packet's source IP address (after applying the mask specified by Source-Address-Mask). In a Permit-List subprofile, specifies the IP address of a host or subnet allowed Telnet access to the TAOS unit.

Usage: Specify an IP address in dotted decimal notation. In a Permit-List subprofile, you can enter the subaddress as part of the Source Address value. If you do, the Source-Address-Mask value is set automatically to the corresponding dotted decimal value. The default is 0.0.0.0. In a Filter profile, the default IP address matches all packets.

Example: `set source-address = 10.27.43.1/27`

Dependencies: In a Filter profile, Source-Address applies only if Type is set to IP-Filter or TOS-Filter.

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter, Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter, TACL > Permit-List

See Also: Input-Filters, IP-Filter, Output-Filters, Source-Address-Mask

Source-Address-Mask

Description: In a Filter profile, specifies a mask to apply to the Source-Address value before comparing the value to the source address in a packet. In a Permit-List subprofile, specifies the subnet mask the unit applies to the Source-Address value before permitting Telnet access to a host.

Description: Specify a value in dotted decimal notation. The default is 0.0.0.0.

In a Filter profile, you can use the Source-Address-Mask 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 TAOS unit applies the mask to the address by performing a logical AND. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask. The default value masks all bits. A mask of all ones (255.255.255.255) masks no bits, and specifies the full source address of a single host.

Example: `set source-address-mask = 255.255.255.224`

Dependencies: Consider the following:

- In a Filter profile, Source-Address-Mask applies only if Type is set to IP-Filter or TOS-Filter.
- In a Permit-List subprofile, you can set a subnet value in dotted decimal notation, or by including a subnet as part of the Source Address value.

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter, Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter, TACL > Permit-List

See Also: Input-Filters, IP-Filter, Output-Filters, Source-Address

Source-IP-Check

Description: Enables or disables antispoofing for the session.

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

- 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 IP Control Protocol (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 disables antispoofing for the session.

Example: `set source-ip-check = yes`

Location: Connection *station* > IP-Options

See Also: IP-Address

Source-Port

Description: Specifies a value to compare with the source-port field in a packet.

Usage: Specify a number from 0 to 65535. The default is 0 (zero), which matches any port.

Example: `set source-port = 25`

Dependencies: Consider the following:

- Source-Port applies only if Type is set to IP-Filter or TOS-Filter.
- Only TCP and UDP packets have source-port fields.
- The Src-Port-Cmp setting specifies the type of comparison the TAOS unit makes.

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter, Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter

See Also: Input-Filters, IP-Filter, Output-Filters, Src-Port-Cmp

SPI

Description: Specifies the Security Parameters Index (SPI).

Usage: Specify a 32-bit numeric value from 1 to 2147483647. The default is 1. The SPI in the Send-AH subprofile must match the L2TP Network Server (LNS) SPI in its receiving Authentication Header (AH) configuration, and vice versa. The SPI in the Send-ESP profile must match the LNS SPI in its receiving Encapsulating Security Payload (ESP) configuration.

Example: `set spi = 5`

Location: IPsec *name* > Recv-AH, IPsec *name* > Recv-ESP, IPsec *name* > Send-AH,
IPsec *name* > Send-ESP

See Also: Active, AH-Type, Auth-Key, Auth-Type, ESP-Type, IV-Len, Key, Key2, Key3, Replay-Protection, Send-ESP, SPI, Version

Split-Code-Dot-User-Enabled

Description: Specifies whether the system can split usernames longer than 5 characters under CACHE-TOKEN authentication.

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

- Yes specifies local splitting of usernames. This setting permits the use of usernames longer than 5 characters, so long as you use a typical 4-digit PIN and 6-digit ACE token code.
- No specifies that the system cannot split usernames.

Example: `set split-code-dot-user-enabled = yes`

Location: Connection > PPP-Options

See Also: Disconnect-On-Auth-Timeout, Enabled, Link-Compression, LQM, LQM-Maximum-Period, LQM-Minimum-Period, MRU, Recv-Password, Send-Password

Src-Net-Address

Description: Specifies an IPX network address that the TAOS unit compares to a packet's source IPX network address.

Usage: Specify an IPX network address in hexadecimal format. The default is 00:00:00:00, which matches all packets.

Example: `set src-net-address = 01:01:01:01`

Dependencies: Src-Net-Address applies only if Type is set to IPX-Filter.

Location: Filter *filter-name* > Input-Filters > IPX-Filter,
Filter *filter-name* > Output-Filters > IPX-Filter

See Also: Input-Filters, IPX-Filter, Output-Filters, Type

Src-Node-Address

Description: Specifies an IPX node number that the TAOS unit compares to a packet's source IPX node number.

Usage: Specify an IPX node number in hexadecimal format. The default is 00:00:00:00, which matches all packets.

Example: `set src-node-address = 01:01:01:01`

Dependencies: Src-Node-Address applies only if Type is set to IPX-Filter.

Location: Filter *filter-name* > Input-Filters > IPX-Filter,
Filter *filter-name* > Output-Filters > IPX-Filter

See Also: Input-Filters, IPX-Filter, Output-Filters, Type

Src-Port-Cmp

Description: Specifies the type of comparison that the unit uses to compare the value of Source-Port to a packet's source-port field.

Usage: Specify one of the following values:

- None (the default) specifies that the TAOS unit does not compare the packet's source port number to the Source-Port value.
- Less specifies that port numbers with a value less than the value specified by Source-Port match the filter.
- Eql specifies that port numbers equal to the value specified by Source-Port match the filter.
- Gtr specifies that port numbers with a value greater than the value specified by Source-Port match the filter.
- Neq specifies that port numbers not equal to the value specified by Source-Port match the filter.

Example: `set src-port-cmp = less`

Dependencies: For Src-Port-Cmp to apply, you must set Type to IP-Filter or TOS-Filter. In addition, you can filter only TCP and UDP packets with the Src-Port-Cmp setting because only TCP and UDP packets contain source ports.

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter, Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter

See Also: Input-Filters, IP-Filter, Output-Filters, Source-Port

Src-Socket

Description: Specifies an IPX socket number that the TAOS unit compares to a packet's source IPX socket number.

Usage: Specify an IPX socket number. The default is 00:00, which matches all packets.

Example: `set src-socket = 01:01`

Dependencies: Src-Socket applies only if Type is set to IPX-Filter.

Location: Filter *filter-name* > Input-Filters > IPX-Filter,
Filter *filter-name* > Output-Filters > IPX-Filter

See Also: Input-Filters, IPX-Filter, Output-Filters, Type

Src-Socket-Cmp

Description: Specifies the type of comparison that the unit uses to compare the Src-Socket value to a packet's source-socket field.

Usage: Specify one of the following values:

- None (the default) specifies that the TAOS unit does not compare the packet's source socket number to the Src-Socket value.
- Less specifies that socket numbers with a value less than the value specified by Src-Socket match the filter.
- Eql specifies that socket numbers equal to the value specified by Src-Socket match the filter.
- Gtr specifies that socket numbers with a value greater than the value specified by Src-Socket match the filter.
- Neq specifies that socket numbers not equal to the value specified by Src-Socket match the filter.

Example: `set src-socket-cmp = less`

Dependencies: For Src-Socket-Cmp to apply, you must set Type to IPX-Filter.

Location: Filter *filter-name* > Input-Filters > IPX-Filter,
Filter *filter-name* > Output-Filters > IPX-Filter

See Also: Input-Filters, IPX-Filter, Output-Filters, Type

SS7-Continuity

Description: A subprofile that enables you to specify the type of incoming and outgoing continuity checks to perform for all channels on a line. Both ends of the connection must agree on the continuity check to be used for the line.

Usage: With a T1 or E1 profile as the working profile, enter `list line-interface ss7-continuity`. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the SS7-Continuity subprofile:

```
admin> list line-interface ss7-continuity
[in T1/{ shelf-1 slot-20 28 }:line-interface:ss7-continuity]
incoming-procedure = loopback
outgoing-procedure = single-tone-2010
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface, T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Incoming-Procedure, Outgoing-Procedure

SS7-Gateway

Description: A profile that contains settings for configuring the Internet Call Diversion (ICD) for softswitch signaling gateway.

Usage: Use the Read and List commands to make SS7-Gateway the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make SS7-Gateway the working profile and list its contents:

```
admin> read ss7-gateway
SS7-GATEWAY read

admin> list
[in SS7-GATEWAY]
enabled = no
control-protocol = asgcp
primary-ip-address = 0.0.0.0
primary-tcp-port = 0
secondary-ip-address = 0.0.0.0
secondary-tcp-port = 0
bay-id = ""
system-type = IASCTNT1B
transport-options = { 0 1000 3000 30000 7 6 no }
use-system-ip-address-as-source = yes
signaling-heartbeat = { no 3 }
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
SS7-GATEWAY written
```

See Also: Bay-ID, Control-Protocol, Enabled, Primary-IP-Address, Primary-TCP-Port, Secondary-IP-Address, Secondary-TCP-Port, Signaling-Heartbeat, System-Type, Transport-Options, Use-System-IP-Address-As-Source

Stacking

Description: A profile that contains settings for a stacked unit.

Usage: Use the Read and List commands to make Stacking the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Stacking profile jim the working profile and list its contents:

```
admin> read stacking jim
STACKING/jim read
```

```
admin> list
[in STACKING/jim]
enabled = no
name = jim
udp-port = 5150
multicast-address = 0.0.0.0
multicast-interface-ip-address = 0.0.0.0
data-ip-address = 0.0.0.0
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
STACKING/jim written
```

See Also: Data-IP-Address, Enabled, Multicast-Address, Multicast-Interface-IP-Address, Name, UDP-Port

Stack-Trace

Description: Indicates the stack trace record created when an error occurred.

Usage: The Stack-Trace setting is read only. It consists of an array of 6 elements.

Example: `stack-trace = [000000]`

Location: Error

See Also: Index, IP-Address, IS-Post, Loadname, Shelf, Slot, Type, User-Profile, Version

Start-With-Menus

Description: Determines whether the terminal server presents a menu interface for an interactive user initiating a connection.

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

- Yes specifies that the terminal server starts user logins in menu mode.
- No specifies that the terminal server starts user logins in command mode.

Example: `set start-with-menus = yes`

Dependencies: If terminal services are disabled, Start-With-Menus does not apply.

Location: Terminal-Server > Menu-Mode-Options

See Also: Menu-Mode-Options

State

Description: Current state of the redundant controller.

Usage: The State setting is read only. It can have one of the following 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 = loading`

Location: Redundancy-Stats > Context-Stats > Context-Stats *N*

Static-Address

Description: A subprofile that enables you to configure up to 100 pairs of Internet Protocol (IP) and Media Access Control (MAC) addresses.

Usage: With DHCP-Server as the working profile, list a Static-Address subprofile. You can then use the Set command to modify the settings in the subprofile. To close the subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Static-Address subprofile:

```
admin> list static-address 1
[in IP-GLOBAL:dhcp-server:static-address[1]]
ip-address = 0.0.0.0
ethernet-address = 00:00:00:00:00:00
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IP-Global > DHCP-Server

See Also: Ethernet-Address, IP-Address

Static-Pref

Description: Specifies the default preference given to static IP routes. 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—Open Shortest Path First (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 static-pref = 50`

Location: IP-Global

See Also: Down-Preference, OSPF-ASE-Pref, OSPF-Pref, Preference, RIP-Pref

Station

Description: In a Connection profile, specifies the name of the remote device that communicates with the TAOS unit. In the Admin-State-Perm-If profile, specifies the name of a nailed-up Point-to-Point Protocol (PPP) or Frame Relay connection indicated by a Connection profile or Remote Authentication Dial-In User Service (RADIUS) user profile.

Usage: 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 TAOS unit does not use the Station name to obtain an IP address.

Location: Admin-State-Perm-If, Connection

See Also: Index, Name

Station-Poll-Address

Description: Specifies the address used by a TAOS unit in an HDLC-NRM-SNRM request to poll a secondary transport protocol data unit (TPDU) station in a short-duration transaction network (SDTN).

Usage: Specify an integer from 0 through 255. The default is 255, which is the all-stations address.

Example: `set station-poll-address = 200`

Dependencies: For HDLC-NRM support, Encapsulation-Protocol must be set to HDLC-NRM and SDTN-Packets-Server must be set to Yes in the Connection profile.

Location: Connection > HDLC-NRM-Options

Status-Length

Description: Specifies the number of lines displayed in the Status window, including dividing lines. (For the values 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: Status-Length must be less than Screen-Length by at least six lines.

Location: User

See Also: Screen-Length

STM

Description: A profile that contains configuration settings for the STM-0 card.

Usage: Use the Read and List commands to make STM the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the STM profile with the index { shelf-1 slot-1 0 } the working profile and list its contents:

```
admin> read stm {1 1 0}
STM/{ shelf-1 slot-1 0 } read
admin> list
[in STM/{ shelf-1 slot-1 0 }]
name = " "
physical-address* = { shelf-1 slot-1 0 }
loop-timing = yes
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
STM/{ shelf-1 slot-1 0 } written
```

See Also: Loop-Timing, Name, Physical-Address

Subaddress

Description: Specifies the subaddress portion of the E.164 address of the remote station (if a subaddress is required).

Usage: Specify a subaddress. The default is null.

Example: `set subaddress = 1234`

Location: Connection *station*

See Also: Dial-Number

Sub-Persistence

Description: Specifies the number of seconds that average line utilization (ALU) must persist below the Target-Utilization threshold before the TAOS 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, or 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: Sub-Persistence has little effect when the Seconds-History value is high.

Location: Answer-Defaults > MPP-Answer, Connection *station* > MPP-Options

See Also: Add-Persistence, Bandwidth-Monitor-Direction, Base-Channel-Count, Decrement-Channel-Count, Dynamic-Algorithm, Increment-Channel-Count, Maximum-Channels, Minimum-Channels, Seconds-History, Target-Utilization

Substitute-Recv-Name

Description: Specifies the Point-to-Point Protocol (PPP) called device's name during outgoing calls. Because bidirectional authentication provides a way to formally authenticate the called device during an outgoing call, the name of the device must be checked against a locally defined name. The name can be the dial-out profile name or a substituted name.

Usage: Specify a string of up to 23 characters. The default is null.

Example: `set substitute-recv-name = fred`

Dependencies: Consider the following:

- The value you specify for Substitute-Recv-Name is used only during outgoing calls that use bidirectional authentication.
- If you accept the default of null for Substitute-Recv-Name, the name of the called device is checked against the dial-out profile name.
- Substitute-Recv-Name allows an additional Remote Authentication Dial-In User Service (RADIUS) lookup during an outgoing call.
- Because Substitute-Recv-Name represents the called device's real name, it is sent in RADIUS accounting Start and Stop messages.

Location: Connection > PPP-Options

See Also: Bi-Directional-Auth, Substitute-Send-Name

Substitute-Send-Name

Description: Specifies the name of the PPP calling device during incoming calls to the TAOS unit. This setting provides a unique, substitute name for the calling host to which the TAOS unit connects during incoming calls.

Usage: Specify a name of up to 23 characters. The default is null. If you accept the default, the global system name is used.

Example: `set substitute-send-name = joetnt`

Dependencies: Because bidirectional CHAP authentication provides a way to formally authenticate the calling device during an incoming call, the name of the device must be checked against a locally defined name. The name can be the dial-in profile name or the substituted name provided by Substitute-Send-Name. Although you set this parameter in the PPP-Answer subprofile, the PPP-Options subprofile in the Connection profile includes a copy of this setting.

Location: Answer-Defaults > PPP-Answer, Connection > PPP-Options

See Also: Substitute-Recv-Name

Summarize-RIP-Routes

Description: Specifies whether the TAOS unit or Virtual Router (VRouter) summarizes Routing Information Protocol version 1 (RIP-v1) subnet information when advertising routes. If the TAOS unit summarizes RIP routes, it advertises one route to all the subnets of the same class in the same network.

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

- Yes specifies that the TAOS unit summarizes RIP-v1 subnet information.
- No specifies that the TAOS unit advertises each route as it appears in the routing table.

Example: If Summarize-RIP-Routes is set to Yes, the unit advertises the route to 200.5.8.13/28 (a class C address) as a route to 200.5.8.0. If Summarize-RIP-Routes is set to No, the unit advertises the route to 200.5.8.13/28 as a route to 200.5.8.13.

Dependencies: The Summarize-RIP-Routes setting is not applicable if RIP-v2 is in use or if RIP is turned off.

Location: IP-Global, VRouter

See Also: RIP, RIP-Mode, RIP-Policy

Suppress-Host-Routes

Description: Specifies whether the TAOS unit advertises host routes in each update, which can cause excessive routing overhead:

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

- Yes specifies that host routes are suppressed.
- No specifies that host routes are advertised.

Example: The following set of commands configures the TAOS unit to suppress host routes:

```
admin> read ip-global
IP-GLOBAL read

admin> set suppress-host-routes = yes

admin> write
IP-GLOBAL written
```

Dependencies: If you set Suppress-Host-Routes to Yes, routes are suppressed according to the following rules:

- If a Connection profile specifies a Remote-Address setting with a subnet mask of less than 32 bits, host routes for the interface are suppressed while the session is being negotiated. After the session is established, only network routes are advertised for the interface.
- If a Connection profile specifies a Remote-Address setting with a subnet mask of /32, host routes for the interface are not suppressed.

Location: IP-Global

See Also: Pool-Summary

Suspect-Access-Resource-Enabled

Description: Specifies that whenever a terminating modem, installed MultiDSP card, or installed Hybrid Access card has received four or more calls for which it cannot establish a connection, the TAOS unit sends a Simple Network Management Protocol (SNMP) trap to all managers in the alarm group. Once the managing TAOS unit sends the trap, the suspect terminating resource is not assigned to terminate calls until all available resources are exhausted.

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

- Yes directs the TAOS unit to send a trap when a terminating modem, installed MultiDSP card, or installed Hybrid Access card has received four or more calls for which it could not establish a connection.
- No instructs the TAOS unit not to send the suspectAccessResource trap.

Example: `set suspect-access-resource-enabled = yes`

Dependencies: The Suspect-Access-Resource-Enabled value has an effect only on TAOS units with one or more of the following slot cards installed:

- Analog Modem
- Series56 II or Series56 III Digital Modem
- MultiDSP
- Hybrid Access II or Hybrid Access III

Location: Trap *name*

See Also: Alarm-Enabled, Community-Name, Host-Address, Host-Name, Port-Enabled, Security-Mode

SVC-Address-Info

Description: Indicates an assigned address (for informational purposes only).

Usage: The value of SVC-Address-Info is a read-only ASCII string. The default is null.

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > ATM-Address, Connection *station* > ATM-Options > SVC-Options > Incoming-Caller-Addr, Connection *station* > ATM-Options > SVC-Options > Outgoing-Called-Addr

See Also: E164-Native-Address, Numbering-Plan

SVC-Enabled

Description: Specifies whether the system accepts incoming Asynchronous Transfer Mode (ATM) Switched Virtual Circuit (SVC) calls.

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

- Yes specifies that the system accepts ATM SVC calls.
- No specifies that the system does not accept ATM SVC calls.

Example: `set svc-enabled = yes`

Location: Answer-Defaults > ATM-Answer

See Also: ATM-Answer

SVC-Options

Description: A subprofile that enables you to set values for Switched Virtual Circuits (SVCs).

Usage: With a Frame-Relay, ATM-Interface, or Connection profile as the working profile, list the SVC-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the SVC-Options subprofile:

```
admin> list svc-options
[ in ATM-INTERFACE/ { { any-shelf any-slot 0 } 0 } :svc-options ]
enabled = no
atm-protocol = uni-3.1
atm-address = { undefined "" { undefined { "" "" } { "" "" "" } } +
insert-calling-party-addr = yes
q93b-options = { 2 1 4000 30000 0 10000 4000 120000 4000 }
qsaal-options = { 64 4 25 67 1000 0 0 0 15000 }
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* }, Connection *station* > ATM-Options, Frame-Relay *fr-name*

See Also: ATM-Address, ATM-Protocol, Enabled, FR-Address, Insert-Calling-Party-Addr, Q93B-Options, QSAAL-Options

SWAN

Description: Specifies the action to take when the code image for a Serial WAN (SWAN) card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- Load causes the system to load the image, even if no card of that type is installed.
- Skip causes the system to skip the image, even if a card of that type is installed.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, T3, UDS3, UE1, Unknown-Cards, UT1

SWAN (profile)

Description: A profile that contains line-configuration settings for the Serial WAN (SWAN) card.

Usage: Use the Read and List commands to make SWAN the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the SWAN profile with the index { shelf-1 slot-15 2 } the working profile and list its contents:

```
admin> read swan {1 15 2}
SWAN/{ shelf-1 slot-15 2 } read
admin> list
[in SWAN/{ shelf-1 slot-15 2 }]
name = 1:15:2
physical-address* = { shelf-1 slot-15 2 }
enabled = no
line-config = { 0 0 static { any-shelf any-slot 0 } }
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
SWAN/{ shelf-1 slot-15 2 } written
```

See Also: Enabled, Line-Config, Name, Physical-Address

SWAN-Stat

Description: A profile that displays information about the state of a Serial WAN (SWAN) line.

Usage: Use the Read and List commands to make SWAN-Stat the working profile and list its contents.

Example: To make the SWAN-Stat profile with the index { shelf-1 slot-8 1 } the working profile and list its contents:

```
admin> read swan-stat {1 8 1}
SWAN-STAT/{ shelf-1 slot-8 1 } read
admin> list
[in SWAN-STAT/{ shelf-1 slot-8 1 }]
physical-address* = { shelf-1 slot-8 1 }
line-state = disabled
error-count = 0
```

Dependencies: The SWAN-Stat profile is read only.

See Also: Error-Count, Line-State, Physical-Address

Switched-Call-Type

Description: Specifies the type of bearer-channel capability that the TAOS unit sets up for each switched call in a session.

Usage: Specify one of the following values:

Value	Specifies
Voice	The TAOS unit sets up a voice call, even though the unit will transmit data over the channel. The Voice setting assumes that only 56 Kbps is available.
56K-Restricted	The TAOS unit sets up a data call with an explicit request for 56-Kbps restricted data transfer. Data is transmitted to meet the density requirements for Alternate Mark Inversion (AMI)-encoded T1 lines. These requirements dictate that you cannot transmit 16 consecutive zeros. Use this setting only for a connection that uses robbed-bit signaling.
56K-Clear (the default)	The TAOS unit sets up a data call that uses 56-Kbps of the data channel. 56K-Clear is a common setting for T1 PRI lines.

Value	Specifies
64K-Restricted	The TAOS unit sets up a data call with an explicit request for 64-Kbps restricted data transfer. The call must be set up as a data call at a rate of 64 Kbps on an AMI-encoded line. With each transmission, a binary 1 is inserted in the least significant bit position.
64K-Clear	The TAOS unit sets up a data call that uses the full 64-Kbps bandwidth of the data channel.
384K-Restricted	The TAOS unit sets up a data call that connects to Multi-Rate or GlobanD data services at 384 Kbps.
384K-Clear	The TAOS 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 384-Kbps call coded as Multi-Rate, not H0.
1536K-Clear	The TAOS unit sets up a data call that connects to the Switched-1536 data service at 1536 Kbps. Non-Facility Associated Signaling (NFAS) 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.
128K-Clear to 1472K-Clear (in multiples of 64)	Multi-Rate bit rates.
Modem	The TAOS unit sets up the call as a voice call. When the call is up, the unit routes it to a digital modem.
144-56k-v110	56Kbps unrestricted data transfer and a V.110 bit rate of 14,400bps.
288-56k-v110	56Kbps unrestricted data transfer and a V.110 bit rate of 28,800bps.
144-56kr-v110	56Kbps restricted data transfer and a V.110 bit rate of 14,400bps.
288-56kr-v110	56Kbps restricted data transfer and a V.110 bit rate of 28,800bps.
144-64k-v110	64Kbps unrestricted data transfer and a V.110 bit rate of 14,400bps.
288-64k-v110	64Kbps unrestricted data transfer and a V.110 bit rate of 28,800bps.
144-64kr-v110	64Kbps restricted data transfer and a V.110 bit rate of 14,400bps.
288-64kr-v110	64Kbps restricted data transfer and a V.110 bit rate of 28,800bps.

Example: set switched-call-type = 56k-restricted

Dependencies: To ensure data integrity:

- Use only digital end-to-end connectivity. No analog signals can 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.

Keep in mind the following additional considerations:

- If a nailed-up connection is in use, Switched-Call-Type does not apply.
- If a T1 line is set for ESF/B8ZS signaling, the remote switch or router typically requires that you set Switched-Call-Type to 64K-Clear. A setting of 56K-Clear (the default) is required if the line is set to D4/AMI.
- E1 lines typically use a setting of 64K-Clear.
- If a V.110 device makes a call at 14,400bps or 28,800bps to a TAOS unit with a MultiDSP or MultiDSP2 card, the call automatically connects at 14,400bps or 28,800bps, regardless of the setting of Switched-Call-Type.

Location: Frame-Relay *fr-name*

See Also: Data-Service

Switched-Enabled

Description: Indicates whether the unit can make switched calls.

Usage: The Switched-Enabled setting is read only. Yes indicates that the unit can make switched calls. No indicates that the unit can use only nailed-up links.

Example: `switched-enabled = yes`

Location: Base

See Also: Data-Call-Enabled, D-Channel-Enabled, Multi-Rate-Enabled, R2-Signaling-Enabled

Switch-Type

Description: Specifies the type of network switch that provides ISDN service.

Usage: For a PRI line, you can specify one of the following switch-type settings:

Setting	Specifies
ATT-PRI	AT&T, the default in the U.S.
NT1-PRI	Northern Telecom
GloBanD-PRI	Q.931W GloBanD
Japan-PRI	ISDN PRI in Japan
VN3-PRI	French VN3 ISDN PRI
OneTR6-PRI	German ITR6
Net5-PRI	Euro ISDN services in Belgium, the Netherlands, Switzerland, Sweden, and Singapore
Danish-PRI	ISDN services in Denmark
Austral-PRI	PRI service in Australia
NAT-ISDN-2-PRI	National ISDN-2
BT-SS7	Switch type for Signaling System 7 (SS7) data trunks. You must set Signaling-Mode to SS7-Data-Trunk for the BT-SS7 setting to apply.

E1 lines support the following additional Digital Private Network Signaling System (DPNSS) and DASS 2 switch types:

- ISDX-DPNSS
- ISLX-DPNSS
- Mercury-DPNSS
- DASS2 (U.K. only)
- Switch-CAS (for E1 R1 and R2 signaling)

Example: `set switch-type = ntl-pri`

Dependencies: Consider the following:

- The Switch-Type setting is required for ISDN Non-Facility Associated Signaling (NFAS).
- The BT-SS7 setting is equivalent to the Net5-PRI setting except for the cause codes returned for CLID or DNIS authentication failure. With the Net5-PRI or any Switch-Type setting other than BT-SS7, if a call is rejected because of CLID or DNIS authentication failure, the TAOS unit releases the call with cause code 16 (normal clearing) and location 0 (user). If Switch-Type is set to BT-SS7, the TAOS unit releases the call with cause code 63 (service not available) and location 10 (s). The setting takes effect as soon as the profile is written.

Location: T1 {shelf-*N* slot-*NN*} > Line-Interface, E1 {shelf-*N* slot-*NN*} > Line-Interface

See Also: Line-Interface, Signaling-Mode

Syslog-Enabled

Description: Enables or disables forwarding of log messages to the UNIX Syslog server. Syslog is 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.

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

- Yes enables Syslog updating.
- No disables Syslog updating.

Example: `set syslog-enabled = yes`

Dependencies: Consider the following:

- In the Log profile, the Syslog-Enabled value applies to the first data stream.
- In the Auxiliary-Syslog [1] subprofile, the Syslog-Enabled value applies to the second data stream.
- In the Auxiliary-Syslog [2] subprofile, the Syslog-Enabled value applies to the third data stream.
- The settings in the Auxiliary-Syslog subprofile affect an individual Syslog stream, and override the values specified in the Log profile.

Location: Log, Log > Auxiliary-Syslog

See Also: Facility, Host

Syslog-Level

Description: Indicates the level of log messages to direct to a specified Syslog server. Messages at or above the specified level are sent to the server.

Usage: Specify one of the following settings

Setting	Lowest-level message indicates
None	No log message is directed to the Syslog server.
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	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 (the default)	State and status changes that are commonly not of general interest have occurred.
Debug	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. If you set Syslog-Level to Notice, messages with a level of Notice or higher are sent to the Syslog server.

Example: `set syslog-level = notice`

Dependencies: Consider the following:

- The Syslog-Level value in the Log profile affects the first data stream.
- The Syslog-Level value in the Auxiliary-Syslog [1] subprofile affects the second data stream.
- The Syslog-Level value in the Auxiliary-Syslog [2] subprofile affects the third data stream.
- The settings in the Auxiliary-Syslog subprofile affect an individual Syslog stream, and override the values specified in the Log profile.

Location: Log, Log > Auxiliary-Syslog

See Also: Facility, Host, Port, Syslog-Enabled

System

Description: A profile that contains system-wide settings for call management.

Usage: Use the Read and List commands to make System the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the System profile the working profile and list its contents:

```
admin> read system
SYSTEM read

admin> list
[in SYSTEM]
name = test-227
system-rmt-mgmt = yes
use-trunk-groups = yes
call-routing-sort-method = item-first
idle-logout = 0
parallel-dialing = 2
single-file-incoming = yes
analog-encoding = u-law
sessionid-base = 0
new-nas-port-id-format = yes
perm-conn-upd-mode = all
userstat-format = %i %l %s %r %d %a %u %c %t %n
max-dialout-time = 20
boot-sr-version = 2.1
num-digits-trunk-groups = 1
exclusive-port-routing = no
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
SYSTEM written
```

See Also: Analog-Encoding, Boot-SR-Version, Call-Routing-Sort-Method, Exclusive-Port-Routing, Idle-Logout, Name, Max-Dialout-Time, Num-Digits-Trunk-Groups, Parallel-Dialing, Perm-Conn-Upd-Mode, SessionID-Base, Single-File-Incoming, System-Rmt-Mgmt, Userstat-Format, Use-Trunk-Groups

System-IP-Addr

Description: Designates the source address for IP traffic originating from the TAOS unit or from the global Virtual Router (VRouter).

Usage: Specify an IP address. The default is 0.0.0.0. When you configure a system with redundant shelf controllers, you must set the System-IP-Addr value to the address of the soft IP interface, and not to the address of a particular physical interface. The system IP address must be a single, unchanging address that always maps to the current primary controller. The soft IP interface address is always associated with the current primary controller.

The following algorithm determines the source address of packets from the TAOS unit:

- 1** The source address of IP-routing protocol packets is always the local address of the transmitting interface.
- 2** For incoming Telnet sessions, the source address of transmitted packets is the destination address of the originating TCP SYN packet.
- 3** If the IP-Global profile setting for System-IP-Addr is nonzero, all other transmitted packets have System-IP-Addr as the source address.
- 4** The source address of all other transmitted packets is the local address of the transmitting interfaces.

Protocols that follow this algorithm include the following:

- TCP: Defender, Rlogin, Terminal Access Controller Access Control Plus (TACACS+), Telnet
- UDP: Ascend Password Protocol (APP), Ascend Tunnel Management Protocol (ATMP), Domain Name System (DNS), Remote Authentication Dial-In User Service (RADIUS) accounting, RADIUS authentication, SECURID, Simple Network Management Protocol (SNMP), Syslog, TFTP, Traceroute, Virtual Tunnel Protocol (VTP)

Example: `set system-ip-addr = 10.2.3.4`

Dependencies: Consider the following:

- If the System-IP-Addr becomes unreachable because of a topology change in the network, you can still use Telnet to reach any of the unit's interface addresses (subject to packet filtering throughout the network).
- In an H.323 environment, set System-IP-Addr to the shelf-controller IP address.
- In an Internet Protocol Device Control (IPDC) environment, if the system allocates its own listen address, set System-IP-Addr to the IP address of a LAN interface other than the shelf-controller port.
- The TAOS unit can allocate its own system IP address as the listen IP address and Real-Time Transport Protocol (RTP) port and can specify its own send address and RTP port. For Voice over IP (VoIP) calls, you must avoid routing RTP traffic through the TAOS unit's shelf controller. Therefore, when allowing the TAOS gateway to allocate its own address, you must set the System-IP-Addr value to an interface address other than the shelf-controller Ethernet port.

Location: IP-Global

See Also: Global-VRouter, IP-Address, Local-Address, Remote-Address

System-Password

Description: Specifies a password for access to the terminal server.

Usage: Specify a password of up to 20 characters. The password is case sensitive. The default is null.

Example: `set system-password = unit0`

Dependencies: If terminal services are disabled, System-Password does not apply. If Security-Mode is set to None, the terminal server does not require a password.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Aux-Send-Password, Password, Recv-Password, Security-Mode, Send-Password, Telnet-Password, Terminal-Mode-Configuration

System-Rmt-Mgmt

Description: Enables or disables remote management across multichannel calls.

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

- Yes allows remote management of the TAOS unit.
- No prevents remote management of the TAOS unit.

Example: `set system-rmt-mgmt = yes`

Location: System

See Also: Remote-Configuration

System-Type

Description: Specifies an ASCII string that the TAOS unit sends to the media gateway controller in the device registration message when Control-Protocol is set to IPDC-0.x. The TAOS unit does not interpret the value. Interpretation on the signaling gateway is gateway dependent.

Usage: Specify a text string. The default is null.

Location: SS7-Gateway

See Also: Control-Protocol

T

T1

Description: A profile that contains configuration settings for a T1 line and its channels.

Usage: Use the Read and List commands to make T1 the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the T1 profile with the index { shelf-1 slot-15 2 } the working profile and list its contents:

```
admin> read t1 {1 15 2}
T1/{ shelf-1 slot-15 2 } read

admin> list
[in T1/{ shelf-1 slot-15 2 }]
name = trunk-1
nfas-group-id = 0
physical-address* = { shelf-1 slot-15 2 }
line-interface = { no d4 ami eligible middle-priority inband +
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
T1/{ shelf-1 slot-15 2 } written
```

See Also: Line-Interface, Name, Physical-Address

T1-Duration

Description: Specifies the value of the acknowledgment-delay timer in milliseconds. This timer specifies the maximum delay for an acknowledgment when an Information frame (I-frame) is received.

Usage: Specify a number from 0 to 2147483647. The default is 1000 milliseconds (1 second).

Example: `set t1-duration = 2000`

Dependencies: The value you specify for T1-Duration must be less than the T2 duration timer specified on the signaling gateway.

Location: SS7-Gateway > Transport-Options

See Also: ACK-Threshold, Device-ID, Heart-Beat, T2-Duration, T3-Duration, Window-Size

T1-Inter-Digit-Timeout

Description: Specifies the number of milliseconds the T1 Digital Signal Processor (DSP) waits between digits before considering Dialed Number Information Service/Automatic Number Identification (DNIS/ANI) collection complete.

Usage: Specify a number from 100 to 6000 milliseconds. For backward compatibility, the default is 3 seconds. The setting takes effect with the next incoming call. Specifying a lower value improves call setup time.

Example: `set t1-inter-digit-timeout = 2000`

Dependencies: T1-Inter-Digit-Timeout does not apply unless Collect-Incoming-Digits is set to Yes.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Collect-Incoming-Digits

T1-Retrans-Timer

Description: Specifies the maximum amount of time in ticks the transmitter must wait for an acknowledgment before initiating a recovery procedure.

Usage: Specify a number between 500 and 2000. The default value is 1000 (1 second).

Example: `set t1-retran-timer = 1000`

Location: Answer-Defaults > X75-Answer,
Connection *station* > X75-Options

See Also: Frame-Length, K-Frames-Outstanding, N2-Retransmissions

T1-Stat

Description: A profile that displays information about the state of a T1 line and its channels.

Usage: Use the Read and List commands to make T1-Stat the working profile and list its contents.

Example: To make the T1-Stat profile with the index { shelf-1 slot-8 1 } the working profile and list its contents:

```
admin> read t1-stat {1 8 1}
T1-STAT/{ shelf-1 slot-8 1 } read
```

```

admin> list
[in T1-STAT/{ shelf-1 slot-8 1 }]
physical-address* = { shelf-1 slot-8 1 }
line-state = loss-of-sync
channel-state = [unavailable unavailable unavailable +
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 = True
ais-receive = False
yellow-receive = False
ber-receive = False
carrier-established = False
network-loopback = False

```

Dependencies: The T1-Stat profile is read only.

See Also: AIS-Receive, BER-Receive, Carrier-Established, Channel-State, Error-Count, Line-State, Loss-Of-Carrier, Loss-Of-Sync, Network-Loopback, Physical-Address, Yellow-Receive

T2-Duration

Description: Specifies the value of the transmission timeout timer in milliseconds. This timer specifies how long this endpoint must wait for an acknowledgment to a heartbeat frame.

Usage: Specify a number from 0 to 2147483647. The default is 3000 milliseconds (3 seconds).

Example: `set t2-duration = 4000`

Dependencies: The value you specify for T2-Duration must be greater than the T1 duration timer specified on the signaling gateway.

Location: SS7-Gateway > Transport-Options

See Also: ACK-Threshold, Device-ID, Heart-Beat, T1-Duration, T3-Duration, Window-Size

T3

Description: Specifies the action to take when the code image for a T3 card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- Load causes the system to load the image, even if no card of that type is installed.
- Skip causes the system to skip the image, even if a card of that type is installed.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, UDS3, UE1, Unknown-Cards, UT1

T3 (profile)

Description: A profile that contains configuration settings for a DS3 line.

Usage: Use the Read and List commands to make T3 the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the T3 profile with the index { shelf-1 slot-15 2 } the working profile and list its contents:

```
admin> read t3 {1 15 2}
T3/{ shelf-1 slot-15 2 } read
admin> list
[in T3/{ shelf-1 slot-15 2 }]
name = trunk-3
physical-address* = { shelf-1 slot-15 2 }
enabled = no
frame-type = ml3
line-length = 0-255
loopback = no-loopback
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
T3/{ shelf-1 slot-15 2 } written
```

See Also: Enabled, Frame-Type, Line-Length, Loopback, Name, Physical-Address

T302-Timer

Description: Specifies the number of milliseconds the system waits for additional called number information for an incoming call. The TAOS unit begins collecting the trailing digit information, and starts the T302 timer (the Setup Ack timer) for each call Setup message from the switch that does *not* include the Sending Complete Information Element. The TAOS unit stops the timer when it receives a message that includes the Sending Complete Information Element. The unit stops waiting for trailing digits to collect when the T302 timer stops or expires.

Usage: Specify a value from 100 to 30000 (0.10 second to 30 seconds). The default is 10000 (10 seconds).

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface, E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Overlap-Receiving, PRI-Prefix-Number, Trailing-Digits

T303-ms

Description: Specifies the timer (in milliseconds) for a response after the SETUP message is sent. The timer is stopped when a CONNECT, CALL PROCEEDING, or RELEASE COMPLETE message is received.

Usage: Specify an integer from 500 to 5000. The default value is 4000.

Example: `set t303-ms = 1000`

Location: ATM-Interface {{shelf-*N* slot-*N* *N*} *N*} > SVC-Options > Q93B-Options

See Also: Max-Restart, Max-Statenv, T308-ms, T309-ms, T310-ms, T313-ms, T316-ms, T322-ms

T308-ms

Description: Specifies the timer (in milliseconds) for a response after a RELEASE message is sent. This timer is called a *release indication timer*. The timer is started when the RELEASE message is sent and is stopped when the RELEASE or RELEASE COMPLETE message is received.

Usage: Specify an integer from 5000 to 50000. The default value is 30000.

Example: `set t308-ms = 40000`

Location: ATM-Interface {{shelf-*N* slot-*N* *N*} *N*} > SVC-Options > Q93B-Options

See Also: Max-Restart, Max-Statenv, T303-ms, T309-ms, T310-ms, T313-ms, T316-ms, T322-ms

T309-ms

Description: Specifies the timer (in milliseconds) for Q.SAAL to reconnect. After this time has elapsed, calls are dropped.

Usage: Specify an integer from 0 to 200000. The default is 0 (zero), which specifies that a default value based an ATM signaling protocol is used.

Example: `set t309-ms = 200000`

Location: ATM-Interface {{shelf-*N* slot-*N* *N*} *N*} > SVC-Options > Q93B-Options

See Also: Max-Restart, Max-Statenv, T303-ms, T308-ms, T310-ms, T313-ms, T316-ms, T322-ms

T310-ms

Description: Specifies the timer (in milliseconds) for a response after a SETUP message is received. This timer is called the *call proceeding timer*.

Usage: Specify an integer from 5000 to 50000. The default value is 10000.

Example: `set t310-ms = 5000`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > Q93B-Options

See Also: Max-Restart, Max-Statennq, T303-ms, T308-ms, T309-ms, T313-ms, T316-ms, T322-ms

T313-ms

Description: Specifies the timer (in milliseconds) for a response after a CONNECT message is sent. This timer is 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: Specify an integer from 1000 to 10000. The default value is 4000.

Example: `set t313-ms = 2000`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > Q93B-Options

See Also: Max-Restart, Max-Statennq, T303-ms, T308-ms, T309-ms, T310-ms, T316-ms, T322-ms

T316-ms

Description: Specifies the timer (in milliseconds) for a response after a RESTART message is sent. This timer is 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 = 10000`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > Q93B-Options

See Also: Max-Restart, Max-Statennq, T303-ms, T308-ms, T309-ms, T310-ms, T313-ms, T322-ms

T322-ms

Description: Specifies the timer (in milliseconds) for a response after a STATUS ENQ message is sent.

Usage: Specify an integer from 1000 to 10000. The default value is 4000.

Example: `set t322-ms = 2000`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > Q93B-Options

See Also: Max-Restart, Max-Statennq, T303-ms, T308-ms, T309-ms, T310-ms, T313-ms, T316-ms

T391-Val

Description: Sets the Link Integrity Verification polling timer (in seconds) for the time that must elapse between status requests.

Usage: Specify the number of seconds as an integer from 5 to 30. The value you enter must be less than the value of T392-Val. The default is 10, which indicates that after N391-Val status requests spaced 10 seconds apart, the UNI-DTE device requests a full status report.

Example: `set t391-val = 15`

Dependencies: If Link-Type is set to DCE, T391-Val does not apply.

Location: Frame-Relay *fr-name*

See Also: Link-Type, N391-Val, T392-Val

T392-Val

Description: Specifies the interval (in seconds) in which Status Enquiry messages must be received. The network records an error if it does not receive a Status Enquiry within T392 seconds.

Usage: Specify an integer from 5 to 30. The default is 15.

Example: `set t392-val = 20`

Dependencies: If Link-Type is set to DTE, T392-Val does not apply.

Location: Frame-Relay *fr-name*

See Also: Link-Type, T391-Val

T3-Duration

Description: Specifies the value of the persistent error timer in milliseconds. This timer specifies the maximum duration of attempts to reestablish a link before the transport layer flushes the data queues and sends an error indication.

Usage: Specify a number from 0 to 2147483647. The default is 30000 milliseconds (30 seconds).

Example: `set t3-duration = 40000`

Location: SS7-Gateway > Transport-Options

See Also: ACK-Threshold, Device-ID, Heart-Beat, T1-Duration, T2-Duration, Window-Size

T3-Stat

Description: A profile that displays information about the state of a DS3 line and its individual multiplexed DS2 lines.

Usage: Use the Read and List commands to make T3-Stat the working profile and list its contents.

Example: To make the T3-Stat profile with the index { shelf-1 slot-8 1 } the working profile and list its contents:

```
admin> read t3-stat {1 8 1}
T3-STAT/{ shelf-1 slot-8 1 } read

admin> list
[in T3-STAT/{ shelf-1 slot-8 1 }]
physical-address* = { shelf-1 slot-8 1 }
line-state = active
ds2-state = [active active active active active active active]
loss-of-signal = False
loss-of-frame = False
yellow-receive = False
ais-receive = False
```

Dependencies: The T3-Stat profile is read only.

See Also: AIS-Receive, DS2-State, Line-State, Loss-of-Frame, Loss-Of-Signal, Physical-Address, Yellow-Receive

Table-Config N

Description: A subprofile that enables you to configure entries for a local Domain Name System (DNS) table.

Usage: With DNS-Local-Table as the working profile, list the Table-Config subprofiles. To close each subprofile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the Table-Config subprofiles:

```
admin> list table-config
[in IP-GLOBAL:dns-local-table:table-config]
table-config[1] = { host1.abc.com 10.1.1.2.3 }
table-config[2] = { " " 0.0.0.0 }
table-config[3] = { " " 0.0.0.0 }
table-config[4] = { " " 0.0.0.0 }
table-config[5] = { " " 0.0.0.0 }
table-config[6] = { " " 0.0.0.0 }
table-config[7] = { " " 0.0.0.0 }
table-config[8] = { " " 0.0.0.0 }
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: IP-Global > DNS-Local-Table

See Also: Auto-Update, Enabled

Tac-Auth-Client

Description: A subprofile that defines how the TAOS unit interacts as a client of Terminal Access Controller Access Control (TACACS) authentication servers.

Usage: With External-Auth as the working profile, list the Tac-Auth-Client subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the Tac-Auth-Client subprofile:

```
admin> list tac-auth-client
[ 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
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: External-Auth

See Also: Auth-Key, Auth-Port, Auth-Server-N, Auth-Src-Port, Auth-Timeout

TACL

Description: A profile that enables you to permit Telnet access to the TAOS unit from the IP addresses listed in a Telnet Access Control List (TACL).

Usage: Use the Read and List commands to make TACL the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make TACL the working profile and list its contents:

```
admin> read tac1
TACL read

admin> list
[ in TACL ]
enable-permit = no
permit-list = { no 0.0.0.0/0 0.0.0.0 }
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
TACL written
```

See Also: Enable-Permit

TacPlus-Acct-Client

Description: A subprofile that defines how the TAOS unit interacts as a client of TACACS+ accounting servers.

Usage: With External-Auth as the working profile, list the TacPlus-Acct-Client subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the TacPlus-Acct-Client subprofile:

```
admin> list tacplus-acct-client
[in EXTERNAL-AUTH:tacplus-acct-client]
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 = " "
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: External-Auth

See Also: Acct-Key, Acct-Port, Acct-Server-N, Acct-Src-Port

TacPlus-Auth-Client

Description: A subprofile that defines how the TAOS unit interacts as a client of TACACS+ authentication servers.

Usage: With External-Auth as the working profile, list the TacPlus-Auth-Client subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the TacPlus-Auth-Client subprofile:

```
admin> list tacplus-auth-client
[in EXTERNAL-AUTH:tacplus-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 = " "
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: External-Auth

See Also: Auth-Key, Auth-Port, Auth-Server-N, Auth-Src-Port

Tag

Description: Specifies a value that links the SNMPv3-Notification profile with the Trap profile specifying the host address to which notification messages are sent.

Usage: Specify up to 255 characters. The default is null.

Example: `set tag = newtag`

Location: SNMPv3-Notification *name*

Target-Params-Name

Description: Specifies the SNMPv3-Target-Param profile for which to generate traps.

Usage: Specify up to 22 characters.

Example: `set target-params-name = profile1`

Location: Trap *name*

Target-Utilization

Description: Specifies a percentage of line utilization to use as a threshold for determining when to add or subtract bandwidth. The device adds bandwidth when average line utilization (ALU) exceeds the Target-Utilization value, and subtracts bandwidth when it falls below that value.

Usage: Specify a number from 0 to 100. The default is 70.

Example: `set target-utilization = 70`

Location: Answer-Defaults > MPP-Answer, Connection *station* > MP-Options

See Also: Add-Persistence, Bandwidth-Monitor-Direction, Base-Channel-Count, Decrement-Channel-Count, Dynamic-Algorithm, Increment-Channel-Count, Maximum-Channels, Minimum-Channels, MPP-Answer, MPP-Options, Seconds-History, Sub-Persistence

Tcc-ms

Description: Specifies the retry time (in milliseconds) for control Protocol Data Units (PDUs).

Usage: Specify a value from 0 to 3000. The default value is 1000.

Example: `set tcc-ms = 500`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options > QSAAL-Options

See Also: Max-Cc, Max-Pd, Max-Stat, Tidle-ms, Tkeepalive-ms, Tnoresponse-ms, Tpoll-ms, Window-Size

TCP

Description: Enables or disables the TCP command from the terminal-server interface.

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

- Yes enables a user to initiate a TCP session from the terminal server.
- No prevents a user from initiating a TCP session from the terminal server.

Example: `set tcp = yes`

Dependencies: If terminal services are disabled, TCP does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Ping, PPP, Rlogin, SLIP, Telnet, Terminal-Mode-Configuration, Traceroute

TCP-Clear-Answer

Description: A subprofile containing default settings for TCP-Clear connections.

Usage: With Answer-Defaults as the working profile, list the TCP-Clear-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the TCP-Clear-Answer subprofile:

```
admin> list tcp-clear-answer
[ in ANSWER-DEFAULTS:tcp-clear-answer ]
enabled = yes
detect-end-of-packet = no
end-of-packet-pattern = ""
flush-length = 256
flush-time = 20
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Detect-End-Of-Packet, Enabled, End-Of-Packet-Pattern, Flush-Length, Flush-Time

TCP-Clear-Options

Description: A subprofile with default settings for TCP-Clear connections.

Usage: With a Connection profile as the working profile, list the TCP-Clear-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the TCP-Clear-Options subprofile:

```
admin> list tcp-clear-options
[in CONNECTION/tim:tcp-clear-options]
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
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: Consider the following:

- For TCP-Clear-Options to apply, you must set Enabled to Yes in the TCP-Clear-Answer subprofile.
- TCP-Clear connections are managed on a per-VRouter basis. If a Connection profile or Remote Authentication Dial-In User Service (RADIUS) profile is associated with a VRouter and configured for TCP-Clear, the system locates the specified host only in the VRouter's routing table.

Location: Connection *station*

See Also: Detect-End-Of-Packet, End-Of-Packet-Pattern, Flush-Length, Flush-Time, Host, Host2, Host3, Host4, Port, Port2, Port3, Port4, TCP-Clear-Answer

TCP-Estab

Description: Specifies whether a filter must match only established TCP connections.

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

- Yes specifies that the filter matches only packets that are part of established TCP connections.
- No specifies that the filter can match packets that are not part of an established TCP connection.

Example: `set tcp-estab = yes`

Dependencies: TCP-Estab applies only if Protocol is set to 6 (TCP).

Location: Filter *filter-name* > Input-Filters > IP-Filter,
Filter *filter-name* > Output-Filters > IP-Filter

See Also: Input-Filters, IP-Filter, Output-Filters, Protocol

TCP-Timeout

Description: Specifies a timeout period for TCP connection attempts that use the DNS-List-Attempt feature.

Usage: Specify an integer indicating the number of seconds for a TCP timeout. Valid values range from 0 to 200 seconds. At the default value of 0 (zero), the system attempts a fixed number of retries at escalating intervals, adding up to about 170 seconds total. (Other limits in the system terminate TCP retries after about 170 seconds, even if the value is set to a higher number.) If you set TCP-Timeout to a nonzero value, the value is the number of seconds TCP retries persist. After the specified number of seconds, the retries stop and the connection is considered lost.

Example: `set tcp-timeout = 30`

Location: IP-Global

See Also: DNS-List-Attempt, DNS-List-Size

Telco-Options

Description: A subprofile that enables you to set telephone-company options for a connection.

Usage: With a Connection profile as the working profile, list the Telco-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Telco-Options subprofile:

```
admin> list telco-options
[in CONNECTION/tim:telco-options]
answer-originate = ans-and-orig
call-type = nailed-mode-off
nailed-groups = 1
ft1-caller = no
force-56kbps = no
data-service = 56k-restricted
call-by-call = 0
billing-number = " "
transit-number = " "
dialout-allowed = no
nas-port-type = any
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: Answer-Originate, Billing-Number, Call-By-Call, Call-Type, Data-Service, Dialout-Allowed, Force-56Kbps, FT1-Caller, Nailed-Groups, NAS-Port-Type, Transit-Number

Telnet

Description: Enables or disables the Telnet command from the terminal-server interface.

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

- Yes specifies that operators can invoke Telnet sessions from the terminal-server interface.
- No disables the use of Telnet in the terminal server.

Example: `set telnet = yes`

Dependencies: If terminal services are disabled, Telnet does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration > Telnet-Options

See Also: Ping, PPP, Rlogin, SLIP, TCP, Telnet-Options, Terminal-Mode-Configuration, Traceroute

Telnet-Host-Auth

Description: Determines whether immediate Telnet sessions require local authentication or authentication only by the Telnet host.

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

- Yes specifies that the session requires authentication only by the Telnet host.
- No specifies that the session must be locally authenticated before undergoing authentication by the Telnet host.

Example: `set telnet-host-auth = yes`

Dependencies: If terminal services are disabled, Telnet-Host-Auth does not apply.

Location: Terminal-Server > Immediate-Mode-Options

See Also: Immediate-Mode-Options, Telnet

Telnet-Mode

Description: Specifies the default Telnet mode.

Usage: Specify one of the following values:

- ASCII (the default) specifies standard 7-bit mode. In 7-bit mode, bit 8 is set to 0 (zero).
- Binary specifies that the TAOS 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.
- Transparent specifies that you can send and receive binary files without having to be in Binary mode. You can run the same file transfer protocols that Binary mode makes available.

Example: `set telnet-mode = ascii`

Dependencies: Consider the following:

- In 8-bit binary mode, the Telnet escape sequence does not operate. The Telnet session can close only if one end of the connection quits the session. If you are a local user not connected through a digital modem, the remote-end user must quit.
- A user can override the Binary setting on the Telnet command line.
- If terminal services are disabled, Telnet-Mode does not apply.
- Not all devices support the Binary mode option. Some devices partially follow the Telnet RFC, but do not enforce the Telnet restriction of using only 7-bit ASCII. They accept 8-bit data and, after doing the appropriate processing, forward all data received. If you specify Transparent for these devices, you can escape the IAC character and add a null after every CR to cause the devices to work.

Location: Terminal-Server > Terminal-Mode-Configuration > Telnet-Options

See Also: Telnet, Telnet-Options, Terminal-Mode-Configuration

Telnet-Options

Description: A subprofile that contains terminal-server configuration options for interactive users.

Usage: With Terminal-Server as the working profile, list the Terminal-Mode-Configuration subprofile's Telnet-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Telnet-Options subprofile:

```
admin> list terminal-server terminal-mode-configuration telnet-options
[in TERMINAL-SERVER:terminal-mode-configuration:telnet-options]
telnet = no
telnet-mode = ascii
auto-telnet = no
local-echo = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server

See Also: Auto-Telnet, Local-Echo, Telnet, Telnet-Mode

Telnet-Password

Description: Specifies the password that users must enter to access the TAOS unit by means of Telnet. If you specify a password, a user is allowed three tries of 60 seconds each to enter the correct password.

Usage: Specify a password of up to 20 characters. The default is null. If you accept the default, the TAOS unit does not prompt a user for a password.

Example: `set telnet-password = unit0`

Location: IP-Global

See Also: Auto-Telnet, Telnet, Telnet-Host-Auth

Temporary-Route

Description: Specifies that the TAOS unit adds the route to the routing table only when the link is up. Temporary-Route is especially useful for nailed-up IP-routing connections.

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

- Yes excludes a route from the routing table when its connection is down.
- No includes the route in the routing table even if its connection is down.

Example: `set temporary-route = no`

Location: Connection *station* > IP-Options

See Also: IP-Options, IP-Routing-Enabled, Private-Route, RIP

Terminal-Mode-Configuration

Description: A subprofile containing terminal-server configuration options for interactive users.

Usage: With Terminal-Server as the working profile, list the Terminal-Mode-Configuration subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the Terminal-Mode-Configuration subprofile:

```
admin> list terminal-mode-configuration
[in TERMINAL-SERVER:terminal-mode-configuration]
silent-mode = no
clear-screen = yes
system-password = ""
banner = "*** Lucent Terminal Server ***"
login-prompt = "Login: "
password-prompt = "Password: "
third-login-prompt = ""
third-prompt-sequence = last
prompt = "lucent% "
terminal-type = vt100
```

```
clear-call = no
buffer-chars = yes
ping = no
traceroute = no
tcp = no
telnet-options = { no ascii no no }
ip-add-msg = "IP address is "
prompt-format = no
login-timeout = 300
rlogin-options = { no 1023 128 }
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: Terminal-Server

See Also: Banner, Buffer-Chars, Clear-Call, Clear-Screen, IP-Add-Msg, Login-Prompt, Password-Prompt, Ping, Prompt, Prompt-Format, Rlogin-Options, Silent-Mode, System-Password, TCP, Telnet-Options, Terminal-Type, Third-Login-Prompt, Traceroute

Terminal-Server

Description: A profile that enables you to configure terminal-server features.

Usage: Use the Read and List commands to make Terminal-Server the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make Terminal-Server the working profile and list its contents:

```
admin> read terminal-server
TERMINAL-SERVER read

admin> list
[in TERMINAL-SERVER]
enabled = no
security-mode = none
modem-configuration = { will-v42 33600-max-baud +
terminal-mode-configuration = { no yes "" +
immediate-mode-options = { none no "" 0 }
menu-mode-options = { no no no "" 0.0.0.0 "" 0.0.0.0 "" 0.0.0.0+
ppp-mode-configuration = { no 5 no session-ppp }
slip-mode-configuration = { no no }
dialout-configuration = { no no 5000 }
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
TERMINAL-SERVER written
```

See Also: Dialout-Configuration, Enabled, Immediate-Mode-Options, Menu-Mode-Options, Modem-Configuration, PPP-Mode-Configuration, Security-Mode, SLIP-Mode-Configuration, Terminal-Mode-Configuration

Terminal-Type

Description: Specifies the default terminal type for Telnet and Rlogin sessions.

Usage: Specify a terminal type. You can enter up to 15 characters. The default is `vt100`.

Example: `set terminal-type = vt100`

Dependencies: If terminal services are disabled, Terminal-Type does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Terminal-Mode-Configuration

Term-Rate

Description: Specifies the bit rate of a serial port. When you modify the bit rate of a serial port, you might also need to change the data-rate setting of the terminal accessing that port.

Usage: Specify one of the following values (in bits per second):

57600
38400
19200
9600 (the default)
4800
2400

Example: `set term-rate = 9600`

Location: Serial {shelf-*N* slot-*N* *N*}

See Also: Auto-Logout, Flow-Control, Physical-Address, User-Profile

Text-*N*

Description: Specifies text that the TAOS unit displays in the terminal-server menu for the Telnet host specified by Host-*N*.

Usage: Specify a text string describing the corresponding Telnet host. The default is null.

Example: `set text-1 = database-server`

Dependencies: When terminal services are disabled, Text-*N* does not apply. In addition, Text-*N* is ignored if Remote-Configuration is set to Yes.

Location: Terminal-Server > Menu-Mode-Options

See Also: Menu-Mode-Options, Remote-Configuration

TFTP-Host-Name

Description: Specifies the symbolic hostname of a TFTP server that holds the full configuration file for the client.

Usage: Specify a symbolic hostname. The default is null.

Example: `set tftp-host-name = sanfran`

Dependencies: Because the TFTP-Host-Name value must be a hostname, the TAOS unit must be configured to access a Domain Name System (DNS) server for address resolution.

Location: IP-Global > DHCP-Server

See Also: Active, Boot-File-Path, Default-Lease-Duration, Default-Max-Lease, Default-Pool, Lease-Duration, Server-Address, Static-Address

Thermal

Description: A profile that enables you to control fantray operations.

Usage: Use the Read and List commands to make Thermal the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make Thermal the working profile and list its contents:

```
admin> read thermal
THERMAL read

admin> list
[in THERMAL]
fantray-lownoise-rpm = 2500
operation-mode = full-speed-only
low-temperature-trigger = 34
high-temperature-trigger = 40
alarm-temperature-trigger = 55
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
THERMAL written
```

See Also: Alarm-Temperature-Trigger, Fantray-Lownoise-RPM, High-Temperature-Trigger, Low-Temperature-Trigger, Operation-Mode

Third-Data-Forward-Character

Description: Specifies the hexadecimal value of the third character to be used as a trigger to forward data.

Usage: Specify a hexadecimal value. The default is 15.

Example: `set third-data-forward-character = 16`

Location: Connection *station* > Visa2-Options

See Also: First-Data-Forward-Character, Fourth-Data-Forward-Character, Second-Data-Forward-Character

Third-Login-Prompt

Description: Specifies an optional third prompt for a terminal-server login. When a user logs into the terminal server, he or she supplies a username and password. The Third-Login-Prompt setting enables the TAOS unit to get additional information from the user. The unit does not use the information, but passes it to the Remote Authentication Dial-In User Service (RADIUS) server. The user can enter up to 80 characters.

Usage: Specify up to 20 characters. The default is null, which specifies that no third prompt appears.

Example: `set third-login-prompt = ID Number>>`

If Third-Prompt-Sequence is set to First, the terminal server displays the third prompt before the login and password prompts:

```
ID Number>>
Login:
Password:
```

If Third-Prompt-Sequence is set to Last, the terminal server displays the third prompt after the login and password prompts:

```
Login:
Password:
ID Number>>
```

Dependencies: Consider the following:

- If authentication does not occur through the RADIUS server, the terminal server does not display the third prompt.
- If terminal services are disabled, or if Auth-Type is set to a value other than RADIUS, Third-Login-Prompt does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Auth-Type, Login-Prompt, Password-Prompt, Prompt, Prompt-Format, Terminal-Mode-Configuration, Third-Prompt-Sequence

Third-Party

Description: Enables or disables Open Shortest Path First (OSPF) third-party routing for a static route. When Third-Party is set to Yes, the Gateway-Address value is the third-party router for the route.

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

- Yes enables third-party routing for the OSPF router.
- No disables third-party routing for the OSPF router.

Example: `set third-party = yes`

Location: IP-Route *name*

See Also: Gateway-Address

Third-Prompt-Sequence

Description: Specifies whether the Third-Login-Prompt should appear before or after the Login-Prompt and Password-Prompt in the login sequence.

Usage: Specify First or Last. The default is Last.

Example: `set third-prompt-sequence = first`

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Login-Prompt, Password-Prompt, Prompt, Prompt-Format, Terminal-Mode-Configuration, Third-Login-Prompt

Throttle-No-Port-Match-UDP-Traffic-On-Slot

Description: Enables or disables reception of UDP packets for UDP ports currently unknown to the TAOS unit.

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

- Yes disables reception of UDP packets for UDP ports currently unknown to the TAOS unit. The system discards UDP packets until the UDP port is known. The setting of Yes is recommended for MultiVoice gateways, to prevent overloading of the shelf controller when both gateways do not complete the Voice over IP (VoIP) call setup at the same time.
- No enables reception of UDP packets for UDP ports currently unknown to the TAOS unit. The system sends the unknown port packets to the shelf controller for processing.

Example: `set throttle-no-port-match-udp-traffic-on-slot = yes`

Location: IP-Global

See Also: Send-ICMP-Dest-Unreachable

Ticks

Description: Specifies the distance to the destination network, in IBM PC clock ticks (one-eighteenth of a second). The Ticks setting is for round-trip timer calculation and for determining the nearest server of a given type.

Usage: Enter an integer. The default is 12.

Example: `set ticks = 6`

Location: IPX-Route *name*

See Also: Active-Route, Dest-Network, Hops, Name, Profile-Name, Server-Node, Server-Socket, Server-Type

Tidle-ms

Description: Specifies the polling interval (in milliseconds) for when the connection is idle.

Usage: Specify a value from 1000 to 20000. The default value is 15000.

Example: `set tidle-ms = 2000`

Dependencies: Tidle-ms applies only to the Asynchronous Transfer Mode (ATM) UNI 3.1 signaling protocol.

Location: ATM-Interface { {shelf-*N* slot-*N N*} *N* } > SVC-Options > QSAAL-Options

See Also: Max-Cc, Max-Pd, Max-Stat, Tcc-ms, Tkeepalive-ms, Tnoresponse-ms, Tpoll-ms, Window-Size

Time

Description: A subprofile that specifies the current hour, minute, and second.

Usage: With Timedate as the working profile, list the Time subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Time subprofile:

```
admin> list time
[in TIMEOUT/time]
hour = 12
minute = 37
second = 33
```

You can then use the Set command to modify the settings in the subprofile.

```
admin> set hour = 16
```

As an alternative, you can simply use the Set command:

```
admin> set time hour = 16
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: You can also use the Date command to set the current hour, minute, and second.

Location: Timedate

See Also: Date

Timedate

Description: A profile that shows the current system time and date.

Usage: Use the Read and List commands to make Timedate the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make Timedate the working profile and list its contents:

```
admin> read timedate
TIMEDATE read

admin> list
[in TIMEDATE]
time = { 12 37 33 }
date = { Friday October 18 1996 }
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
TIMEDATE written
```

See Also: Date, Time

Tkeepalive-ms

Description: Specifies the poll interval (in milliseconds) when the interface is in a transient state.

Usage: Specify a value from 0 to 3000. The default is 0 (zero), which specifies that a default value based on an ATM signaling protocol is used.

Example: `set tkeepalive-ms = 1000`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options > QSAAL-Options

See Also: Max-Cc, Max-Pd, Max-Stat, Tcc-ms, Tidle-ms, Tnoresponse-ms, Tpoll-ms, Window-Size

Tnresponse-ms

Description: Specifies the maximum interval (in milliseconds) between receipt of STAT PDUs.

Usage: Specify a value from 0 to 20000. The default is 0 (zero), which specifies that a default value based an ATM signaling protocol is used.

Example: `set tnresponse-ms = 500`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } > SVC-Options > QSAAL-Options

See Also: Max-Cc, Max-Pd, Max-Stat, Tcc-ms, Tidle-ms, Tkeepalive-ms, Tpoll-ms, Window-Size

Toggle-Screen

Description: Specifies whether an interactive user can switch between terminal-server menu mode and command mode.

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

- Yes specifies that terminal-server users can switch between command mode and menu mode.
- No specifies that users have access only to the screen that you configure to come up when a user logs in.

Example: `set toggle-screen = no`

Dependencies: If terminal services are disabled, Toggle-Screen does not apply.

Location: Terminal-Server > Menu-Mode-Options

See Also: Menu-Mode-Options, Start-With-Menus

T-Online

Note: This setting is for a customer-specific application. It is not intended for general use.

Description: Specifies whether the TAOS unit routes calls to a T-Online server. PRI-to-PRI switching for T-Online provides a network-side implementation of NET-5 to support switching calls from the Deutsche Telekom public network to a T-Online server. If T-Online is enabled, the unit compares the telephone number and subaddress number it obtains from the call Setup and Info messages to the Dirdo information stored in Remote Authentication Dial-In User Service (RADIUS). It switches the inbound call to the T-Online server if it finds any of the following matches in RADIUS:

- The telephone number and subaddress of the incoming call match a telephone number and subaddress entry in RADIUS.
- The telephone number matches a telephone number entry in RADIUS and there is no subaddress.
- The subaddress matches a subaddress entry in RADIUS and there is no telephone number.
- There is no incoming telephone number or subaddress.

The TAOS unit begins collecting the subaddress information, and for each call Setup message from the switch that does *not* include “Sending Complete Information Element,” it starts the T302 timer (the Setup Ack timer). The unit stops the timer when it receives a message that includes “Sending Complete Information Element.” The TAOS unit assumes there are no more subaddress digits to collect when the T302 timer stops or expires.

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

- Yes specifies that calls are switched from the public network to T-Online on the basis of a user-defined match.
- No specifies that T-Online switching is disabled.

Example: `set t-online = yes`

Location: System

See Also: T302-Timer, T-Online-Most-Avail-Chan, T-Online-Offset, T-Online-Type

T-Online-Most-Avail-Chan

Note: This setting is for a customer-specific application. It is not intended for general use.

Description: Specifies which link to choose for redirecting a call to a T-Online server.

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

- Yes specifies that the TAOS unit chooses the link with the most available channels.
- No specifies that the TAOS unit chooses the link according to a round-robin method.

Example: `set t-online-most-avail-chan = yes`

Dependencies: Consider the following:

- T-Online-Most-Avail-Chan does not apply if T-Online is set to No.
- Trunk group 8 is reserved for DTPT calls when T-Online is set to Yes.

Location: System

See Also: T302-Timer, T-Online, T-Online-Offset, T-Online-Type

T-Online-Offset

Note: This setting is for a customer-specific application. It is not intended for general use.

Description: Specifies the offset to the TE line number.

The offset you specify is used to form the TE-NT pair of E1 PRI lines. PRI-to-PRI switching requires two E1 PRI lines. A call is received on one line (the TE line, which communicates with the carrier switch) and internally switched to another (the NT line, which communicates with the ZGR server). The TAOS unit determines which line to use for the NT line by applying the offset to the TE line number.

Usage: Specify an integer from 1 to 4.

Example: If T-Online-Offset is set to 1 and the TAOS unit receives a call on E1 PRI line 5, the NT line is line 6.

Dependencies: If T-Online is set to No, T-Online-Offset does not apply.

Location: System

See Also: T302-Timer, T-Online, T-Online-Most-Avail-Chan, T-Online-Type

T-Online-Type

Note: This setting is for a customer-specific application. It is not intended for general use.

Description: Specifies the E1 PRI line's function for T-Online PRI-to-PRI switching.

Usage: Specify one of the following values:

- None (the default) specifies that no PRI-to-PRI switching takes place.
- TE specifies that the line communicates with the carrier switch.
- NT specifies that the line communicates with the ZGR server.

Example: `set t-online-type = TE`

Dependencies: Consider the following:

- If T-Online is set to No, T-Online-Type does not apply.
- One TE-configured line can switch calls to one or more NT-configured lines.

Location: E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: T302-Timer, T-Online, T-Online-Most-Avail-Chan, T-Online-Offset

Top-Status

Description: Specifies the default content of the upper-right portion of the status window.

Usage: Specify one of the following values:

- General-Info (the default) specifies that the TAOS unit displays general information and statistics for the system.
- Log-Window specifies that the TAOS unit displays saved system-event log entries.
- Line-Status specifies that the TAOS unit displays the status of system telephony interfaces.

Example: `set top-status = general-info`

Location: User *name*

See Also: User (profile)

TOS-Filter

Description: Specifies the name of a Filter profile that defines a Type-of-Service (TOS) filter.

Usage: Specify the name of a defined profile. The default is null.

Example: `set tos-filter = my-tos-filter`

Location: Connection *station* > IP-Options

See Also: TOS-Filter (subprofile), TOS-Options

TOS-Filter (subprofile)

Description: A subprofile containing a TOS filter specification. A Filter profile contains several levels of subprofiles. A TOS-Filter subprofile is in an Input-Filters *N* or Output-Filters *N* subprofile.

Usage: With a Filter profile as the working profile, list an TOS-Filter subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the TOS-Filter subprofile:

```
admin> list input-filters 1 tos-filter
[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
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: Filter *filter-name* > Input-Filters > Input-Filters *N*,
Filter *filter-name* > Output-Filters > Output-Filters *N*

See Also: Dest-Address, Dest-Address-Mask, Dest-Port, Dst-Port-Cmp, Input-Filters *N*, Output-Filters *N*, Precedence, Protocol, Source-Address, Source-Address-Mask, Source-Port, Src-Port-Cmp, Type-of-Service

TOS-Options

Description: A subprofile that enables you to configure Type-of-Service (TOS) settings.

Usage: With a Connection or VoIP profile as the working profile, list the TOS-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the TOS-Options subprofile:

```
admin> list ip-options tos-options
[in CONNECTION/"":ip-options:tos-options]
active = no
precedence = 000
type-of-service = normal
apply-to = input
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station* > IP-Options, VoIP {*x y*}

See Also: Active, Apply-To, Precedence, Type-of-Service

Total-Count

Description: 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

See Also: Device-Class, Disabled-Count, Operational-Count

Tpoll-ms

Description: Specifies the poll interval (in milliseconds) when the connection is active.

Usage: Specify a value from 0 to 3000. The default is 0 (zero), which specifies that a default value based on an ATM signaling protocol is used.

Example: `set tpoll-ms = 500`

Location: ATM-Interface { {shelf-*N* slot-*N* } *N* } > SVC-Options > QSAAL-Options

See Also: Max-Cc, Max-Pd, Max-Stat, Tcc-ms, Tidle-ms, Tkeepalive-ms, Tnoresponse-ms, Window-Size

Description: Enables or disables the use of the Traceroute command in the terminal-server interface.

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

- Yes specifies that terminal-server users can use the Traceroute command.
- No disables the Traceroute command.

Example: `set traceroute = yes`

Dependencies: If terminal services are disabled, Traceroute does not apply.

Location: Terminal-Server > Terminal-Mode-Configuration

See Also: Ping, PPP, Rlogin, SLIP, TCP, Telnet, Telnet-Options, Terminal-Mode-Configuration

Traffic-Shaper

Description: Specifies the traffic shaper assigned to the Virtual Circuit (VC).

Usage: Specify a number from 1 to 15. The default is 16, which specifies a nonconfigurable internal shaper. Traffic shaper 16 specifies no bandwidth limitation.

Example: `set traffic-shaper = 1`

Location: Connection *station* > Session-Options

See Also: Traffic-Shapers, Traffic-Shapers N

Traffic-Shapers

Description: A subprofile that contains a series of traffic-shaper subprofiles, one for each different type of Asynchronous Transfer Mode (ATM) traffic.

Usage: With a DS3-ATM, E3-ATM, or OC3-ATM profile as the working profile, enter `list line-config traffic-shapers`. To return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Traffic-Shapers subprofile:

```
admin> list line-config traffic-shapers
[in DS3-ATM/{ any-shelf any-slot 0
}:line-config:traffic-shapers]
traffic-shapers[1] = { no 1000 1000 2 no 0 }
traffic-shapers[2] = { no 1000 1000 2 no 1 }
traffic-shapers[3] = { no 1000 1000 2 no 2 }
traffic-shapers[4] = { no 1000 1000 2 no 3 }
traffic-shapers[5] = { no 1000 1000 2 no 4 }
traffic-shapers[6] = { no 1000 1000 2 no 5 }
traffic-shapers[7] = { no 1000 1000 2 no 6 }
traffic-shapers[8] = { no 1000 1000 2 no 7 }
traffic-shapers[9] = { no 1000 1000 2 no 8 }
```



```
traffic-shapers[10] = { no 1000 1000 2 no 9 }  
traffic-shapers[11] = { no 1000 1000 2 no 10 }  
traffic-shapers[12] = { no 1000 1000 2 no 11 }  
traffic-shapers[13] = { no 1000 1000 2 no 12 }  
traffic-shapers[14] = { no 1000 1000 2 no 13 }  
traffic-shapers[15] = { no 1000 1000 2 no 14 }
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: DS3-ATM {shelf-*N* slot-*N N*} > Line-Config,
E3-ATM {shelf-*N* slot-*N N*} > Line-Config,
OC3-ATM {shelf-*N* slot-*N N*} > Line-Config

See Also: Traffic-Shapers N

Traffic-Shapers *N*

Description: A subprofile that enables you to define the characteristics for different types of data traffic on an Asynchronous Transfer Mode (ATM) interface.

Usage: With a DS3-ATM, E3-ATM, or OC3-ATM profile as the working profile, use the List command to display the configuration for one of the traffic-shaper subprofiles. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Traffic-Shapers[1] subprofile:

```
admin> list line-config traffic-shapers 1  
[in DS3-ATM/{any-shelf any-slot 0}:line-config:traffic-shaper+]  
enabled = no  
bit-rate = 1000  
peak-rate = 1000  
max-burst-size = 2  
aggregate = no  
priority = 0
```

To close the subprofile and return to a higher context in the working profile:

```
admin> list ..
```

Location: DS3-ATM {shelf-*N* slot-*N N*} > Line-Config > Traffic-Shapers,
E3-ATM {shelf-*N* slot-*N N*} > Line-Config > Traffic-Shapers,
OC3-ATM {shelf-*N* slot-*N N*} > Line-Config > Traffic-Shapers

See Also: Aggregate, Bit-Rate, Enabled, Max-Burst-Size, Peak-Rate, Priority

Trailing-Digits

Description: Specifies the number of digits required to follow the prefix number for the TAOS unit to consider the called number complete. Callers can indicate Sending Complete by a method such as dialing the pound-sign (#). If a caller does not indicate Sending Complete and the TAOS unit cannot determine whether the called number was complete, the unit waits until the T302 timer expires, even if the caller has dialed all the required digits. The Trailing-Digits setting enables the unit to reset the timer when the specified number of digits has been received.

Usage: Specify a value from 1 to 6. The default value is 2.

Example: `set trailing-digits = 1`

Dependencies: If Overlap-Receiving is set to No, the PRI-Prefix-Number, Trailing-Digits, and T302-Timer settings do not apply.

Location: T1 {shelf-*N* slot-*N* *N*} > Line-Interface, E1 {shelf-*N* slot-*N* *N*} > Line-Interface

See Also: Overlap-Receiving, PRI-Prefix-Number, T302-Timer

Transaction-Server

Description: A profile that enables you to specify values for the metrics used in the server selection table.

Usage: Use the Read and List commands to make Transaction-Server the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Transaction-Server profile the working profile and list its contents:

```
admin> read transaction-server
TRANSACTION-SERVER read

admin> list
[in TRANSACTION-SERVER]
enabled = yes
hunting-mechanism = cyclic
selection-timeout = 10000
data-ack-timeout = 10000
keep-alive-timeout = 30
qtp-port = 3350
metric-max = 15
no-conn-ack-increment = 8
call-reject-increment = 4
call-ack-decrement = 1
available-metric = 1
partly-congested-metric = 4
congested-metric = 10
shutdown-metric = 14
no-first-status-metric = 10
no-second-status-metric = 16
max-qtp-pdu-size = 512
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write  
TRANSACTION-SERVER written
```

See Also: Available-Metric, Call-Ack-Decrement, Call-Reject-Increment, Congested-Metric, Data-Ack-Timeout, Enabled, Hunting-Mechanism, Keep-Alive-Timeout, Max-QTP-PDU-Size, Metric-Max, No-Conn-Ack-Increment, No-First-Status-Metric, No-Second-Status-Metric, Partly-Congested-Metric, QTP-Port, Selection-Timeout, Shutdown-Metric

Transfer-to-Operator

Description: Specifies the dial string a caller enters when requesting operator assistance.

Usage: Specify up to five digits, with an asterisk (*) in either the first or second position. You can specify the asterisk (*) and then any numbers from 0 through 9. The default is *0. To disable operator assistance, specify the null value.

Example: `set transfer-to-operator = *9`

Dependencies: Consider the following:

- A MultiVoice gateway must have Single-Dial-Enable set to No.
- In one of the ingress translation tables used by MultiVoice Access Manager (MVAM), you must define a translation rule that contains the actual dialed number used to connect calls to operator assistance.

Location: VoIP { *x y* }

See Also: Single-Dial-Enable

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 should take into account transmission and propagation delays. The default is 1.

Example: `set transit-delay = 5`

Location: IP-Interface { {shelf-*N* slot-*N* *N*} *N*} > OSPF,
Connection *station* > IP-Options > OSPF-Options

See Also: IP-Options, OSPF, OSPF-Options, Retransmit-Interval

Transit-Number

Description: Specifies an Interexchange Carrier (IEC) for long-distance PRI calls.

Usage: Specify one of the following dialing prefixes:

288 (AT&T)

222 (MCI)

333 (Sprint)

The default is null. If you accept the default, the TAOS unit uses any available IEC for long-distance calls.

Example: `set transit-number = 222`

Dependencies: If a nailed-up Frame-Relay datalink connection is in use, Transit-Number does not apply.

Location: Connection *station* > Telco-Options, Frame-Relay *fr-name*

See Also: Telco-Options

Transport-Options

Description: A subprofile that contains settings for changing the operation of SSL DDL timers.

At times, you might need to change the duration of various Signaling System 7 (SS7) DDL timers to fine-tune a signaling link. For example, you might want to change timeouts when integrating a TAOS unit with existing signaling gateways. The values in the Transport-Options subprofile are used to set time intervals for waiting and responding to the various signaling link processes.

Usage: With SS7-Gateway as the working profile, list the Transport-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Transport-Options subprofile:

```
admin> list transport-options
[ in SS7-GATEWAY:transport-options ]
device-id = 0
t1-duration = 1000
t2-duration = 3000
t3-duration = 30000
window-size = 7
ack-threshold = 6
heart-beat = nos
type = ascend
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: SS7-Gateway

See Also: ACK-Threshold, Device-ID, Heart-Beat, T1-Duration, T2-Duration, T3-Duration, Type, Window-Size

Trap

Description: A profile containing settings that determine how the TAOS 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 TAOS unit sends a traps Protocol Data Unit (PDU) to the SNMP manager.

Usage: Use the Read and List commands to make Trap the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Trap profile host-231 the working profile and list its contents:

```
admin> read trap host-231
TRAP/host-231 read

admin> list
[in TRAP/host-231]
host-name* = host-231
community-name = unit0
host-address = 10.2.3.4/24
alarm-enabled = yes
security-enabled = yes
port-enabled = no
slot-enabled = yes
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
dirdo-enabled = yes
slot-profile-change-enabled = yes
power-supply-enabled = yes
authentication-enabled = yes
call-log-dropped-pkt-enabled = yes
config-change-enabled = yes
suspect-access-resource-enabled = no
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
megaco-link-status-enabled = no
call-log-serv-change-enabled = no
voip-gk-change-enabled = no
wan-line-state-change-enabled = no
active-enabled = yes
host-port = 162
inform-time-out =
inform-retry-count =
notify-tag-list = default
target-params-name = default
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
TRAP/host-231 written
```

See Also: Host-Address, Host-Name, Host-Port

True-Connect-Enable

Description: Enables or disables true-connect signaling for Voice over IP (VoIP) calls.

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

- Yes enables delay of PSTN alerting and connect messages in order to match the equivalent H.323 alerting and connect messages. If you specify Yes, an alerting message is sent to the ingress PSTN switch only when an H.323 alerting message is received on the ingress VoIP gateway. Similarly, a PSTN connect message is sent only when the H.323 VoIP call has been answered. This setting ensures that no charges are incurred for incomplete calls. The setting takes effect with the next incoming call. It has no effect on outgoing calls.
- No disables delay of PSTN alerting and connect messages. If you specify No, an alerting message is sent to the ingress PSTN switch as soon as the connection is established with the ingress MultiVoice gateway. This setting results in the caller incurring a PSTN charge at the time of connection to the local gateway, before the called party has received and answered the call from the far-end gateway.

Example: `set true-connect-enable = yes`

Dependencies: Consider the following:

- You must set Default-Call-Type to VoIP for T1 or E1 trunks used for incoming VoIP calls that require true-connect signaling. Setting Default-Call-Type to VoIP causes *all* calls received on the trunk to be mapped to VoIP.
- With ISDN trunks, Lucent recommends that you set the T310 timeout on the telco switch or PBX to 30 seconds or greater when using the true-connect feature. The T310 timeout includes the time that the called party's telephone is ringing, so a 10-second timeout can cause the near-end gateway to terminate the call too soon.
- When the true-connect feature is enabled and a VoIP call fails before the PSTN call is fully connected, the gateway is still able to send an appropriate tone or voice announcement to the caller.

Location: VoIP {*x y*}

See Also: Cut-Thru-Enable-Nearend, Default-Call-Type

Trunk-Group

Description: Specifies a trunk-group number.

- In a T1, E1, E3-ATM, DS3-ATM, OC3-ATM, or SWAN profile, Trunk-Group assigns a channel to a trunk group.
- In a Call-Route profile, Trunk-Group indicates a trunk group whose incoming calls are routed to the address in the index field.

Usage: Specify a trunk-group number from 2 to 9. In a T1, E1, E3-ATM, DS3-ATM, or SWAN profile, the default is 9. In a Call-Route or OC3-ATM profile, the default is 0 (zero), which matches any trunk-group number.

Example: `set trunk-group = 4`

Dependencies: Use-Trunk-Groups must be set to Yes for Trunk-Group to have an effect.

Location: Call-Route { { {shelf-*N* slot-*N* *N*} *N*} *N*},
DS3-ATM {shelf-*N* slot-*N* *N*} > Line Config,
E1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line Config,
SWAN {shelf-*N* slot-*N* *N*} > Line-Config,
T1 {shelf-*N* slot-*N* *N*} > Line-Interface > Channel-Config *N*

See Also: Call-Route, Channel-Config *N*, Line-Config, Num-Digits-Trunk-Groups, Use-Trunk-Groups

Trunk-Group-Callback-Control

Description: Specifies the trunk group number that the unit prepends to the number supplied by the user for CBCP Callback.

Usage: Enter an integer. The default is null.

Example: `trunk-group-callback-control = 9`

Location: Connection *station* > PPP-Options

See Also: CBCP-Enabled, Mode-Callback-Control

Trunk-Prefix-Enable

Description: Specifies a trunk group for connecting Voice over IP (VoIP) calls to the called end point on an egress MultiVoice gateway.

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

- Yes causes an egress MultiVoice gateway to use a preselected trunk group, assigned by either the ingress MultiVoice gateway or the MultiVoice Access Manager (MVAM) device, to route outgoing calls to the PSTN.
- No specifies that the egress MultiVoice gateway selects trunk groups for outgoing calls.

Example: `set trunk-prefix-enable = yes`

Dependencies: Consider the following:

- Trunk groups must be enabled on the egress MultiVoice gateway.
- The size of the trunk groups must be defined on all egress MultiVoice gateways.
- Trunk group numbers must be assigned for egress T1 trunks.

Location: VoIP {*x y*}

See Also: Trunk-Quiesce-Enable

Trunk-Quiesce-Enable

Description: Enables or disables deactivation of a T1 PRI line when a gateway is unavailable.

The trunk deactivation feature enables MultiVoice gateways to automatically deactivate trunks used for Voice over IP (VoIP) calls when a gateway becomes unavailable. This feature enables gatekeepers in the MultiVoice network to route calls to other available MultiVoice gateways, to use network resources more efficiently, and to improve service quality for users.

Trunk deactivation prevents the Public Switched Telephone Network (PSTN) switch from routing subsequent calls to the trunks configured for VoIP. Current calls remain active until those calls are terminated by the caller or PSTN. When trunk deactivation is enabled, trunks configured to accept VoIP calls are made unavailable to the PSTN under the following conditions:

- A MultiVoice gateway cannot register with either a primary or secondary gatekeeper.
- A MultiVoice gateway's trunk connection with the PSTN is unavailable, forcing the MultiVoice gateway to unregister itself from its gatekeepers.

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

- Yes enables deactivation of a T1 PRI line when a MultiVoice gateway is unavailable.
- No disables deactivation of a T1 PRI line when a MultiVoice gateway is unavailable.

Example: `set trunk-quiesce-enable = yes`

Dependencies: Only T1 trunks that use ISDN PRI signaling and have been configured for VoIP can be deactivated systemwide by the Trunk-Quiesce-Enable setting.

Location: VoIP {x y}

See Also: Trunk-Prefix-Enable

TS-Idle-Mode

Description: Specifies when the TAOS unit is to reset the terminal-server idle-session timer.

Usage: Specify one of the following values:

- No-Idle (the default) disables the idle timer.
- Input-Only-Idle specifies that the TAOS unit resets the timer when an input character is received.
- Input-Output-Idle specifies that the TAOS unit resets the timer when either input or output characters are processed.

Example: `set ts-idle-mode = input-only-idle`

Location: Answer-Defaults > Session-Info, Connection *station* > Session-Options

See Also: Session-Info, Session-Options, TS-Idle-Timer

TS-Idle-Timer

Description: Specifies the number of seconds a terminal-server session can remain idle before being terminated.

Usage: Specify a number from 0 to 65535. The default is 120.

Example: `set ts-idle-timer = 360`

Dependencies: The TS-Idle-Timer setting has no effect if TS-Idle-Mode is set to No-Idle.

Location: Answer-Defaults > Session-Info, Connection *station* > Session-Options

See Also: Session-Info, Session-Options, TS-Idle-Mode

Tunnel-Address

Description: Specifies the IP address of the far-end IP Security (IPSec) endpoint.

Usage: Specify an IP address in dotted decimal notation. For a Layer 2 Tunneling Protocol (L2TP) connection, specify the IP address of the L2TP Network Server (LNS) at the remote end of the tunnel. For a TCP-Clear connection, specify the address of a security gateway or dial-in host. The default is 0.0.0.0.

Example: `set tunnel-address = 10.10.10.1`

Location: IPSec *name*

See Also: Active, Encap-Mode, Name, Recv-AH, Recv-ESP, Send-AH, Send-ESP

Tunneling-Protocol

Description: Specifies the protocol to use when creating a tunnel for this profile.

Usage: Specify one of the following values:

- ATMP-Protocol specifies Ascend Tunnel Management Protocol (ATMP).
- L2TP-Protocol specifies Layer 2 Tunneling Protocol (L2TP). You must choose this setting in order to pass traffic to an L2TP Network Server (LNS).
- L2F-Protocol specifies Layer 2 Forwarding (L2F). You must choose this setting to send traffic to a home gateway.
- PPTP-Protocol specifies Point-to-Point Tunneling Protocol (PPTP). You must choose this setting in order to pass traffic to a PPTP Network Server (PNS).
- IPINIP specifies that IP packets are encapsulated in IP.

Example: `set tunneling-protocol = l2tp-protocol`

Note: The TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: Connection *station* > Tunnel-Options

See Also: Home-Network-Name, Max-Tunnels, Password, Primary-Tunnel-Server, Profile-Type, Secondary-Tunnel-Server, UDP-Port

Tunnel-Options

Description: A subprofile that enables you to configure Ascend Tunnel Management Protocol (ATMP), Layer 2 Tunneling Protocol (L2TP), or Layer 2 Forwarding (L2F) settings.

Usage: With a Connection profile as the working profile, list the Tunnel-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Tunnel-Options subprofile:

```
admin> list tunnel-options
[in CONNECTION/tim: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 = ""
vrouter = ""
client-auth-id = ""
server-auth-id = ""
assignment-id = ""
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: Assignment-ID, ATMP-HA-RIP, Client-Auth-ID, Home-Network-Name, Max-Tunnels, Password, Primary-Tunnel-Server, Profile-Type, Secondary-Tunnel-Server, Server-Auth-ID, Tunneling-Protocol, UDP-Port, VRouter

Tunnel-Server

Description: A profile that enables you to configure settings for a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnel to a specific endpoint.

Usage: Use the Read and List commands to make Tunnel-Server the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the Tunnel-Server profile *berkeley* the working profile and list its contents:

```
admin> read tunnel-server berkeley
TUNNEL-SERVER/berkeley read

admin> list
[in TUNNEL-SERVER:berkeley]
server-endpoint* = berkeley
enabled = yes
shared-secret = ""
ipsec-profile = ""
client-auth-id = ""
server-auth-id = ""
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write  
TUNNEL-SERVER/berkeley written
```

See Also: Client-Auth-ID, Enabled, IPSec-Profile, Server-Auth-ID, Server-Endpoint, Shared-Secret

TX-Cell-Payload-Scramble-Disabled

Description: Enables or disables scrambling of the 48-byte Asynchronous Transfer Mode (ATM) payload in transmitted cells.

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

- Yes disables scrambling of the 48-byte ATM payload in transmitted cells.
- No enables scrambling of the 48-byte ATM payload in transmitted cells.

Example: `set tx-cell-payload-scramble-disabled = yes`

Dependencies: Set TX-Cell-Payload-Scramble-Disabled to Yes only if the receiving switch has disabled the corresponding descramble function.

Location: OC3-ATM {shelf-*N* slot-*N* *N*} > Line Config

See Also: TX-Scramble-Disabled

TX-Data-Rate-Limit

Description: Specifies the maximum data rate (in Kbps) to be transmitted across the connection. You can use this setting to limit bandwidth for a connection according to the rate charged for the account.

Usage: Specify a number from 0 to 64000. The default is 0 (zero), which disables the data-rate-limit feature. If the value you specify is larger than the actual bandwidth provided by the line, the connection behaves as though the data-rate limit were disabled, except that additional computations are performed unnecessarily.

Example: `set tx-data-rate-limit = 32000`

Dependencies: The system activates configurable transmit data-rate limits only for connections that use unchannelized DS3 cards. If you specify a value for a connection that does not use these cards, the system ignores the settings.

Location: Connection > Session-Options

See Also: RX-Data-Rate-Limit

TX-Scramble-Disabled

Description: Enables or disables scrambling of the entire Asynchronous Transfer Mode (ATM) transmit stream.

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

- Yes disables scrambling of the entire ATM transmit stream.
- No enables scrambling of the entire ATM transmit stream.

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 {shelf-*N* slot-*N* *N*} > Line Config

See Also: TX-Cell-Payload-Scramble-Disabled

Type

Description: In a Filter profile, specifies whether the current filter is a generic filter, an IP filter, or a route filter:

- A generic filter focuses on certain bytes or bits in a packet, and compares the contents of that location with a value defined in the filter. To use generic filters effectively, you need to know the contents of certain bytes in the packets you wish to filter.
- An IP filter focuses on known fields in IP packets (source or destination address, or protocol, for example).
- A route filter can forward or drop packets on the basis of the specified route.

In the SS7-Gateway > Transport-Options subprofile, specifies the type of Transport layer.

In an Error profile, indicates the type of error that occurred.

Usage: In a Filter profile, specify one of the following values:

- Generic-Filter (the default) specifies a generic filter.
- IP-Filter specifies an IP filter.
- IPX-Filter specifies an IPX filter.
- Route-Filter specifies a route filter.
- TOS-Filter specifies a Type-of-Service (TOS) filter.

In the SS7-Gateway > Transport-Options subprofile, specify one of the following values:

- Ascend (the default) specifies the transport layer used by the ASGCP and IPDC protocols: TCP/IP-based data delivery with built-in redundancy and retransmission.
- TCP-Encaps-2 specifies that the system uses a TCP/IP stream with a 2-octet header added to every signaling message. The TCP-Encaps-2 setting is required for Q.931+ and does not apply unless Control-Protocol is set to Q931-Plus.

In an Error profile, the Type setting is read only.

Example: `set type = generic-filter`

Dependencies: When Type is set to TCP-Encaps-2, all parameters in the Transport-Options subprofile, except the Heartbeat parameter, are not applicable.

Location: Error, Filter *filter-name* > Input-Filters, Filter *filter-name* > Output-Filters, SS7-Gateway > Transport-Options

See Also: Index, Input-Filters, IP-Address, IS-Post, Loadname, Output-Filters, Shelf, Slot, Stack-Trace, User-Profile, Version

Type-Filter

Description: Specifies whether the IPX SAP filter will explicitly include the service in the SAP table or exclude it.

Usage: Specify one of the following values:

- Exclude (the default) specifies that the filter excludes the service from the SAP table.
- Include specifies that the filter includes the service in the SAP table. Choose this setting to include a specific service when previous input or output filters have excluded a general type of service.

Example: `set type-filter = include`

Location: IPX-SAP-Filter > Input-IPX-SAP-Filters,
IPX-SAP-Filter > Output-IPX-SAP-Filters

See Also: Server-Name, Server-Type, Valid-Filter

Type-of-Service

Description: Specifies the type of service for the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits used to set precedence for priority queuing. The next four bits of the TOS byte are used to choose a link according to the type of service. When TOS is enabled, you can set one of the following values in the packet:

- Normal specifies normal service (the default).
- Cost minimizes monetary cost.
- Reliability maximizes reliability.
- Throughput maximizes throughput.
- Latency minimizes delay.

Example: `set type-of-service = cost`

Dependencies: For the Type-of-Service setting to apply, you must set Active to Yes in the TOS-Options subprofile, or Type to TOS-Filter in the Input-Filters or Output-Filters subprofile.

Location: Connection *station* > IP-Options > TOS-Options,
Filter *filter-name* > Input-Filters > TOS-Filter,
Filter *filter-name* > Output-Filters > TOS-Filter,
VoIP {*x y*} > TOS-Options

See Also: Active, Apply-To, Precedence

U

UDP-Cksum

Description: Enables or disables the use of UDP checksums on the interface. If you enable UDP checksums, the TAOS unit generates a checksum whenever it sends out a UDP packet. It sends out UDP packets for queries and responses related to the following protocols and facilities:

- ATMP
- DNS
- ECHOSERV
- RADIUS
- RIP
- SNTP
- SYSLOG
- TACACS
- TFTP

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

- Yes generates UDP checksums for queries and responses for protocols that use UDP.
- No disables UDP checksums.

Example: `set udp-cksum = yes`

Dependencies: You might want to enable UDP-Cksum 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.

Location: IP-Global

See Also: Protocol

UDP-Port

Description: Specifies a UDP port as follows:

- In an ATMP profile, specifies the User Datagram Protocol (UDP) port that the TAOS unit uses locally to manage the Ascend Tunnel Management Protocol (ATMP) tunnel.
- In a Connection profile, sets the default UDP port to use when communicating with a Home Agent.
- In a Stacking profile, specifies the UDP port number to use for intrastack control packets.

Usage: Specify a UDP port number. The default is 5150. When you use the value for a tunnel, both ends of the tunnel must agree on the number. When you use the value for a stack, all members of the stack must use the same UDP port number. Multiple stacks can specify the same port number, because the port does not have to be unique to a stack.

Example: `set udp-port = 5100`

Dependencies: In a Connection profile, you can override the value of UDP-Port by specifying a UDP port in the Primary-Tunnel-Server or Secondary-Tunnel-Server setting. If you change the UDP-Port setting, the new value does not take effect until you reset the system.

Location: ATMP, Connection *station* > Tunnel-Options, Stacking *name*

See Also: Agent-Mode, Agent-Type, Data-IP-Address, Home-Network-Name, Max-Tunnels, Password, Primary-Tunnel-Server, Profile-Type, Retry-Limit, Retry-Timeout, Secondary-Tunnel-Server

UDP-Queue-Length

Description: Specifies the maximum number of UDP packets that can reside in the input queue for the Layer 2 Forwarding (L2F) Network Access Server (NAS).

Usage: Specify a value from 0 to 512. The default is 256. A value of zero (0) specifies that the packets are not dropped, no matter how busy the UDP subsystem gets. Use the default value with caution. If the queue grows too large in an extremely loaded routing environment, the system can run out of memory.

Example: `set udp-queue-length = 512`

Note: The TAOS unit can operate as an L2F NAS in communication with an L2F home gateway that is a Cisco router running Cisco IOS 11.3. The current implementation of L2F was designed to interoperate only with Cisco IOS 11.3 from Cisco Systems. Other software versions or tunnel peers might not be supported.

Location: L2-Tunnel-Global

See Also: L2F-Mode, L2F-Retry-Count, L2F-Retry-Interval, L2F-System-Name, L2F-Tunnel-Secret

UDS3

Description: Specifies the action to take when the code image for an unchannelized DS3 card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, T3, UE1, Unknown-Cards, UT1

UE1

Description: Specifies the action to take when the code image for an E1 FrameLine card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, T3, UDS3, Unknown-Cards, UT1

Unknown-Cards

Description: Specifies the action to take when the code image for newly supported cards is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, T3, UDS3, UE1, UT1

Up-Status

Description: Indicates the status of a device.

Usage: The Up-Status setting is read only. It can have one of the following values:

- 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 {{shelf-*N* slot-*N* *N*} *N*}

See Also: Device-Address, Device-State, Reqd-State

Use-Answer-For-All-Defaults

Description: Specifies whether values in the Answer-Defaults profile should override values in the default Internet profile when the TAOS unit uses Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control (TACACS) to validate an incoming call.

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

- Yes instructs the TAOS unit to use the Answer-Defaults profile for defaults. When you specify Yes, the 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 TAOS unit uses the default Internet profile for defaults. When you specify No, the 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

Use-Exceeded-Enabled

Description: Specifies whether the system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it, or when the system DS0 usage has been exceeded.

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

- Yes specifies that the system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it, or when 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 when the system DS0 usage has been exceeded.

Example: `set use-exceeded-enabled = no`

Location: Trap *host-name*

See Also: Port-Enabled

User

Description: Indicates the username for the Rlogin session.

Usage: The User value is read only.

Example: user = robin

Location: Ext-Tsrv > Hosts-Info *N*

See Also: Service

User (profile)

Description: A profile that defines a name, a password, privileges, and default displays for user login accounts.

Usage: Use the Read and List commands to make User the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the User profile default the working profile and list its contents:

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

admin> list
[in USER/default]
name* = default
password = ""
active-enabled = yes
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
screen-width = 80
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
USER/default written
```

See Also: Active-Enabled, Allow-Code, Allow-Diagnostic, Allow-Password, Allow-System, Allow-Termserve, Allow-Update, Bottom-Status, Default-Status, Idle-Logout, Left-Status, Log-Display-Level, Nailed-Up-Group, Password, Prompt, Screen-Length, Screen-Width, Status-Length, Top-Status, Use-Scroll-Regions

User-N

Description: Specifies the username for Rlogin sessions with Host-N.

Usage: Specify a text string of up to 31 characters. The default is null.

Example: `set user-1 = robin`

Dependencies: User-N applies only when Service-N is set to Rlogin.

Location: Terminal-Server > Menu-Mode-Options

See Also: Host-N, Service-N

User-Profile

Description: In the IP-Global profile, specifies the name of the default User profile associated with Telnet sessions. In a Serial profile, specifies the name of the default User profile associated with serial access to the command interface. In an Error profile, indicates the name of the user that reset the unit.

Usage: In the IP-Global or Serial profile, specify the name of a User profile. For the IP-Global profile, the default is null. For the Serial profile, the default is `admin`. In either profile, a null value specifies that the user must log in explicitly. In an Error profile, the User-Profile setting is read only.

Example: `set user-profile = default`

Location: Error, IP-Global, Serial {shelf-N slot-N N}

See Also: Index, IP-Address, IS-Post, Loadname, Shelf, Slot, Stack-Trace, Type, Version

Userstat-Format

Description: Enables you to customize the output of the Userstat command or a Finger query.

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 (shelf.slot.line/chan). The shelf number is always 1.
%s	11	Slot:Item	Shelf:slot:item/logical-item of the host port. The shelf number is always 1.

String	Field width	Output text	Meaning
%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 hours: minutes:seconds
%t	10	IdleTime	Amount of time idle, in hours:minutes:seconds
%n	24	Dialed#	Number dialed, if known
%f	24	Calling#	Calling-line ID, if known

The default value of Userstat-Format causes the standard session-listing output format for both the Userstat command and Finger queries.

Example: An administrator customizes the session-listing output to include only the Username, Svc, and ConnTime information, and specifies 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          (PPP) @ 1:22:34
jimmyq        (PPP) @ 3:44:19
sallyg        (PPP) @ 5:12:56
<end user list> 3 active user(s)
```

Location: System

See Also: Finger, Userstat-Format

User-User-Info

Description: Indicates the contents of the ISDN user-user information element in the Setup message for the incoming call.

Usage: The User-User-Info value is a read-only hexadecimal value.

Example: user-user-info=00:04:05:06:07:08:09:10:01:02:03:04:05:+

Location: Call-Info

See Also: User-User-Infolen

User-User-Infolen

Description: Indicates the size (in bytes) of the value of User-User-Info.

Usage: The User-User-Infolen value is read only.

Example: `user-user-infolen = 120`

Location: Call-Info

See Also: User-User-Info

Use-Scroll-Regions

Description: Specifies whether the VT100 scroll-region commands are used to reduce screen redraws when the status screen is displayed.

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

- Yes specifies that the VT100 scroll-region commands are used to reduce screen redraws.
- No disables the VT100 scroll-region commands. If the status screen is not redrawing properly, try setting Use-Scroll-Regions to No.

Example: `set use-scroll-regions = yes`

Location: User *name*

See Also: Bottom-Status, Default-Status, Left-Status, Top-Status

Use-System-IP-Address-As-Source

Description: Enables or disables the use of the system address as the source address for packets generated by the TAOS unit.

The System-IP-Addr parameter of the IP-Global profile specifies the source address of all packets generated by the system (such as the connection request packets sent to a signaling gateway to establish communication). By default, the TAOS unit uses the system address as its source address in the packets it sends to the signaling gateway.

However, for some sites, administrative policy or other constraints introduce a requirement to use the system address for some purposes, but to use a separate source address for communication with the signaling gateway. For example, although a site might require a certain system address for compatibility with other routers, this requirement might cause an address space conflict, or might cause delays and timeouts in the receipt of acknowledgements from signaling gateways. Or, a site might decide to separate the signaling control network from the Internet for security purposes. To integrate the TAOS unit into your system's infrastructure and enable it to communicate efficiently with signaling gateways, you can specify that the TAOS unit does not use the system address as its source address for signaling packets.

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

- Yes enables the use of the system address as the source address for packets generated by the unit.
- No disables the use of the system address as the source address for packets generated by the unit. Instead, the unit uses the IP address of the Ethernet interface on which the signaling packets are sent.

Example: `set use-system-ip-address-as-source = no`

Location: SS7-Gateway

See Also: System-IP-Addr

Use-Trunk-Groups

Description: Enables or disables the use of trunk groups for all network lines. When trunk groups are enabled, channels must be assigned trunk-group numbers.

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

- Yes specifies that all channels must be assigned a trunk-group number for outgoing calls.
- No disables trunk groups.

Example: `set use-trunk-groups = yes`

Dependencies: When Use-Trunk-Groups is set to Yes, the T1 or E1 channel configuration must specify Trunk-Group assignments.

Location: System

See Also: Call-Type, Channel-Config N, Dial-Number, Num-Digits-Trunk-Groups, Trunk-Group

UsrRad-Options

Description: A subprofile that defines connection-specific Remote Authentication Dial-In User Service (RADIUS) accounting options.

Usage: With a Connection profile as the working profile, list the UsrRad-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the UsrRad-Options subprofile:

```
admin> list usrRad-options
[ 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
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: RADIUS accounting must be configured in the Rad-Acct-Client subprofile of the External-Auth profile.

Location: Connection *station*

See Also: Acct-Host, Acct-ID-Base, Acct-Key, Acct-Port, Acct-Timeout, Acct-Type, Rad-Acct-Client

UT1

Description: Specifies the action to take when the code image for a T1 FrameLine card is present in a tar file.

Usage: Specify one of the following settings:

- Auto (the default) causes the system to load images for cards that are installed in the TAOS unit, and to skip images for cards that are not installed.
- 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.

Dependencies: A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot -r command to permanently remove a card 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 cards that are no longer installed in the system.

Location: Load-Select

See Also: 8E1, 8T1, AMDM, Carrier-Established, DNS-List-Attempt, DS3-ATM, Enet2, HDLC2, SWAN, T3, UDS3, UE1, Unknown-Cards

V

V42/MNP

Description: Specifies how the digital modems negotiate LAPM/MNP error control with the analog modem at the other end of the connection.

Usage: Specify one of the following values:

- Will-V42 (the default) specifies that the modems request LAPM/MNP, but accept the call if it is not provided.
- Wont-V42 specifies that the modems do not use LAPM/MNP at all.
- Must-V42 specifies that the modems request LAPM/MNP, and drop the call if it is not provided.

Example: `set v42/mnp = will-v42`

Dependencies: If terminal services are disabled, V42/MNP does not apply.

Location: Terminal-Server > Modem-Configuration

See Also: Modem-Configuration

V120-Answer

Description: A subprofile containing default settings for V.120 calls.

Usage: With Answer-Defaults as the working profile, list the V120-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the V120-Answer subprofile:

```
admin> list v120-answer
[ in ANSWER-DEFAULTS:v120-answer ]
enabled = yes
frame-length = 256
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Enabled, Frame-Length

Valid-Entry

Description: In a Filter profile, enables or disables the current input or output filter. In a Permit-List subprofile, enables or disables the permit-list entry.

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

- Yes activates the filter or permit list.
- No disables the filter or permit list.

Example: `set valid-entry = yes`

Location: Filter *filter-name* > Input-Filters, Filter *filter-name* > Output-Filters
TACL > Permit-List

See Also: Input-Filters, Output-Filters, Permit-List

Valid-Filter

Description: Enables or disables the IPX SAP input or output filter.

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

- Yes enables the IPX SAP filter.
- No disables the IPX SAP filter. If you specify No, the TAOS unit skips the filter when it applies the entire IPX SAP filter to SAP data.

Example: `set valid-filter = yes`

Location: IPX-SAP-Filter > Input-IPX-SAP-Filters,
IPX-SAP-Filter > Output-IPX-SAP-Filters

See Also: Server-Name, Server-Type, Type-Filter

Value

Description: Specifies a hexadecimal number to be compared to specific bits in packets after the generic filter's Offset, Len, and Mask calculations have been performed.

Usage: Specify a hexadecimal number representing up to 12 bytes.

Example: `set value = aaaa0300000080f3`

Location: Filter *filter-name* > Input-Filters > Gen-Filter,
Filter *filter-name* > Output-Filters > Gen-Filter

See Also: Gen-Filter, Input-Filters, Output-Filters

VC-Fault-Management

Description: Specifies the fault management type for the Virtual Circuit (VC).

Usage: Specify one of the following settings:

- None (the default) specifies that no fault management is performed on the VC.
- Segment-Loopback specifies that the system sends an OAM F5 segment loopback cell to the remote device every five seconds.
- End-to-End-Loopback specifies that the system sends an OAM F5 end-to-end loopback cell to the remote device every five seconds.

Example: `set vc-fault-management = segment-loopback`

Location: Connection *station* > ATM-Options

See Also: VC-Max-Loopback-Cell-Loss

VCI

Description: Specifies the Virtual Circuit Identifier (VCI) for the connection.

Usage: Specify a number from 32 to 1023. The default is 32.

Location: Connection *station* > ATM-Options

See Also: VPI

VC-Max-Loopback-Cell-Loss

Description: Specifies the number of consecutive loopback cells lost before the system clears the connection. When a PVC is cleared, the interface is in an inactive state until the system can reestablish the connection.

Usage: Specify an integer. The default is 1.

Example: `set vc-max-loopback-cell-loss = 5`

Location: Connection *station* > ATM-Options

See Also: VC-Fault-Management

Version

Note: The TAOS unit does not support firewalls at this time.

Description: In the Firewall profile, specifies the firewall version. In an Error profile, specifies the software version that was running when an error occurred. In the Recv-ESP or Send-ESP subprofile of the IPSec profile, specifies the Encapsulating Security Payload (ESP) version.

Usage: If you change this setting in the Firewall profile, one of the following messages appears:

```
error: Base 64 decode failed
error: Firewall does not load properly (corrupted?)
```

In an Error profile, the Version setting is read only. In the Recv-ESP or Send-ESP subprofile of the IPSec profile, you can specify 1 (for version 1) or 2 (for version 2).

Location: Error, Firewall *name*, IPSec *name* > Recv-ESP, IPSec *name* > Send-ESP

See Also: ESP-Type

Visa2-Answer

Description: A subprofile that lets you specify whether the system rejects incoming Visa-II calls.

Usage: With the Answer-Defaults profile as the working profile, list the Visa2-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Visa2-Answer profile:

```
admin> list visa2-answer
[in ANSWER-DEFAULTS:visa2-answer]
enabled = no
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Enabled

Visa2-Options

Description: A subprofile that contains settings for Visa terminal calls.

Usage: With a Connection profile as the working profile, list the Visa2-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the Visa2-Options subprofile:

```
admin> list visa2-options
[in CONNECTION/robin:visa2-options]
enabled = no
idle-character-delay = 10000
first-data-forward-character = 04
second-data-forward-character = 06
third-data-forward-character = 15
fourth-data-forward-character = 05
1-char-sequence = 03
2-char-sequence = 00:03:00:00
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Connection *station*

See Also: 1-Char-Sequence, 2-Char-Sequence, Enabled, First-Data-Forward-Character, Fourth-Data-Forward-Character, Idle-Character-Delay, Second-Data-Forward-Character, Third-Data-Forward-Character

VJ-Header-Prediction

Description: Specifies whether Van Jacobson IP header prediction should be negotiated on incoming calls.

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

- Yes 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 *station* > IP-Options

See Also: IP-Answer, IP-Options, IPX-Routing-Enabled

Voice-Ann-Dir

Description: Specifies the location of voice announcement files on a PCMCIA flash memory card in the TAOS unit.

Usage: Specify a directory. You can enter up to 40 characters. The default is `/current`. When the system receives a request to play an announcement, it looks in the specified directory on the flash card in slot 1. If the card is not present or the voice announcement file is not found, the system looks for the specified directory on flash card 2.

Example: `set voice-ann-dir = /current/newyork`

Dependencies: For Voice-Ann-Dir to apply, you must set H323-Voice-Ann-Enabled to Yes.

Location: VoIP {*x y*}

See Also: Early-Ringback-Enable, H323-Voice-Ann-Enabled, Voice-Ann-Enc

Voice-Ann-Enc

Description: Specifies G.711 U-Law or G.729 encoding of voice announcements that report call progress to callers.

Usage: Specify one of the following values:

- G711-ULaw enables the use of G.711 U-Law encoding for voice announcement play out.
- G729 enables the use of G.729 encoding for voice announcement play out.

Example: `set voice-ann-enc=g729`

Dependencies: Consider the following:

- The MultiVoice gateway must be configured to use voice announcements to report call progress.
- Before a MultiVoice gateway is configured to use G.729 voice announcement encoding, voice announcement files must be converted to G.729-compatible format. Lucent Technologies offers a tool, at no charge to MultiVoice customers, that creates G.729 encoded voice-announcement files.
- The MultiVoice gateway must be configured to use G.729 voice-announcement encoding when the Lucent Technologies prepaid-billing-message set is used for reporting call progress and for playing out billing announcements.
- Changes to the Voice-Ann-Enc value are effective with the next VoIP call.

Location: VoIP {x y}

See Also: Voice-Ann-Dir

VoIP

Description: A profile that enables you to configure Voice over IP (VoIP).

Usage: Use the Read and List commands to make VoIP the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the VoIP profile with the index { 0 0 } the working profile and list its contents:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> list
[ in VOIP/{ 0 0 } ]
voip-index* = { 0 0 }
gatekeeper-ip = 0.0.0.0
vpn-mode = no
packet-audio-mode = g711-ulaw
frames-per-packet = 2
tos-options = { no 101 latency both }
silence-det-cng = no
gatekeeper-ip-sec = 0.0.0.0
gatekeeper-keepalive = 120
registration-retries = 5
registration-retry-timer = 5
primary-retries = 1
ena-adap-jitter-buffer = yes
max-jitter-buffer-size = 19
initial-jitter-buffer-size = 2
maxcalls = 2688
cut-thru-enable-nearend = yes
single-dial-enable = no
h323-voice-ann-enabled = no
voice-ann-dir = /current
call-inter-digit-timeout = 6000
```

```
silence-threshold = 0
dtmf-tone-passing = dtmf-tone-passed-inband
rt-fax-options = { no yes yes yes yes }
call-hairpin = no
call-keep-alive-timeout = 0
clid-suppress = no
true-connect-enable = no
g711-transparent-data = no
allow-g711-fallback = yes
allow-coder-fallback = yes
trunk-quiesce-enable = no
early-ringback-enable = no
trunk-prefix-enable = no
voice-ann-enc = g711-ulaw
gk-mlg-control = yes
transfer-to-operator = *0
sequential-calls-enable = yes
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
VOIP/{ 0 0 } written
```

See Also: Allow-G711-Fallback, Call-Hairpin, Call-Inter-Digit-Timeout, Call-Keep-Alive-Timeout, CLID-Suppress, Cut-Thru-Enable-Nearend, DTMF-Tone-Passing, Early-Ringback-Enable, Ena-Adap-Jitter-Buffer, Frames-Per-Packet, G711-Transparent-Data, Gatekeeper-IP, Gatekeeper-IP-Sec, Gatekeeper-Keepalive, Gk-Mlg-Control, H323-Voice-Ann-Enabled, Initial-Jitter-Buffer-Size, Maxcalls, Max-Jitter-Buffer-Size, Packet-Audio-Mode, Primary-Retrieves, Registration-Retrieves, Registration-Retry-Timer, RT-Fax-Options, Sequential-Calls-Enable, Silence-Det-Cng, Silence-Threshold, Single-Dial-Enable, TOS-Options, Transfer-to-Operator, True-Connect-Enable, Trunk-Prefix-Enable, Trunk-Quiesce-Enable, Voice-Ann-Dir, Voice-Ann-Enc, VPN-Mode

VoIP-Enabled

Description: Indicates whether the unit enables Voice over IP (VoIP).

Usage: The VoIP-Enabled setting is read only. Yes indicates that VoIP is enabled. No indicates that VoIP is not enabled.

Example: voip-enabled = yes

Location: Base

See Also: VoIP-Max-Capacity-Allowed

VoIP-GK-Change-Enabled

Description: Enable or disables trap generation when the registered gatekeeper changes (Ascend Trap 39). If a new gatekeeper is registered with the MultiVoice gateway, a register request (RRQ) message is sent from the MultiVoice gateway to the new gatekeeper. When the MultiVoice gateway receives the admission request (ARQ) message from the new gatekeeper, the generated trap sends the following information to the Simple Network Management Protocol (SNMP) manager:

- The new gatekeeper index (voipCfgGkIndex)
- The IP address of new gatekeeper (voipCfgGkIpAddress)
- The absolute time to show when the gatekeeper change occurred (sysAbsoluteCurrentTime)

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

- Yes enables trap generation when the registered gatekeeper changes.
- No disables trap generation when the registered gatekeeper changes.

Example: `set voip-gk-change-enabled = yes`

Location: Trap *name*

See Also: Call-Log-Serv-Change-Enabled, WAN-Line-State-Change-Enabled

VoIP-Index

Description: A subprofile that enables you to specify a Dialed Number Information Service (DNIS) number for processing calls from the Public Switched Telephone Network (PSTN) as Voice over IP (VoIP) calls.

Usage: With VoIP as the working profile, list the VoIP-Index subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the VoIP-Index subprofile:

```
admin> list voip-index
[in VOIP/{ 8903190 0 }:voip-index
gateway-access-number = 8903190
far-end-number = 0
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: VoIP {*x y*}

See Also: Far-End-Number, Gateway-Access-Number

VoIP-Max-Capacity-Allowed

Description: Indicates whether the unit enforces a maximum VoIP call-processing limit.

Usage: The VoIP-Max-Capacity-Allowed setting is read only. Yes indicates that the unit enforces a maximum VoIP call-processing limit, regardless of how many DS3, T3, MultiDSP, or Ethernet slot cards are installed. No indicates that the unit does not enforce a limit.

Example: `voip-max-capacity-allowed = yes`

Location: Base

See Also: VoIP-Enabled

VPI

Description: Specifies the Virtual Path Identifier (VPI) for the connection.

Usage: Specify a number from 0 to 15. The default is 0 (zero).

Location: Connection *station* > ATM-Options

See Also: VCI

VPI-VCI-Range

Description: Specifies a range of values in the Virtual Path Identifier and Virtual Channel Identifier (VPI-VCI) pair.

Usage: Select the best combination of VPI and VCI bit sizes to fit the list of supported VPI-VCI pairs obtained from your network provider. The new values take effect as soon as you write the OC3-ATM, E3-ATM, or DS3-ATM profile. The default setting of 0-15/32-4095 is the range of values that can be represented with a 4-bit VPI and 12-bit VCI. This setting is compatible with earlier releases. Following are the possible ranges and their relevant bit sizes:

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

Location: DS3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
E3-ATM {shelf-*N* slot-*N* *N*} > Line-Config,
OC3-ATM {shelf-*N* slot-*N* *N*} > Line-Config

See Also: VCI, VPI

VPN-Mode

Description: Specifies whether the TAOS unit collects a MultiVoice user's Personal Identification Number (PIN) when MultiVoice is configured to perform H.323 call processing.

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

- Yes specifies that the TAOS unit does not prompt for a PIN from the user.
- No specifies that the TAOS unit prompts for a PIN from the user. The unit presents the caller with either a dial tone or a series of prompts indicating that a PIN is required.

Example: `set vpn-mode = yes`

Dependencies: The VPN-Mode value has no effect on Automatic Number Identification (ANI) authentication for H.323 call processing.

Location: VoIP {*x y*}

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 an IPX-Interface profile assigns the IPX interface to a 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 = vrouter-2`

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 knows about only those interfaces that explicitly specify the same VRouter, this feature enables the system to separate traffic for different LNS systems. Note that the TAOS unit 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.
- If you do not specify a VRouter in an IPX-Interface profile, the interface belongs to the global VRouter.

Location: Connection *station*, Connection *station* > Tunnel-Options, IP-Interface {shelf-*N* slot-*N* *N*}, IP-Route *name*

See Also: Inter-VRouter, VRouter (profile), VRouter-IP-Address

VRouter (profile)

Description: A profile that enables you to configure settings for a Virtual Router (VRouter).

Usage: Use the Read and List commands to make VRouter the working profile and list its contents. You can then use the Set command to modify the settings in the profile. To close the profile and save your changes, enter the Write command.

Example: To make the VRouter profile `vrouter-1` the working profile and list its contents:

```
admin> read vrouter vrouter-1
VROUTER/vrouter-1 read

admin> list
[in VROUTER/vrouter-1]
name = vrouter1
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 +
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
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
ipx-routing-enabled = no
ipx-dialin-pool = " "
```

After making any changes to the settings in the profile, save your modifications by entering the following command:

```
admin> write
VROUTER/vrouter-1 written
```

Dependencies: Deleting a VRouter profile deletes the Virtual Router. If you delete a VRouter with active connections, a reset is recommended. If a system reset is not possible, you should manually tear down the VRouter's active connections and then modify the local Connection, IP-Interface, and IP-Route profiles that point to the VRouter before deleting the VRouter profile.

See Also: Active, Allow-As-Client-DNS-Info, Assign-Count, Name, Client-Primary-DNS-Server, Client-Secondary-DNS-Server, DNS-Primary-Server, DNS-Secondary-Server, Domain-Name, IPX-Dialin-Pool, IPX-Routing-Enabled, Pool-Base-Address, Pool-Name, Pool-Summary, RIP-Policy, RIP-Trigger, Sec-Domain-Name, Summarize-RIP-Routes, VRouter-IP-Address

VRouter-IP-Address

Description: Specifies the system address for the Virtual Router (VRouter).

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

Example: `set vrouter-ip-address = 200.40.60.5`

Location: VRouter *name*

See Also: Assign-Count, Name, Pool-Base-Address, Pool-Name, Pool-Summary, RIP-Policy, RIP-Trigger, Summarize-RIP-Routes

W

WAN-Line-State-Change-Enabled

Description: Enables or disables trap 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 (wanLineIfInde).
- 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: Specify Yes or No. The default is No.

- Yes enables trap generation if the state of an E1 or T1 line changes.
- No disables trap generation if the state of an E1 or T1 line changes.

Example: `set wan-line-state-change-enabled = yes`

Location: Trap *name*

See Also: Call-Log-Serv-Change-Enabled, VoIP-GK-Change-Enabled

Warmstart-Enabled

Description: Specifies whether the system generates a trap when the TAOS unit reinitializes itself but neither the configuration of the Simple Network Management Protocol (SNMP) manager nor that of the system itself is altered.

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

- Yes specifies that the system generates a trap when the TAOS unit reinitializes itself in such a way that neither the configuration of the SNMP manager nor that of the system itself is altered.
- No specifies that the system does not generate a trap when the TAOS unit reinitializes itself in such a way that neither the configuration of the SNMP manager nor that of the system itself is altered.

Example: `set warmstart-enabled = no`

Location: Trap *host-name*

See Also: Coldstart-Enabled

Window-Size

Description: Specifies a window size:

- In the QSALL-Options subprofile, the Window-Size value specifies the Q.SAAL window size.
- In the SS7-Gateway profile, the Window-Size value specifies the maximum number of sequentially numbered data packets that can be sent while awaiting acknowledgment at any given time.

Usage: Specify an integer:

- In the QSALL-Options subprofile, specify an integer from 16 to 128. The default is 64.
- In the SS7-Gateway profile, specify an integer from 1 to 63. The default is 7.

Example: `set window-size = 128`

Location: ATM-Interface { {shelf-*N* slot-*N* *N* } *N* } > SVC-Options > QSAAL-Options, SS7-Gateway > Transport-Options

See Also: ACK-Threshold, Device-ID, Heart-Beat, Max-Cc, Max-Pd, Max-Stat, T1-Duration, T2-Duration, T3-Duration, Tcc-ms, Tidle-ms, Tkeepalive-ms, Tnoresponse-ms, Tpoll-ms, Window-Size

Write-Access-Hosts

Description: An array specifying up to eight IP addresses of SNMP managers with Write permission. The TAOS 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. You can then set the Write-Access-Hosts parameter by specifying its numeric index and entering an address.

Example: To list the array elements and specify the Write-Access-Hosts[1] value:

```
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
write-access-hosts[6] = 0.0.0.0
write-access-hosts[7] = 0.0.0.0
write-access-hosts[8] = 0.0.0.0
admin> set 1 10.2.3.4/24
```

To specify the Write-Access-Hosts[1] value without first listing the array:

```
admin> set write-access-hosts 1 10.2.3.4/24
```

Dependencies: For the Write-Access-Hosts setting to restrict read-write access to the TAOS unit, you must set the Enforce-Address-Security parameter to Yes in the SNMP profile.

Location: SNMP

See Also: Enabled, Enforce-Address-Security, Read-Access-Hosts, Read-Community, Read-Write-Community

X

X75-Answer

Description: A subprofile containing default settings for X.75 calls.

Usage: With Answer-Defaults as the working profile, list the X.75-Answer subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the X75-Answer subprofile:

```
admin> list x75-answer
[in ANSWER-DEFAULTS:x75-answer]
enabled = yes
k-frames-outstanding = 7
n2-retransmissions = 10
t1-retran-timer = 1000
frame-length = 1024
```

To return to a higher context in the working profile:

```
admin> list ..
```

Location: Answer-Defaults

See Also: Frame-Length, K-Frames-Outstanding, N2-Retransmissions, T1-Retrans-Timer

X75-Options

Description: A subprofile that contains settings for X.75 calls.

Usage: With a Connection profile as the working profile, list the X75-Options subprofile. You can then use the Set command to modify the settings in the subprofile. To close the profile and return to a higher context in the working profile, enter the List command, followed by a space and two periods.

Example: To list the contents of the X75-Options subprofile:

```
admin> list x75-options
[in CONNECTION/tim:x75-options]
k-frames-outstanding = 7
n2-retransmissions = 10
t1-retran-timer = 1000
frame-length = 1024
```

To return to a higher context in the working profile:

```
admin> list ..
```

Dependencies: X.75 calls must be enabled in the Answer-Defaults profile.

Location: Connection *station*

See Also: Frame-Length, K-Frames-Outstanding, N2-Retransmissions, T1-Retrans-Timer

XCOM-SS7

Description: Enables or disables Internet Protocol Device Control (IPDC) processing on the unit.

Usage: Specify Enabled or Disabled. The default is Enabled.

- Enabled specifies that IPDC processing is enabled on the unit.
- Disabled specifies that IPDC processing is disabled on the unit.

Example: `xcom-ss7 = disabled`

Location: Base

See Also: VoIP-Enabled

Y

Yellow-Receive

Description: Specifies 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: The Yellow-Receive setting is read only. True specifies that the local device has received a Yellow Alarm indication. False specifies that the local device has not received a Yellow Alarm indication.

Location: T1-Stat {shelf-*N* slot-*N* *N*}, T3-Stat {shelf-*N* slot-*N* *N*}

See Also: AIS-Receive

Index

Symbols

? command 1-4

Numerics

2DS framing mode 2-182

3DES-CBC mode 2-160, 2-243, 2-244

A

AAL5 multiplexing 2-43

accounting

 RADIUS 2-369, 2-507

 TACACS+ 2-464

add-on numbers

 Called-Number-Type 2-78

 CallRoute 1-10

 Phone-Number 2-335

address pools 2-14

 Assign-Address 2-35

 Assign-Count 2-35

 Auth-Pool 2-56

 chaining 2-339

 OSPF, and 2-341

 pool summary 2-341

 Pool-Base-Address 2-339

 Pool-Chaining 2-339

 Pool-For-Async-Framed-User 2-340

 Pool-Name 2-340

 Pool-Number 2-341

 Pool-OSPF-Adv-Type 2-341

addresses

 Address-Pool 2-14

 assigned 2-445

 BOOTP-Enabled 2-73

 calling-party in outgoing calls 2-219

 default pool 2-126

 destination IP 2-128

 device address 2-242, 2-416, 2-423

 Device-Address 2-131

 dynamic assignment 2-35, 2-298, 2-339, 2-340

 fax servers 2-170

 filtering 2-128, 2-129, 2-130, 2-388, 2-434

 gateway for static route 2-191

 interface 2-219

 IP 2-163, 2-221

 IP direct, for 2-222

 IP on a WAN link 2-379

 IP on Ethernet 2-221

 IP-Address 2-221

 MAC 2-160, 2-161, 2-163, 2-270, 2-364, 2-439

 numbered interfaces on 2-260

 physical 2-336

 pools 2-341

 primary DNS server 2-143

 primary NetBIOS server 2-303

 RARP-Enabled 2-372

 remote numbered interface, of 2-212

 routing calls for 2-215

 secondary DNS server 2-143

 secondary NetBIOS server 2-303

 Secondary-IP-Address 2-397

 SNMP manager 2-206

 stacking data traffic, for 2-120

 static 2-439

 static routes, in 2-128, 2-191

 system 2-452

 terminal-server menu, in 2-207

 VRouter 2-143, 2-520

administering devices 1-17

administering SNMP interfaces 1-45

AESA

 Address-Prefix 2-13

 AESA-Address 2-16

 AFI 2-17

 ATM-Address 2-43

 DCC-AESA 2-177

 DSP-Portion 2-147

 E164-AESA 2-177

 ESI 2-160

 Format 2-177

 HO-DSP 2-201

 ICD-AESA 2-177

 IDI 2-209

 IDP-Portion 2-211

 Numbering-Plan 2-311

 SEL 2-402

AIM 2-19

AMI encoding 2-156

Analog Modem card, code image in tar file 2-28

Index

A

- ANIR signals
 - R1-ANIR-Delay 2-367
 - R1-ANIR-Timer 2-367
- antispoofing 2-433
- AppleTalk connections
 - AppleTalk-Options 2-30
 - Atalk-Default-Zone 2-36
 - Atalk-Dialin-Pool-End 2-36
 - Atalk-Dialin-Pool-Start 2-37
 - Atalk-Net-End 2-38
 - Atalk-Net-Start 2-38
 - Atalk-Peer-Mode 2-39
 - Atalk-Router 2-39
 - Atalk-Static-NetEnd 2-41
 - Atalk-Static-NetStart 2-41
 - Atalk-Static-ZoneName 2-41
 - Atalk-Zone-List 2-42
 - beginning of network range 2-37, 2-38
 - defining virtual network 2-37
 - end of network range 2-36, 2-38
 - Hint-Net-Hi 2-200
 - Hint-Net-Lo 2-200
 - Hint-Net-Node 2-201
 - Hint-Zone 2-201
 - routing 2-37, 2-39, 2-40
- AppleTalk node numbers 2-201
- AppleTalk routing
 - Atalk-Peer-Mode 2-39
 - Atalk-Router 2-39
 - Atalk-Routing-Enabled 2-40
- AppleTalk zones
 - Atalk-Default-Zone 2-36
 - Atalk-Static-ZoneName 2-41
 - Atalk-Zone-List 2-42
 - Hint-Zone 2-201
- ARA connections
 - ARA-Answer 2-31
 - ARA-Enabled 2-31
 - ARA-Options 2-32
 - Encapsulation-Protocol 2-156
 - Maximum-Connect-Time 2-275
 - Recv-Password 2-377
- ARPTable command 1-6
- ASBR calculations 2-33
- ASE
 - tags 2-34
 - type associated with RIP routes 2-384
 - type of external metric 2-115
 - type of LSA 2-34
- ASGCP 2-114
- asynchronous I-frames 2-36
- AT commands 2-42, 2-49
- ATM direct
 - ATM-Direct-Enabled 2-44
 - ATM-Direct-Profile 2-45
- ATM settings
 - ATM1483Type 2-43
 - ATM-Direct-Enabled 2-44
 - ATM-Direct-Profile 2-45
 - ATM-Interface 2-45
 - ATM-Options 2-45
 - Enabled 2-154
 - Encapsulation-Protocol 2-156
 - FR-08-Mode 2-178
 - Name 2-302
 - RX-Cell-Payload-Descramble-Disabled 2-392
 - RX-Descramble-Disabled 2-393
 - VC-Fault-Management 2-511
 - VCI 2-511
 - VC-Max-Loopback-Cell-Loss 2-511
 - VPI 2-517
- ATM SVC settings
 - Address-Prefix 2-13
 - AESA-Address 2-16
 - AFI 2-17
 - ATM-Address 2-43
 - ATM-Answer 2-44
 - ATM-Interface 2-45
 - ATM-Protocol 2-47
 - ATMSVC-Route 2-48
 - DSP-Portion 2-147
 - E164-Native-Address 2-152
 - Encapsulation-Protocol 2-156
 - ESI 2-160
 - Format 2-177
 - HO-DSP 2-201
 - IDI 2-209
 - IDP-Portion 2-211
 - Incoming-Caller-Addr 2-213
 - Insert-Calling-Party-Addr 2-219
 - Max-CC 2-274
 - Max-Pd 2-277
 - Max-Restart 2-278
 - Max-Stat 2-278
 - Max-Stateng 2-279
 - Name 2-301
 - Numbering-Plan 2-311
 - Outgoing-Called-Addr 2-325
 - SEL 2-402
 - SVC-Address-Info 2-445
 - SVC-Enabled 2-445
 - SVC-Options 2-445
 - T303-ms 2-459
 - T308-ms 2-459
 - T309-ms 2-459
 - T310-ms 2-460
 - T313-ms 2-460
 - T316-ms 2-460
 - T322-ms 2-460
 - Tcc-ms 2-465
 - Tidle-ms 2-477
 - Tkeepalive-ms 2-478

Tnoresponse 2-479
 Tpoll-ms 2-483
 Window-Size 2-521
 ATMlines command 1-7
 ATMP tunnels
 Agent-Mode 2-17
 Agent-Type 2-18
 ATMP profile 2-46
 ATMP-HA-RIP 2-47
 ATMP-SAP-Reply 2-48
 Force-Fragmentation 2-177
 Foreign Agents 2-17
 gateways 2-18
 Home Agent replying to Nearest Server Query 2-48
 Home Agent's gateway profile 2-47
 Home Agents 2-17
 Home-Agent-Password 2-202
 Home-Network-Name 2-202
 Idle-Timer 2-210
 Max-Tunnels 2-279
 MTU limit 2-291
 Password 2-331
 Primary-Tunnel-Server 2-354
 Profile-Type 2-360
 Retry-Limit 2-381
 Retry-Timeout 2-382
 routers 2-18
 Secondary-Tunnel-Server 2-398
 Tunneling-Protocol 2-494
 Tunnel-Options 2-494
 ATMSVCroute command 1-8
 attenuation
 buildout value 2-117
 digital modem 2-287
 AUI 2-161
 Auth command 1-9
 authentication
 assigning IP address pool 2-340
 bidirectional 2-442, 2-443
 Cache-Token 2-375, 2-407, 2-434
 called-number 2-53, 2-54, 2-77, 2-101, 2-108, 2-209, 2-328
 CHAP 2-62, 2-71, 2-127, 2-375, 2-405
 CHAP with dynamic passwords 2-375
 CLID 2-78, 2-99, 2-100, 2-101, 2-102
 MS-CHAP 2-375, 2-405
 PAP 2-62, 2-127, 2-276, 2-375, 2-404
 PAP with dynamic passwords 2-375
 PAP-Token and CHAP 2-375
 PAP-Token-CHAP 2-65, 2-262
 protocol for incoming call 2-375
 protocol for outgoing call 2-404
 Receive-Auth-Mode 2-375
 requiring for incoming async framed users 2-52
 Send-Auth-Mode 2-404

authentication key
 first pass of 3DEC-CBC encryption 2-243
 hashing 2-243
 second pass of 3DES-CBC encryption 2-243
 third pass of 3DEC-CBC encryption 2-244
 authentication services
 RADIUS 2-369
 TACACS 2-463
 TACACS+ 2-464
 authentication transforms
 3DES-CBC 2-160
 AH-Type 2-18
 DES-CBC 2-160
 ESP 2-160
 ESP-v2 2-62
 MD5 2-18, 2-63
 SHA1 2-18, 2-63
 version-2 MD5 2-18, 2-63
 version-2 SHA1 2-18, 2-63

B

B8ZS encoding 2-156
 backup connections 2-66
 bandwidth
 Add-Persistence 2-13
 BACP-Enable 2-67
 Bandwidth-Monitor-Direction 2-67
 Base-Channel-Count 2-69
 Call-Type 2-91
 Data-Service 2-121
 Decrement-Channel-Count 2-124
 Dynamic-Algorithm 2-150
 Force-56Kbps 2-176
 Increment-Channel-Count 2-215
 Max-Bundle-Members 2-273
 Maximum-Channels 2-275
 Min-Bandwidth 2-284
 Minimum-Channels 2-284
 RX-Data-Rate-Limit 2-393
 Seconds-History 2-399
 Sub-Persistence 2-442
 Target-Utilization 2-465
 TX-Data-Rate-Limit 2-496
 banner information
 Banner 2-68
 Banner N 2-68
 Ext-Tsrv 2-165
 Init-Banner N 2-216
 bidirectional authentication
 Bi-Directional-Auth 2-71
 Substitute-Recv-Name 2-442
 Substitute-Send-Name 2-443
 billing numbers 2-72

Index

C

- bit rate, serial port 2-473
- bit-error rate threshold 2-70
- boot loader 2-74
- BOOTP settings
 - Active 2-11
 - BOOTP-Enabled 2-73
 - BOOTP-Relay 2-73
 - BOOTP-Servers 2-73
 - SLIP-BOOTP 2-422
- broadcast networks 2-305, 2-310, 2-320

C

- cable length
 - DS3 2-200
 - E3 2-200
- Cache-Token authentication
 - Bi-Directional-Auth 2-71
 - Local-Profiles-First 2-262
 - Receive-Auth-Mode 2-375
 - Send-Password 2-407
 - Split-Code-Dot-User-Enabled 2-434
- call information 2-80
- call logging
 - active call-logging server 2-87
 - call-log hosts 2-82, 2-83
 - Call-Log-Enable 2-82
 - Call-Log-Host-N 2-83
 - Call-Log-ID-Base 2-83
 - Call-Log-Key 2-84
 - Call-Log-Port 2-85
 - Call-Log-RADIUS-Compat 2-85
 - Call-Log-Reset-Time 2-86
 - Call-Log-Server-Index 2-87
 - Call-Log-Stop-Only 2-87
 - Call-Log-Timeout 2-88
 - enabling 2-82
 - multiple requests in single packet 2-85
 - retries 2-84
 - returning to primary call-log host 2-86
 - session ID format 2-83
 - settings 2-82
 - shared secret 2-84
 - Stop packets without usernames 2-87
 - timeout 2-88
 - UDP destination port 2-85
 - VSA compatibility mode 2-85
- call management
 - Analog-Encoding 2-28
 - Idle-Logout 2-210
 - Parallel-Dialing 2-330
 - System-Rmt-Mgmt 2-454
 - system-wide settings 2-452
 - Use-Trunk-Groups 2-507

- call routing
 - call type 2-89
 - Call-Route profile 2-88
 - Call-Route-Info 2-89
 - calls received on line/channel 2-351
 - calls received on telephone number 2-335
 - calls received on trunk group 2-491
 - default call type for inband T1 2-124
 - device address to route to 2-215
 - displaying the database 1-10
 - Entry-Number 2-159
 - sort methods 2-90
- call types 2-447
- callback security
 - Callback 2-75
 - Delay-Callback 2-127
 - Expect-Callback 2-164
- called-number authentication
 - Auth-ID-Fail-Return-Busy 2-53
 - Auth-Keep-User-Name 2-54
 - CalledNumber 2-77
 - CLID-Auth-Mode 2-101
 - Collect-Incoming-Digits 2-108
 - ID-Auth-Prefix 2-209
 - Overlap-Receiving 2-328
- Call-Log-Limit-Retry 2-84
- Callroute command 1-10
- CBCP callback 2-92
- C-Bit-ADM framer mode 2-181
- C-Bit-Parity framing mode 2-182
- C-Bit-PLCP framer mode 2-181
- cellular connections 2-93
- channel configuration 2-93
 - Call-Route-Info 2-89
 - Channel-Config 2-93
 - Channel-Config N 2-94
 - Channel-Usage 2-95
 - Nailed-Group 2-300
 - Phone-Number 2-335
 - Trunk-Group 2-491
- channel information, Error-Count 2-159
- channel state information 2-94
- channels
 - added 2-215
 - adding bandwidth from available 2-13
 - add-on numbers, and 2-335
 - CHAP, and 2-375
 - configuring E1 2-151
 - data calls using R2 signaling 2-176
 - D-channel (ISDN) signaling 2-124
 - distributing calls across cards for bundled 2-137
 - FT1-Caller 2-188
 - group number assigned to nailed-up 2-301
 - how the unit uses nailed-up 2-301

-
- L2TP receive window size for data 2-248
 - maximum number 2-275
 - minimum number 2-284
 - nailed-up 2-300
 - number removed when bandwidth changes 2-124
 - PAP-Token, and 2-375
 - PAP-Token-CHAP, and 2-262
 - password unit sends when adding to MP+ call 2-65
 - setting up a connection 2-69
 - SS7 incoming continuity checks for 2-214
 - SS7 outgoing continuity checks for 2-326
 - subtracting bandwidth 2-442
 - T1 2-455
 - T1 statistics 2-456
 - trunk groups, and 2-507
 - type of SS7 continuity checks 2-436
 - CHAP authentication
 - Auth-Type 2-62
 - bidirectional 2-71
 - Bi-Directional-Auth 2-71
 - Delay 2-127
 - Receive-Auth-Mode 2-375
 - Send-Auth-Mode 2-405
 - Send-Password 2-407
 - CIR timer 2-97
 - Clear command 1-12
 - CLeval command 1-13
 - CLID 2-100
 - CLID authentication
 - Auth-ID-Fail-Return-Busy 2-53
 - Auth-ID-Timeout-Return-Busy 2-53
 - Auth-Keep-User-Name 2-54
 - Auth-Rsp-Required 2-59
 - Caller-ID 2-78
 - CLID 2-99
 - CLID-Auth-Mode 2-100
 - CLID-Selection 2-101
 - CLID-Suppress 2-102
 - Collect-Incoming-Digits 2-108
 - ID-Auth-Prefix 2-209
 - Receive-Auth-Mode 2-375
 - Send-Auth-Mode 2-404
 - clocking
 - Clocking 2-106
 - Clock-Mode 2-107
 - Clock-Priority 2-107
 - Clock-Source 2-108
 - Divider 2-140
 - Exp 2-164
 - internal clock speed 2-164
 - Clock-Source command 1-13
 - clock-source settings
 - Clock-Priority 2-107
 - Clock-Source 2-108
 - Clr-History command 1-14
 - coaxial cable 2-161
 - codecs
 - A-Law encoding 2-28
 - encoding standard 2-28
 - G.711 2-25
 - Packet-Audio-Mode 2-329
 - preferred audio 2-329
 - selecting alternate 2-23
 - U-Law encoding 2-28
 - Code-level commands
 - Format 1-34
 - Fsck 1-34
 - commands
 - ? 1-4
 - ARptable 1-6
 - ATMlines 1-7
 - ATMSVCroute 1-8
 - Auth 1-9
 - Callroute 1-10
 - Clear 1-12
 - CLeval 1-13
 - Clock-Source 1-13
 - Clr-History 1-14
 - Connection 1-15
 - Date 1-15
 - Debug 1-16
 - Delete 1-16
 - Device 1-17
 - Dir 1-17
 - Dircode 1-19
 - DNStab 1-20
 - DS3link 1-21
 - Elsig 1-24
 - E1-Stats 1-25
 - Ether-Display 1-26
 - Fanstatus 1-27
 - Fatal-History 1-28
 - FE-Loop 1-29
 - Filtcache 1-30
 - Filterdisp 1-31
 - Format 1-34
 - Fsck 1-35
 - FWALLdblog 1-36
 - FWALLversion 1-37
 - Get 1-38
 - HDLC 1-41
 - Help 1-44
 - If-Admin 1-45
 - IGMP 1-46
 - IPcache 1-48
 - IP-Pools 1-49
 - IProute 1-49
 - Line 1-51
 - List 1-55
 - Load 1-56
 - Log 1-62

Index

D

commands (*continued*)

- LS 1-65
- Mkdir 1-66
- Modem 1-66
- MV 1-68
- Netstat 1-68
- Netware 1-75
- New 1-75
- NSlookup 1-78
- NVRAM 1-79
- OAMloop 1-80
- Open 1-81
- OSPF 1-82
- Ping 1-97
- Power 1-98
- PRIdisplay 1-99
- PrtCache 1-100
- Quiesce 1-101, 1-102
- Quit 1-102
- Read 1-103
- Redundant-Controller-Switch 1-105
- Refresh 1-106
- Remote 1-107
- Reset 1-109
- Rlogin 1-110
- RM 1-110
- Save 1-111
- Screen 1-113
- Set 1-114
- Show 1-116
- Slot 1-118
- snmpAuthPass 1-122
- snmpPrivPass 1-122
- Status 1-123
- SWANlines 1-124
- T1channels 1-125
- T1-Stats 1-127
- Telnet 1-128
- Terminal-Server 1-129
- Thermalstatus 1-130
- Tokencount 1-131
- Traceroute 1-133
- UDS3lines 1-135
- Uptime 1-136
- Userstat 1-138
- Userstat, customizing output 2-504
- Version 1-140
- View 1-141
- Whoami 1-142
- Write 1-142

configuration

- backup to file 1-111
- restoring from file 1-56

congestion-control settings

- CL1-Action 2-97
- CL1-Level 2-98
- CL2-Action 2-98

- CL2-Level 2-98
- Congestion-Control subprofile 2-110
- Congestion-Control-Type 2-111

Connection command 1-15

countries

- generating local call-progress tones 2-116
- identifying enabled 2-116

CSLIP

- Encapsulation-Protocol 2-156
- HDLC command 1-41

CSU

- CSU-Build-Out 2-117
- DSX-Line-Length 2-149
- Front-End-Type 2-186

D

D4 framing mode 2-182

DASS 2 signaling 2-251, 2-308, 2-418, 2-450

data calls 2-119

data rates

- Call-Info 2-80
- Data-Service 2-121
- maximum receive 2-393
- maximum transmit 2-496
- TX-Data-Rate-Limit 2-496

data services 2-121

data-rate limits

- RX-Data-Rate-Limit 2-393
- TX-Data-Rate-Limit 2-496

Date command 1-15

DCC-AESA format 2-177

D-channel signaling 2-124

deactivating digital modems 2-250

deactivating T1 lines or channels 2-270

Debug command 1-16

default routes

- client connections, for 2-409
- external routes summarized by 2-33
- ignoring 2-212
- IP 2-12, 2-102
- null address 2-128
- VOIP traffic, for 2-191

Delete command 1-16

DES-CBC mode 2-160

Device command 1-17

device information

- Device-Class 2-132
- Device-ID 2-132
- Device-State 2-132, 2-133
- Device-Summary 2-133
- Disabled-Count 2-139

-
- Inet-Profile-Type 2-216
 - Modem-Table-Index 2-287
 - Operational-Count 2-313
 - Reqd-State 2-380
 - Shelf 2-416
 - Shelf-Number 2-416
 - Slot 2-423
 - Slot-Address 2-423
 - Slot-Type 2-425
 - Total-Count 2-483
 - Up-Status 2-502
 - Device-Address, components of 2-242, 2-416, 2-423
 - DHCP settings
 - Active 2-11
 - Boot-File-Path 2-72
 - Client-WINS-Addr-Assign 2-105
 - Client-WINS-Primary-Addr 2-105
 - Client-WINS-Secondary-Addr 2-106
 - Default-Lease-Duration 2-125
 - Default-Max-Lease 2-125
 - Default-Pool 2-126
 - DHCP-Config 2-134
 - DHCP-Options 2-134
 - DHCP-Server 2-134
 - Ethernet-Address 2-163
 - Lease-Duration 2-251
 - Maximum-Leases 2-276
 - Pool-Number 2-341
 - Reply-Enabled 2-380
 - Server-Address 2-409
 - Static-Address 2-439
 - TFTP-Host-Name 2-474
 - Diagnostic-level commands
 - Callroute 1-10
 - Clock-Source 1-13
 - Debug 1-16
 - Device 1-17
 - DS3link 1-21
 - E1sig 1-24
 - E1-Stats 1-25
 - Ether-Display 1-26
 - FE-Loop 1-29
 - FWALLdblog 1-36
 - FWALLversion 1-37
 - If-Admin 1-45
 - NSlookup 1-78
 - OAMloop 1-80
 - Open 1-81
 - OSPF 1-82
 - Ping 1-97
 - PRIdisplay 1-99
 - PrtCache 1-100
 - Rlogin 1-109
 - Slot 1-118
 - T1-Stats 1-127
 - Telnet 1-128
 - Tokencount 1-131
 - Traceroute 1-133
 - dial number for outbound connections 2-135
 - DID numbers
 - All-Calls-Are-Fax 2-21
 - Fax-DID 2-168
 - Fax-Incoming-Call-Type 2-169
 - digital modems
 - Data-Service 2-122
 - Device-Address 2-131
 - Dialout-Allowed 2-135
 - Dialout-Configuration 2-136
 - Exclusive-Port-Routing 2-163
 - LAN-Modem 2-250
 - LAN-Modem-Enabled 2-250
 - Log 1-64
 - Max-Baud-Rate 2-272
 - Modem 1-66
 - Slot-Type 2-425
 - Switched-Call-Type 2-448
 - Telnet-Mode 2-470
 - V42/MNP 2-509
 - Dir command 1-17
 - Dircode command 1-19
 - direct-access dial-out 2-138
 - directed broadcast traffic, forwarding 2-139
 - DLCIs
 - link management 2-257
 - MFR bundles, and 2-283
 - sending traps 2-185
 - specifying for Frame Relay 2-140
 - specifying for Frame Relay Direct 2-183, 2-184
 - specifying name for endpoint 2-96
 - DNIS
 - All-Calls-Are-Fax 2-21
 - Auth-Keep-User-Name 2-54
 - CalledNumber 2-77
 - CLID-Auth-Mode 2-100
 - Collect-Incoming-Digits 2-108
 - E1-Inter-Digit-Timeout 2-152
 - Fax-DNIS 2-169
 - Gateway-Access-Number 2-190
 - ID-Auth-Prefix 2-209
 - Single-Dial-Enable 2-421
 - T1-Inter-Digit-Timeout 2-456
 - VoIP-Index 2-516
 - DNS lookups 1-78
 - DNS servers
 - Allow-As-Client-DNS-Info 2-22
 - Client-DNS-Addr-Assign 2-103
 - Client-DNS-Primary-Addr 2-103
 - Client-DNS-Secondary-Addr 2-104
 - Client-Primary-DNS-Server 2-104
 - Client-Secondary-DNS-Server 2-104
 - DNS-List-Size 2-142
-

Index

E

- DNS servers (*continued*)
 - DNS-Primary-Server 2-143
 - DNS-Secondary-Server 2-143
 - making client addresses available 2-103
 - making local servers available 2-22
 - presenting addresses 2-103
 - primary address to send 2-103, 2-104
 - primary for connected interfaces 2-143
 - primary for VRouter 2-143
 - secondary address to send 2-104
 - secondary for connected interfaces 2-143
 - secondary for VRouter 2-143
 - DNS settings
 - Allow-As-Client-DNS-Info 2-22
 - Auto-Update 2-64
 - Client-DNS-Addr-Assign 2-103
 - Client-DNS-Primary-Addr 2-103
 - Client-DNS-Secondary-Addr 2-104
 - Client-Primary-DNS-Server 2-104
 - Client-Secondary-DNS-Server 2-104
 - DNS-List-Attempt 2-141
 - DNS-List-Size 2-142
 - DNS-Local-Table 2-142
 - DNS-Primary-Server 2-143
 - DNS-Secondary-Server 2-143
 - Domain-Name 2-144
 - Host-Name 2-206
 - Sec-Domain-Name 2-397
 - Table-Config N 2-462
 - DNS tables
 - Auto-Update 2-64
 - configuring local 2-142
 - displaying 1-20
 - DNS-List-Size 2-142
 - DNS-Local-Table 2-142
 - DNStab command 1-20
 - IP-Address 2-222
 - maximum number of hosts 2-142
 - returning multiple hostnames 2-141
 - updating automatically 2-64
 - DNStab command 1-20
 - DoS attacks, protecting against 2-139
 - DPNSS signaling 2-251, 2-308, 2-418, 2-450
 - DS3-ATM card, code image in tar file 2-146
 - DS3-ATM framer modes 2-181
 - DS3-ATM lines
 - Activation 2-11
 - Aggregate 2-18
 - Bit-Rate 2-72
 - Call-Route-Info 2-89
 - DS3-ATM profile 2-146
 - Framer-Mode 2-181
 - High-Tx-Output 2-200
 - Line-Config 2-252
 - Loopback 2-266
 - Max-Burst-Size 2-273
 - Nailed-Group 2-300
 - Name 2-301
 - Peak-Rate 2-333
 - Priority 2-355
 - Traffic-Shapers 2-484
 - Traffic-Shapers N 2-485
 - Trunk-Group 2-491
 - VPI-VCI-Range 2-517
 - DS3link command 1-21
 - DSP
 - DSP-Portion 2-147
 - ESI 2-160
 - HO-DSP 2-201
 - SEL 2-402
 - DSX 2-186
 - DTE-monitored event count 2-300
 - DTMF digits, decoding 2-108, 2-147
 - DTMF R2 signaling 2-418
 - DTMF tones
 - call progress 2-196
 - filtering 2-149
 - duplex mode 2-150
 - DWS calls 2-298
- ## E
- E.164 addresses
 - Address-Prefix 2-13
 - AFI 2-17
 - ATM-Address 2-43
 - CLID 2-99
 - FR-Address 2-179
 - Numbering-Plan 2-311
 - Subaddress 2-442
 - E1 card, code image in tar file 2-3
 - E1 FrameLine card, code image in tar file 2-501
 - E1 lines 2-480
 - Answer-Delay 2-29
 - Back-To-Back 2-66
 - Caller-ID 2-78
 - Call-Route-Info 2-89
 - Channel-Config 2-93
 - Channel-Config N 2-94
 - Channel-Usage 2-95
 - Clock-Priority 2-107
 - Clock-Source 2-108
 - default call type 2-124
 - E1 profile 2-151
 - E1-Inter-Digit-Timeout 2-152
 - Enabled 2-154
 - Frame-Type 2-182
 - Front-End-Type 2-186

-
- Group-B-Answer-Signal 2-194
 - Group-B-Busy-Signal 2-195
 - Group-B-Collect-Signal 2-195
 - Group-II-Signal 2-194
 - Incoming-Call-Handling 2-214
 - Incoming-Procedure 2-214
 - Inter-Digit-Time-Out 2-219
 - ISDN-Emulation-Side 2-241
 - Layer3-End 2-251
 - Line-Interface 2-253
 - Loop-Avoidance 2-266
 - Nailed-Group 2-300
 - NL-Value 2-308
 - Number-Complete 2-311
 - Outgoing-Procedure 2-326
 - Overlap-Receiving 2-328
 - Phone-Number 2-335
 - Preferred-Source 2-351
 - PRI-Prefix-Number 2-355
 - SS7-Continuity 2-436
 - T302-Timer 2-458
 - T-Online-Type 2-481
 - Trailing-Digits 2-486
 - E1 MFC-R2 signaling 2-311
 - E164-AESA format 2-177
 - E1sig command 1-24
 - E1-Stats command 1-25
 - E3-ATM lines
 - Aggregate 2-18
 - Bit-Rate 2-72
 - Call-Route-Info 2-89
 - E3-ATM profile 2-151
 - Enabled 2-154
 - Framer-Mode 2-181
 - High-Tx-Output 2-200
 - Line-Config 2-252
 - Loopback 2-266
 - Max-Burst-Size 2-273
 - Nailed-Group 2-300
 - Name 2-301
 - Peak-Rate 2-333
 - Physical-Address 2-336
 - Priority 2-355
 - Traffic-Shapers 2-484
 - Traffic-Shapers N 2-485
 - Trunk-Group 2-491
 - VPI-VCI-Range 2-517
 - early ringback tone 2-152
 - enabling features 2-154
 - encapsulation methods 2-156
 - encapsulation protocols 2-156
 - errors on T1 channels 2-159
 - escape sequences 2-157
 - ESF framing mode 2-182
 - ESI 2-147, 2-160
 - ESP 2-160
 - ESP-v2 2-242
 - Ether-Display command 1-26
 - Ethernet address 2-163
 - Ethernet interface types 2-161
 - Ethernet interfaces
 - Ethernet profile 2-162
 - MAC address and link state 2-161
 - port speed 2-281
 - type of physical 2-161
 - Ethernet packets 1-26
 - Ethernet-2 card, code image in tar file 2-158
 - exclusive port routing 2-163
 - external metrics
 - Cost 2-115
 - RIP-ASE-Type 2-384
- F**
- Fanstatus command 1-27
 - fantray
 - Alarm-Temperature-Trigger 2-20
 - Fantray-Lownoise-RPM 2-168
 - high-temperature threshold 2-199
 - High-Temperature-Trigger 2-199
 - low noise speed 2-168
 - low-temperature threshold 2-268
 - Low-Temperature-Trigger 2-268
 - Operation-Mode 2-314
 - RPM of 2-168
 - Thermal 2-474
 - fatal error log 1-14, 1-28
 - Fatal-History command 1-28
 - FDL protocol 2-170
 - FE-Loop command 1-29
 - FGD signaling 2-170
 - Filtcache command 1-30
 - filter caches 1-30, 2-125
 - Filterdisp command 1-31
 - filters
 - Action 2-10
 - Add-Metric 2-13
 - applying SAP to connection 2-394
 - Call-Filter 2-79
 - Comp-Neq 2-109
 - Data-Filter 2-120
 - Default-Filter-Cache-Time 2-125
 - Dest-Address 2-128
 - Dest-Address-Mask 2-129
 - Dest-Net-Address 2-129
 - Dest-Node-Address 2-130
 - Dest-Port 2-130
-

Index

F

filters (*continued*)

- Dest-Socket 2-130
 - Dst-Port-Cmp 2-148
 - Dst-Socket-Cmp 2-148
 - enabling SAP 2-510
 - Filter profile 2-171
 - Filter-Name 2-171
 - Filter-Persistence 2-172
 - Filter-Required 2-172
 - Forward 2-178
 - Gen-Filter 2-191
 - input 2-217, 2-218
 - Input-Filters 2-217
 - Input-Filters N 2-218
 - IP-Filter 2-224
 - IPX-Filter 2-233
 - Len 2-252
 - Mask 2-271
 - More 2-288
 - Offset 2-313
 - output 2-327
 - Output-Filters 2-327
 - Output-Filters N 2-327
 - Output-IPX-SAP-Filters 2-328
 - persistence across state changes 2-172
 - Precedence 2-350
 - Protocol 2-361
 - Route-Address 2-388
 - Route-Filter 2-390
 - Route-Filter subprofile 2-390
 - Route-Mask 2-391
 - SAP 2-218, 2-239, 2-394
 - Server-Name 2-410
 - Server-Type 2-412
 - Source-Address 2-432
 - Source-Address-Mask 2-432
 - Source-Port 2-433
 - Src-Net-Address 2-434
 - Src-Node-Address 2-434
 - Src-Port-Cmp 2-435
 - Src-Socket 2-435
 - Src-Socket-Cmp 2-436
 - TCP-Estab 2-467
 - TOS 2-482
 - TOS-Options 2-482
 - Type-of-Service 2-482, 2-498
 - types 2-497
 - Valid-Entry 2-510
 - Value 2-510
- Finger queries 2-173, 2-504
- firewalls
- enabled 2-174
 - Firewall profile 2-173
- Flash
- file-system checking a card 1-34
 - formatting a card 1-34
 - listing the contents of a card 1-19
 - restoring configuration 1-56
 - saving configurations to a file 1-111
- flow control methods 2-175
- Format command 1-34
- fractional T1 calls 2-188
- frame length 2-179
- Frame Relay connections 2-187
- Active 2-11
 - Billing-Number 2-72
 - Call-By-Call-ID 2-76
 - Called-Number-Type 2-77
 - Circuit-Name 2-96
 - circuits 2-96, 2-97
 - Circuit-Type 2-97
 - configuring MFR 2-297
 - configuring the datalink 2-180
 - DCEN392-Val 2-123
 - DCEN393-Val 2-123
 - DLCI 2-140
 - DLCIs 2-140
 - DLCIs for redirect connections 2-184
 - enabling 2-154
 - Encapsulation-Protocol 2-156
 - FR-08-Mode 2-178
 - FR-Address 2-179
 - Frame-Relay profile 2-180
 - Frame-Relay-Enabled 2-181
 - Frame-Relay-Profile 2-181
 - FR-Answer 2-183
 - FR-Direct-DLCI 2-183
 - FR-Direct-Enabled 2-184
 - FR-Direct-Profile 2-184
 - FR-DLCI 2-184
 - FR-Link-Type 2-185
 - FR-Name 2-186
 - FR-Profile 2-187
 - link-management options 2-257
 - Link-Mgmt-DLCI 2-257
 - logical interfaces 2-258
 - Max-Bundle-Members 2-273
 - MFR-Bundle-Name 2-283
 - MFR-Bundle-Type 2-284
 - Min Bandwidth 2-284
 - MRU 2-290
 - N391-Val 2-299
 - N392-Val 2-299
 - N393-Val 2-300
 - Nailed-Mode 2-301
 - Nailed-Up-Group 2-301
 - PVCs 2-97
 - redirect 2-181, 2-184
 - Station 2-440
 - SVCs 2-97
 - T391-Val 2-461
 - T392-Val 2-461

framed protocol, requiring 2-179

framer modes

 C-Bit-ADM 2-181

 C-Bit-PLCP 2-181

framer rates 2-182

framing modes 2-182

 2DS 2-182

 C-Bit-Parity 2-182

 D4 2-182

 ESF 2-182

 G703 2-182

 M13 2-182

framing on T1 or E1 lines 2-182

front-end types

 CSU 2-186

 DSX 2-186

 Long-Haul 2-186

 Short-Haul 2-186

Fsck command 1-35

FWALLdblog command 1-36

FWALLversion command 1-37

G

G.711 U-Law encoding 2-513

G.729 encoding 2-513

G703 framing mode 2-182

gatekeepers

 primary 2-189

 secondary 2-190

 time interval between registration attempts 2-190

gateways

 address 2-191

 default 2-102

 DTMF tones, and 2-149

 ICD for softswitch 2-220, 2-437

 ringback tone, and 2-152

 secondary signaling 2-397, 2-398

 security 2-494

 selecting preferred codec 2-23, 2-25

 telephone number of remote device 2-168

 unavailable 2-492

 voice announcements, and 2-196

 VoIP 2-490

Get command 1-38

Goertzel input samples 2-147

group numbers

 Nailed-Group 2-300

 Nailed-Groups 2-300

 Nailed-Up-Group 2-301

group-B signal

 as busy signal 2-195

 as response to collect call 2-195

 before incoming call is answered 2-194

group-II signal 2-194

H

H.323

 call processing 2-421

 gatekeeper functions 2-189, 2-190

 Gatekeeper-IP 2-189

 Gatekeeper-IP-Sec 2-190

 Idle-Timer 2-211

 supported audio codecs 2-23

 voice announcements 2-196

hardware handshake (serial port) 2-175

hardware revision level 2-196

hardware rework count 2-196

HDLC command 1-41

HDLC-NRM settings

 Async-Drop 2-36

 Encapsulation-Protocol 2-156

 HDLC-NRM-Answer 2-197

 HDLC-NRM-Options 2-198

 Poll-Rate 2-338

 Poll-Retry-Counter 2-338

 Poll-Timeout 2-338

 Primary 2-352

 SDTN-Packets-Server 2-396

 SNRM-Response-Timeout 2-430

 SNRM-Retry-Counter 2-430

 Station-Poll-Address 2-441

Hello packets

 Dead-Interval 2-124

 Hello-Interval 2-199

 Hello-Timer 2-199

 Poll-Interval 2-338

Help command 1-44

help text 1-4, 1-44

HO-DSP 2-147, 2-201

hops 2-202

host routes, suppressing 2-444

hosts

 address for trap-PDUs 2-206

 displayed in menu mode 2-206

 displayed in terminal-server menu 2-206

 DNS hostname 2-203

 Ext-Tsrv 2-165

 first login 2-203

 fourth login 2-205

 name 2-206

 port for Telnet 2-345

 second login 2-204

 terminal-server menu, in 2-207

 third login 2-204

 type of service for 2-413

Hybrid Access II card, code image in tar file 2-197

I

ICD for softswitch 2-220, 2-437

ICD-AESA format 2-177

ICMP 2-315, 2-361

- destination-unreachable packets 2-406
- echo requests 1-97, 2-209
- redirect packets 2-212

IDI 2-209

idle indicator 2-210

idle sessions

- IP or IPX 2-210
- Telnet 2-210
- WAN 2-210

idle time, monitoring 2-210, 2-493

idle tunnels 2-210

If-Admin command 1-45

IGMP command 1-46

immediate mode 2-213

inband signaling 1-52

incoming calls

- additional called-number information 2-458
- ANI processing 2-368
- ARA 2-31
- ATM address 2-213
- authenticating with CLID 2-100
- authenticating with DNIS 2-100
- authentication protocol for 2-404
- CBCP methods 2-285
- CLID present for 2-100
- default call type 2-124
- determining which CLID to use 2-101
- distributing across host cards 2-91, 2-137
- dynamic IP address assignment 2-35
- enabling 2-30
- framed 2-179
- group-B signal 2-194
- header prediction 2-513
- IP fax 2-21, 2-168, 2-169
- maximum number of minutes connected 2-273
- overlap receiving 2-328
- processing 2-214, 2-220
- R2 signaling for 2-311
- requiring profile for 2-360
- sharing profiles 2-415
- single-file or parallel 2-421
- system defaults 2-28
- treated as voice 2-90
- types of service 2-302
- validating 2-502

index, for call routing 2-215

Interface-Address, components 2-219

interfaces

- how addressed 2-227
- IP on Ethernet 2-221
- remote station name 2-440

IP calls, default settings 2-222

IP direct 2-222

IP fax

- All-Calls-Are-Fax 2-21
- Allow-Coder-Fallback 2-24
- Dialer-Type 2-135
- fax servers 2-170
- Fax-DID 2-168
- Fax-DNIS 2-169
- Fax-Incoming-Call-Type 2-169
- Fax-Servers 2-170
- handling incoming calls as 2-21
- Idle-Timer 2-211
- Incoming-Fax-Port 2-214
- IP-Fax profile 2-223
- IP-Fax-Enabled 2-223
- login name 2-410
- Outgoing-Fax-Port 2-326
- password 2-411
- Server-Login 2-410
- Server-Password 2-411
- TCP port for incoming calls 2-214
- TCP port for outgoing calls 2-326
- trunk groups 2-312

IP interface table 1-68

IP interfaces

- Active 2-11
- configuration options 2-226
- Data-IP-Address 2-120
- IP-Address 2-221
- Management-Only-Interface 2-270
- multicasting 2-292
- soft 2-120, 2-221, 2-452
- System-IP-Addr 2-452
- VRouters, and 2-519

IP packet forwarding, card-to-card 2-229

IP packets, with source-route option set 2-145

IP route caches

- enabled 2-229
- size limit 2-230

IP routes

- Active-Route 2-12
- ASE-Tag 2-34
- ASE-Type 2-34
- Cost 2-115
- Dest-Address 2-128
- Gateway-Address 2-191
- Inter-VRouter 2-220
- IP-Options 2-227
- IP-Route profile 2-229

-
- Metric 2-283
 - Name 2-301
 - Preference 2-351
 - Private-Route 2-356
 - Third-Party 2-476
 - VRouter 2-518
 - IP routing table 1-68
 - IPcache command 1-48
 - IPDC 2-114
 - IProute command 1-49
 - IPSec settings
 - Active 2-11
 - AH-Type 2-18
 - authentication transforms 2-18
 - Auth-Key 2-54
 - Auth-Type 2-62
 - Encap-Mode 2-155
 - encapsulation mode 2-155
 - ESP-Type 2-160
 - IPSec profile 2-231
 - IPSec-Profile 2-231
 - IV-Len 2-242
 - Key 2-243
 - Key2 2-243
 - Key3 2-244
 - Recv-AH 2-376
 - Recv-ESP 2-376
 - Replay-Protection 2-380
 - Send-AH 2-404
 - Send-ESP 2-405
 - SPI 2-433
 - Tunnel-Address 2-494
 - Version 2-511
 - IPX header compression 2-235
 - IPX routes
 - Active-Route 2-12
 - Dest-Network 2-129
 - Hops 2-202
 - IPX-Dialin-Pool 2-232
 - IPX-Route profile 2-237
 - IPX-Routing-Enabled 2-238
 - Name 2-301
 - network numbers 2-304
 - Profile-Name 2-359
 - Server-Node 2-410
 - Server-Socket 2-411
 - Server-Type 2-412
 - static 2-237
 - Ticks 2-477
 - IPX SAP filters 2-394
 - input 2-218
 - Input-IPX-SAP-Filters 2-218
 - IPX-SAP-Filter-Name 2-239
 - output 2-328
 - Output-IPX-SAP-Filters 2-328
 - Type-Filter 2-498
 - Valid-Filter 2-510
 - IPX settings
 - global 2-234
 - interface 2-235
 - IPX SAP behavior 2-394
 - IPX SAP filters 2-410, 2-412, 2-498, 2-510
 - IPX-Answer 2-232
 - IPX-Dialin-Pool 2-232
 - IPX-Frame 2-233
 - IPX-Header-Compression 2-235
 - IPX-Interface 2-235
 - IPX-Net-Number 2-236
 - IPX-Options 2-237
 - IPX-Route 2-237
 - IPX-Type-20 2-240
 - Net-Alias 2-303
 - network numbers 2-236, 2-304
 - packet frame types 2-233
 - packets 2-240
 - Peer-Mode 2-334
 - routes 2-410, 2-411, 2-412, 2-477
 - SAP filters 2-239
 - ISDN User-User IE
 - User-User-Info 2-505
 - User-User-Infolen 2-506
- ## J
- jitter buffer
 - adaptive mode for VoIP calls 2-153
 - disabled 2-329, 2-420
 - dynamic 2-420
 - initial size 2-217
 - maximum size 2-276
- ## L
- L2F tunnels
 - Assignment-ID 2-35
 - Client-Auth-ID 2-102
 - L2F-Mode 2-245
 - L2F-Retry-Count 2-245
 - L2F-Retry-Interval 2-245
 - L2F-System-Name 2-246
 - L2F-Tunnel-Secret 2-246
 - Primary-Tunnel-Server 2-354
 - Profile-Type 2-360
 - Secondary-Tunnel-Server 2-398
 - Server-Auth-ID 2-409
 - Server-Endpoint 2-409
 - Shared-Secret 2-416
 - Tunneling-Protocol 2-494
 - Tunnel-Options 2-494
 - Tunnel-Server 2-495
-

Index

M

L2TP tunnels

- Assignment-ID 2-35
- Client-Auth-ID 2-102
- configuration 2-247
- Control-Connect-Establish-Timer 2-114
- First-Retry-Timer 2-174
- Hello-Timer 2-199
- L2TP-Auth-Enabled 2-247
- L2TP-Mode 2-248
- L2TP-RX-Window 2-248
- L2TP-System-Name 2-248
- L2-Tunnel-Global 2-249
- LAC-Incoming-Call-Timer 2-249
- Primary-Tunnel-Server 2-354
- Profile-Type 2-360
- Retry-Count 2-381
- Secondary-Tunnel-Server 2-398
- Server-Auth-ID 2-409
- Server-Endpoint 2-409
- Shared-Secret 2-416
- Tunneling-Protocol 2-494
- Tunnel-Options 2-494
- Tunnel-Server 2-495

LAN interfaces, physical state 2-258

leases

- default period 2-125
- maximum number of renewals 2-125, 2-276
- number of seconds valid 2-251

Line command 1-51

line information

- channel error counts 2-159
- Channel-State 2-94, 2-95

line-encoding methods 2-156

Line-State 2-255

link states

- Link-State 2-258
- Link-State-Enabled 2-258

link types, Frame Relay 2-258

List command 1-55

Load command 1-56

loading code 1-56

local-echo mode 2-261

Log command 1-62

log messages 2-450

- call information 2-80
- level displayed for a user login 2-264

logins

- Banner 2-68
- Banner N 2-68
- Buffer-Chars 2-74
- Clear-Screen 2-99
- enabling Ping 2-337
- enabling PPP 2-347
- enabling Rlogin 2-387

- enabling SLIP 2-422

- enabling SLIP-BOOTP 2-422

- enabling TCP command 2-466

- enabling Telnet 2-469

- enabling Traceroute command 2-484

- Idle-Logout 2-210

- level of log messages displayed 2-264

- network host 2-203

- Password-Prompt 2-333

- prompt 2-264

- start with Menu mode 2-438

- System-Password 2-454

- TCP port for logins 2-342

- TCP-Timeout 2-468

- Terminal-Type 2-473

- Third-Login-Prompt 2-475

- Third-Prompt-Sequence 2-476

- timeout 2-265

logs

- Auxiliary-Syslog 2-64

- Facility 2-167

- Host 2-203

- Log profile 2-263

- Log-Software-Version 2-265

- Port 2-342

- Syslog-Enabled 2-450

- Syslog-Level 2-451

loopback test 2-266, 2-304

LS command 1-65

LSAs

- ASE-Type 2-34

- displaying information about 1-82

- OSPF command 1-82

- OSPF-Approaching-Overflow-Enabled 2-315

- OSPF-LSDB-Overflow-Enabled 2-319

- OSPF-MaxAgeLSA-Enabled 2-319

- OSPF-OriginateLSA-Enabled 2-321

- Retransmit-Interval 2-381

- Transit-Delay 2-487

M

M13 framing mode 2-182

MAC addresses

- ESI 2-160

- Ether-Info 2-161

- Ethernet-Address 2-163

- IP-Address 2-222

- MAC-Address 2-270

- Proxy-Mode 2-364

- Static-Address 2-439

MAC header, IPX-Frame 2-233

management-only interface 2-270

MAXLink client software 2-276

-
- MD5
 - MD5-Authen-Key 2-280
 - MD5-Auth-Key 2-281
 - mode 2-63
 - memory, clearing 1-78
 - menu mode
 - configuring 2-282
 - default for logins 2-438
 - description of hosts 2-473
 - obtaining from RADIUS 2-379
 - metrics
 - external 2-384
 - maximum for transaction server 2-283
 - Partly-Congested-Metric 2-331
 - RIP 2-283
 - RIP-style 2-391
 - Routing-Metric 2-391
 - Shutdown-Metric 2-416
 - transaction server 2-309, 2-310
 - Type-1 2-384
 - Type-2 2-384
 - WAN links, for 2-391
 - MFR settings
 - Active 2-11
 - configuring 2-297
 - Max-Bundle-Members 2-273
 - MFR-Bundle-Name 2-283
 - MFR-Bundle-Type 2-284
 - Multi-Link-FR 2-297
 - Mkdir command 1-66
 - Modem command 1-66
 - modems
 - 7-Even 2-2
 - Cell-Level 2-92
 - deactivating 2-286
 - dialout feature 2-286
 - Dialout-Allowed 2-135
 - Dialout-Configuration 2-136
 - Direct-Access 2-138
 - disable mode 2-286
 - Modem-Configuration 2-285
 - Modem-Table-Index 2-287
 - Modem-Transmit-Level 2-287
 - modulation 2-287
 - V42/MNP 2-509
 - MP connections
 - BACP-Enable 2-67
 - Base-Channel-Count 2-69
 - configuring for a WAN link 2-289
 - defaults when answering calls 2-288
 - Digital-Call-Routing-Sort-Method 2-137
 - Encapsulation-Protocol 2-156
 - Link-Compression 2-256
 - Maximum-Channels 2-275
 - Minimum-Channels 2-284
 - MP-Answer 2-288
 - MP-Options 2-289
 - PPP-Answer 2-348
 - PPP-Options 2-349
 - Receive-Auth-Mode 2-375
 - Send-Auth-Mode 2-404
 - Target-Utilization 2-465
 - MP+ connections
 - Add-Persistence 2-13
 - authentication for 2-65
 - Aux-Send-Password 2-65
 - Bandwidth-Monitor-Direction 2-67
 - Base-Channel-Count 2-69
 - Call-Type 2-91
 - configuring for a WAN link 2-290
 - Decrement-Channel-Count 2-124
 - defaults when answering calls 2-289
 - Digital-Call-Routing-Sort-Method 2-137
 - Dynamic-Algorithm 2-150
 - Encapsulation-Protocol 2-156
 - Increment-Channel-Count 2-215
 - Link-Compression 2-256
 - MPP-Answer 2-289
 - MPP-Options 2-290
 - Nailed-Groups 2-300
 - PPP-Answer 2-348
 - PPP-Options 2-349
 - Receive-Auth-Mode 2-375
 - Robbed-Bit-Mode 2-388
 - Seconds-History 2-399
 - Send-Auth-Mode 2-404
 - Sub-Persistence 2-442
 - MRU
 - prefragmenting incoming packets 2-177
 - specifying 2-290
 - MS-CHAP authentication
 - Bi-Directional-Auth 2-71
 - Receive-Auth-Mode 2-375
 - Send-Auth-Mode 2-405
 - MTU
 - lower than actual path MTU 2-291
 - specifying 2-291
 - multicast
 - configuring a multicast interface 2-292, 2-297
 - delay before forwarding IGMP message 2-293
 - MBONE-LAN-Interface 2-279
 - MBONE-Profile 2-280
 - Multicast-Allowed 2-292
 - Multicast-Forwarding 2-292
 - Multicast-Group-Leave-Delay 2-293
 - Multicast-Hbeat-Addr 2-293
 - Multicast-Hbeat-Alarm-Threshold 2-294, 2-295, 2-296
 - Multicast-Hbeat-Number-Slot 2-294
 - Multicast-Hbeat-Src-Addr 2-295
 - Multicast-Interface-IP-Address 2-296
-

Index

N

multicast (*continued*)

- Multicast-Member-Timeout 2-296
- Multicast-Rate-Limit 2-297
- Non-Multicast 2-310
 - specifying destination address 2-292

MultiVoice

- configured for H.323 processing 2-421
- country-specific call tones 2-116
- gatekeeper functions 2-189, 2-190
- Gatekeeper-Keepalive 2-190
- H.323 call processing 2-421
- jitter buffer mode 2-153
- Max-Rate 2-277
- passing call-progress tones 2-118
- PIN 2-518
- reregistering with MVAM 2-353
- Send-ICMP-Dest-Unreachable, and 2-406
- Sequential-Calls-Enable 2-407
- voice announcements 2-196

MultiVoice gatekeeper

- generating trap when reregistering 2-516
- registering with 2-79
- routing calls to available MultiVoice gateways 2-492

MultiVoice gateway

- Alert-Progress-Indicator 2-21
- Bearer-Capability 2-70
- Cause-Code-Transparency 2-92
- deactivating trunk 2-492
- disabling reception of UDP packets 2-476
- encoding of voice announcements 2-513
- FGD signaling 2-170
- generating trap when gatekeeper changes 2-516
- Gk-Mlg-Control 2-192
- hairpin dialing 2-79
- Inter-Digit-Time-Out 2-219
- maximum number of registration attempts 2-378
- Number-Complete 2-311
- polling a remote device 2-81
- Proceed-Progress-Indicator 2-358
- RT24 codec, and 2-329
- Signaling-Mode 2-418
- single-stage dialing 2-421
- transparent modem mode 2-189
- trunk groups 2-492
- unavailable 2-492

MV command 1-68

MVAM

- Gatekeeper-IP-Sec 2-190
- Gatekeeper-Keepalive 2-190
- Gk-Mlg-Control 2-192
- Primary-Retrieves 2-353
- registration attempts 2-379
- Registration-Retry-Timer 2-379
- Trunk-Prefix-Enable 2-492

N

nailed-up connections

- Backup 2-66
- Call-Type 2-91
- Nailed-Group 2-300
- Nailed-Groups 2-300
- Nailed-Mode 2-301
- Perm-Conn-Upd-Mode 2-334
- Temporary-Route 2-471

nailed-up interfaces

- Admin-State-Perm-If 2-15
- backup 2-66

names 2-301

NBMA networks 2-305

NetBIOS servers

- primary 2-303
- secondary 2-303

Netstat command 1-68

Netware command 1-75

NetWare servers

- socket number 2-411
- type 2-412

network numbers

- AppleTalk 2-39
- IPX 2-236, 2-240, 2-303, 2-304
- NetWare server 2-129, 2-240
- virtual IPX 2-232

network ranges

- Atalk-Dialin-Pool-End 2-36
- Atalk-Dialin-Pool-Start 2-37
- Atalk-Net-End 2-38
- Atalk-Net-Start 2-38
- Atalk-Static-NetEnd 2-41
- Atalk-Static-NetStart 2-41
- beginning of 2-37, 2-38, 2-41, 2-200
- end of 2-36, 2-38, 2-41, 2-200
- Hint-Net-Hi 2-200
- Hint-Net-Lo 2-200

network-management license, enabled 2-305

New command 1-75

NFAS

- NFAS-Group-ID 2-306
- NFAS-ID 2-308
- signaling 1-52

nonseed routers

- Atalk-Interface 2-37
- Atalk-Router 2-39
- Hint-Net-Hi 2-200
- Hint-Net-Lo 2-200
- Hint-Net-Node 2-201
- Net-Number 2-304

NSlookup command 1-78

numbered interfaces 2-303
 IF-Remote-Address 2-212
 Local-Address 2-260
 Net-Alias 2-303

NVRAM command 1-79

O

OAMloop command 1-80

OC3-ATM

 Line-Config 2-253

OC3-ATM lines

 Aggregate 2-18
 Bit-Rate 2-72
 Call-Route-Info 2-89
 Clock-Priority 2-107
 Clock-Source 2-108
 Enabled 2-154
 Framer-Mode 2-181
 Framer-Rate 2-182
 Line-Config 2-252
 Loopback 2-266
 Loop-Timing 2-266
 Max-Burst-Size 2-273
 Nailed-Group 2-300
 OC3-ATM profile 2-313
 Peak-Rate 2-333
 Priority 2-355
 RX-Cell-Payload-Descramble-Disabled 2-392
 RX-Descramble-Disabled 2-393
 Traffic-Shapers 2-484
 Traffic-Shapers N 2-485
 Trunk-Group 2-491
 TX-Cell-Payload-Scramble-Disabled 2-496
 TX-Scramble-Disabled 2-497
 VPI-VCI-Range 2-517

Open command 1-81

OSPF areas

 Area 2-32
 Area-Type 2-33
 Authen-Type 2-51
 displaying information about 1-82, 1-84
 specifying 2-32
 types 2-33

OSPF command 1-82

OSPF settings

 Active 2-11
 Area 2-32
 Area-Type 2-33
 AS-Boundary-Router 2-33
 ASE preferences 2-315
 ASE-Tag 2-34
 ASE-Type 2-34
 Authen-Type 2-51

Auth-Key 2-54

 configuring 2-321

 configuring on a WAN link 2-321

Cost 2-115

Dead-Interval 2-124

DR-Capable 2-144

Enable 2-154

enabling on Ethernet 2-314

global preferences for OSPF routes 2-322

Hello-Interval 2-199

Host-Name 2-206

Key-ID 2-244

MD5-Authen-Key 2-280

MD5-Auth-Key 2-281

Network-Type 2-305

Non-Multicast 2-310

OSPF profile 2-314

OSPF-ASE-Pref 2-315

OSPF-Global 2-317

OSPF-NBMA-Neighbor 2-320

OSPF-Pref 2-322

Poll-Interval 2-338

Priority 2-355

Retransmit-Interval 2-381

routes learned from RIP 2-384

tagging routes learned from RIP 2-386

Transit-Delay 2-487

outgoing calls

 Answer-Originate 2-30

 calling-party address in 2-219

 Call-Route 2-88

 enabling 2-30

 Expect-Callback 2-164

 Insert-Calling-Party-Addr 2-219

 Phone-Number 2-335

 Substitute-Recv-Name 2-442

 Use-Trunk-Groups 2-507

overlap receiving 2-328

P

PAP authentication

 Auth-Type 2-62

 Bi-Directional-Auth 2-71

 Delay 2-127

 Max-PAP-Auth-Retry 2-276

 Receive-Auth-Mode 2-375

 Send-Auth-Mode 2-404

 Send-Password 2-407

PAP-Token authentication

 Local-Profiles-First 2-262

 Receive-Auth-Mode 2-375

PAP-Token-CHAP authentication

 Aux-Send-Password 2-65

 Local-Profiles-First 2-262

Index

P

- passwords
 - additional channels 2-65
 - ATMP 2-202
 - CLID 2-99
 - DNIS 2-140
 - fax server 2-411
 - Password 2-331
 - Password-For-Direct-Access 2-332
 - Password-Profile 2-333
 - Password-Prompt 2-333
 - PPP connections, for 2-407
 - Recv-Password 2-377
 - Send-Password 2-407
 - Server-Password 2-411
 - System-Password 2-454
 - Telnet 2-471
 - Telnet-Password 2-471
 - terminal-server logins, for 2-454
 - viewing 2-25
- permissions
 - Active-Enabled 2-12
 - Allow-Code 2-23
 - Allow-Diagnostic 2-24
 - Allow-Password 2-25
 - Allow-System 2-26
 - Allow-Termserv 2-27
 - Allow-Update 2-27
 - authenticating a profile 1-9
 - Auto-Logout 2-63
 - Whoami 1-142
- PHS 2-336
- physical addresses 2-336
- physical interfaces
 - Admin-State-Phys-If 2-15
- Physical-Address, components of 2-242, 2-416, 2-423
- Ping command 1-97, 2-337
- polling
 - Poll-Interval 2-338
 - Poll-Rate 2-338
 - Poll-Retry-Counter 2-338
 - Poll-Timeout 2-338
- pool chaining 2-339
- port for immediate login 2-342
- port redirection
 - Port-Number 2-346
 - Port-Redirect-Options 2-347
 - Redirect-Address 2-377
- POST 2-241
- Power command 1-98
- power supplies 1-98
- PPP
 - authentication for 2-139, 2-375, 2-407
 - configuring for a WAN link 2-349
 - defaults when answering calls 2-348, 2-509
 - line-quality monitoring 2-268, 2-269
 - terminal-server logins, in 2-347
- PPP connections
 - Allow-As-Client-DNS-Info 2-22
 - AppleTalk routing, and 2-40
 - Assign-Count 2-35
 - Auth-Send67 2-60
 - backup 2-66
 - Bandwidth-Monitor-Direction 2-67
 - Bi-Directional-Auth 2-71
 - CBCP-Enabled 2-92
 - Client-DNS-Primary-Addr 2-103
 - Client-DNS-Secondary-Addr 2-104
 - Client-Primary-DNS-Server 2-104
 - Client-Secondary-DNS-Server 2-104
 - Delay 2-127
 - Direct 2-138
 - Disconnect-On-Auth-Timeout 2-139
 - Encapsulation-Protocol 2-156
 - FR-DLCI 2-184
 - Info 2-216
 - IP-Add-Msg 2-221
 - Link-Compression 2-256
 - LQM 2-268
 - LQM-Maximum-Period 2-269
 - LQM-Minimum-Period 2-269
 - Mode-Callback-Control 2-285
 - MRU 2-290
 - MTU 2-291
 - PPP command 2-347
 - PPP-Answer 2-348
 - PPP-Mode-Configuration 2-349
 - PPP-Options 2-349
 - Receive-Auth-Mode 2-375
 - Recv-Password 2-377
 - Robbed-Bit-Mode 2-388
 - Send-Auth-Mode 2-404
 - Send-Password 2-407
 - Split-Code-Dot-User-Enabled 2-434
 - Station 2-440
 - Substitute-Recv-Name 2-442
 - Substitute-Send-Name 2-443
 - Trunk-Group-Callback-Control 2-492
- PPTP tunnels
 - L2-Tunnel-Global 2-249
 - PPTP-Enabled 2-350
 - Server-Endpoint 2-409
 - Server-Profile-Required 2-411
 - Tunneling-Protocol 2-494
- precedence settings 2-350
- preferences 2-351
 - RIP 2-385
 - static 2-440
- PRIdisplay command 1-99
- priority values 2-355
- private route caches 2-126

private routes
 Default-Prt-Cache-Time 2-126
 Gateway-Address 2-191
 Name 2-302
 Netmask 2-304
 Private-Route-Table 2-357
 Private-Route-Table profile 2-357
 Route-Description-List 2-389
 Route-Description-List N 2-389

profiles
 Admin-State 2-14
 Admin-State-Perm-If 2-15
 Admin-State-Phys-If 2-15
 Answer-Defaults 2-28
 Atalk-Global 2-37
 ATMP 2-46
 Base 2-68
 Call-Logging 2-82
 Call-Route 2-88
 Connection 2-111
 creating new 1-75
 Date 2-123
 deleting 1-16
 Device-State 2-133
 displaying contents of 1-38
 displaying working profile 1-54
 E1 2-151
 E3-ATM 2-151
 Error 2-159
 Ether-Info 2-161
 Ethernet 2-162
 External-Auth 2-164
 Ext-Tsrv 2-165
 Filter 2-171
 Firewall 2-173
 Frame-Relay 2-180
 indexed by interface address 2-227
 IP-Fax 2-223
 IP-Global 2-224
 IP-Interface 2-226
 IP-Route 2-229
 IPSec 2-231
 IPX-Global 2-234
 IPX-Interface 2-235
 IPX-Route 2-237
 LAN-Modem 2-250
 listing 1-17
 Load-Select 2-260
 Log 2-263
 modifying 1-114
 OC3-ATM 2-313
 reading into edit buffer 1-102
 saving 1-142
 Serial 2-408
 Slot-Info 2-424
 Slot-State 2-425
 Slot-Type 2-426

SNMP 2-427
SNMPv3-Notification 2-428
STM 2-441
SWAN 2-446
SWAN-Stat 2-447
System 2-452
T1 2-455
T1-Stat 2-456
T3 2-458
T3-Stat 2-462
TACL 2-463
Terminal-Server 2-472
Thermal 2-474
TimeDate 2-477, 2-478
Transaction-Server 2-486
Trap 2-489
User 2-503
VRouter 2-519

protocol types 2-361
proxy mode 2-364
PrtCache command 1-100
PSTN settings
 Alert-Progress-Indicator 2-21
 Bearer-Capability 2-70
 Cause-Code-Transparency 2-92
 Proceed-Progress-Indicator 2-358

PVCs
 Backup 2-66
 Circuit-Name 2-96
 Circuit-Type 2-97
 DLCI 2-140
 VC-Max-Loopback-Cell-Loss 2-511

Q

Q.93B layer, configuring 2-365
QSAAL layer, configuring 2-365
QTP
 Acknowledge 2-119
 Call Ack 2-75
 Call Reject 2-88
 Call-Ack-Decrement 2-75
 Connect Acknowledgement 2-309
 Connect Request 2-75, 2-88
 listening for incoming connections 2-366
 maximum number of bytes in message 2-277
 Selection-Timeout 2-402
 Status Message 2-65, 2-309, 2-310
 status updates 2-243

queues
 Queue-Depth 2-366
 RIP 2-386

Quiesce command 1-101, 1-102
Quit command 1-102

R

R1 signaling

- R1-First-Digit-Timer 2-367
- R1-Modified 2-368

R2 signaling

- Force-56Kbps 2-176
- R2-Signaling-Enabled 2-368
- Signaling-Mode 2-418
- Switch-Type 2-450

RADIUS accounting 2-369, 2-507

- Acct-Drop-Stop-On-Auth-Fail 2-4
- Acct-Host 2-4
- Acct-ID-Base 2-4
- Acct-Key 2-5
- Acct-Limit-Retry 2-5
- Acct-Port 2-6
- Acct-RADIUS-Compat 2-6
- Acct-Reset-Time 2-7
- Acct-Server-N 2-7
- Acct-Sess-Interval 2-8
- Acct-Src-Port 2-8
- Acct-Stop-Only 2-8
- Acct-Timeout 2-9
- Acct-Type 2-9
- Rad-Acct-Client 2-369
- user-specific settings 2-507
- UsrRad-Options 2-507

RADIUS authentication 2-369

- Allow-Auth-Config-Rqsts 2-23
- Auth-Attribute-Type 2-49
- Auth-Boot-Host 2-50
- Auth-Boot-Host-2 2-50
- Auth-Boot-Port 2-50
- Auth-Client N 2-51
- Auth-Frm-Adr-Start 2-52
- Auth-ID-Fail-Return-Busy 2-53
- Auth-ID-Timeout-Return-Busy 2-53
- Auth-Keep-User-Name 2-54
- Auth-Key 2-54
- Auth-Netmask 2-56
- Auth-Pool 2-56
- Auth-Port 2-56
- Auth-RADIUS-Compat 2-57
- Auth-Realm-Delimiters 2-58
- Auth-Req-Delim-Count 2-58
- Auth-Req-Strip-Side 2-58
- Auth-Reset-Time 2-59
- Auth-Rsp-Required 2-59
- Auth-Send67 2-60
- Auth-Server-N 2-60
- Auth-Sess-Interval 2-60
- Auth-Session-Key 2-61
- Auth-Src-Port 2-61
- Auth-Timeout 2-62
- Auth-TS-Secure 2-61

Auth-Type 2-62

- displaying a third prompt 2-476
- External-Auth 2-164
- ID-Auth-Prefix 2-209
- Local-Profiles-First 2-261
- NoAttr6-Use-Termsrv 2-309
- Rad-Auth-Client 2-369
- Rad-Auth-Server 2-370
- RADIUS-Server-Compat 2-371
- Rad-Serv-Enable 2-372
- terminal server and 2-379
- third prompt, displaying 2-475
- Use-Answer-For-All-Defaults 2-502

Read command 1-103

real-time fax

- Command-Spoof 2-109
- ECM mode 2-153
- ECM-Enable 2-153
- enabling 2-391
- Fixed-Packets 2-175
- Local-Retransmit-LSF 2-262
- Low-Latency-Mode 2-268
- Max-Rate 2-277
- Packet-Redundancy 2-330
- RT-Fax-Enable 2-391
- RT-Fax-Options 2-392

redundancy settings

- Context-Stats 2-113
- Context-Stats N 2-114
- Fan 2-167
- Function 2-188
- Last-Reboot 2-251
- Primary-Preference 2-352
- Prior-Function 2-354
- Redundancy profile 2-377
- Redundancy-Stats 2-378
- Select-Reason 2-403
- State 2-439

Redundant-Controller-Switch command 1-105

Refresh command 1-106

Remote command 1-107

Reset command 1-109

RIP

- preference 2-385
- queue depth 2-386
- RIP 2-382
- RIP2-Use-Multicast 2-383
- RIP-ASE-Type 2-384
- RIP-Mode 2-384
- RIP-Policy 2-385
- RIP-Pref 2-385
- RIP-Queue-Depth 2-386
- RIP-Tag 2-386
- RIP-Trigger 2-386

RIP-v2
 Home Agent's gateway profile 2-47
 RIP2-Use-Multicast 2-383
 RIP-Mode 2-384

Rlogin
 Clear-Call 2-99
 immediate logins 2-412
 Rlogin 2-387
 Rlogin-Options 2-387
 User 2-503
 User-N 2-504

Rlogin command 1-110

RM command 1-110

route caches
 enabled 2-229
 size limit 2-230

route filters
 Action 2-10
 Add-Metric 2-13
 Route-Address 2-388
 Route-Filter 2-390
 Route-Filter subprofile 2-390
 Route-Mask 2-391
 Type 2-497

routes
 AppleTalk 2-37, 2-39, 2-40
 ATM 2-48
 cache entries 2-230
 caches 2-229
 configuring OSPF 2-321
 Default-Prt-Cache-Time 2-126
 Dialout-Poison 2-136
 Down-Preference 2-144
 enabling a WAN link 2-230
 enabling IPX 2-238
 Ignore-Def-Route 2-212
 Ignore-ICMP-Redirects 2-212
 IP 2-12, 2-115, 2-191, 2-220, 2-229, 2-230, 2-283
 IPX 2-12, 2-202, 2-232, 2-237, 2-359
 metrics for WAN links 2-391
 multicast address for RIP updates 2-383
 OSPF preferences 2-322
 OSPF-ASE-Pref 2-315
 Pool-Summary 2-341
 Preference 2-351
 preferences 2-144
 Private-Route 2-356
 Private-Route-Profile-Required 2-356
 Private-Route-Table 2-357
 Private-Route-Table profile 2-357
 RIP 2-283, 2-383, 2-384, 2-385, 2-386
 RIP on a WAN link 2-382
 RIP on Ethernet 2-384
 RIP preference 2-385
 RIP queue depth 2-386
 RIP version-1 support 2-385, 2-443

 static 2-237
 static preference 2-440
 subnet mask 2-304
 suppressing host 2-444
 temporary 2-471
 Third-Party 2-476
 using the Traceroute command 1-133

RTP packets
 Country 2-117
 DTMF-Tone-Passing 2-149
 Early-Ringback-Enable 2-153
 Frames-Per-Packet 2-182
 Gateway-Address 2-191
 number of compressed audio frames 2-182
 System-IP-Addr 2-453

S

SAP

 advertisements for server 2-410
 applying filter to IPX interface 2-239
 applying filters to connection 2-394
 behavior 2-394
 configuring filter 2-239
 dial-in clients, and 2-334
 Dial-Query 2-137
 enabling filter 2-510
 filters 2-239, 2-394
 home-server proxy feature 2-240
 including service in SAP table 2-498
 input filters 2-218
 IPX-SAP-Filter 2-239
 IPX-SAP-Filter-Name 2-239
 IPX-SAP-HS-Proxy 2-240
 IPX-SAP-HS-Proxy-Net 2-240
 output filters 2-328
 queries 2-137, 2-240
 replying to IPX Nearest Server Query 2-48
 routing IPX without 2-233
 service type 2-412

Save command 1-111

Screen command 1-113

screen length 2-396

screen width 2-396

secret key, for MD5 2-244

security

 Callback 2-75
 CalledNumber 2-77
 caller-ID 2-99
 CLID-Auth-Mode 2-100
 CLID-Selection 2-101
 direct access 2-400
 Enforce-Address-Security 2-158
 level 2-400

Index

S

- security (*continued*)
 - Profiles-Required 2-360
 - Read-Access-Hosts 2-373
 - Read-Community 2-373
 - Read-Write-Community 2-374
 - Read-Write-Enabled 2-374
 - Security-Mode 2-401
 - Toggle-Screen 2-479
 - User-Profile 2-504
 - Write-Access-Hosts 2-522
- seed routers
 - Atalk-Interface 2-37
 - Atalk-Router 2-39
 - Hint-Net-Hi 2-200
 - Hint-Net-Lo 2-200
 - Hint-Zone 2-201
 - IPX-Net-Number 2-236
 - Net-Number 2-304
- SEL 2-147, 2-402
- Selectools software, enabled 2-403
- serial number, for TAOS unit 2-408
- services, types of 2-302
- sessions
 - configuring WAN link options 2-414
 - defaults for answered calls 2-414
 - ensuring unique session IDs 2-413
 - filtering packets 2-171
- Set command 1-114
- SHA1 mode 2-63
- shared profiles 2-415
- shared secrets
 - Acct-Key 2-5
 - Call-Log-Key 2-84
 - L2F-Tunnel-Secret 2-246
 - Password 2-331
 - RADIUS or TACACS+ 2-5
 - Shared-Secret 2-416
 - tunnel authentication, for 2-331
- shelf information
 - Shelf 2-416
 - Shelf-Number 2-416
- shelf number 2-242, 2-416
- Show command 1-116
- signaling gateways
 - Control-Protocol 2-115
 - Heart-Beat 2-198
 - RT-Fax-Enable 2-391
 - Signaling-Mode 2-419
 - T1-Duration 2-455
 - T2-Duration 2-457
 - Transport-Options 2-488
 - Use-System-IP-Address-As-Source 2-506
- signaling, supported modes 2-417
- SLIP connections
 - BOOTP, and 2-422
 - Encapsulation-Protocol 2-156
 - SLIP command 2-422
 - SLIP-Mode-Configuration 2-422
- slot card sessions 1-81
- Slot command 1-118
- slot information
 - Current-State 2-117
 - Reqd-State 2-380
 - Slot 2-423
 - Slot-Address 2-423
 - Slot-Info 2-424
 - Slot-Profile-Change-Enabled 2-424
 - Slot-State 2-425
 - Slot-Type 2-425
 - Slot-Type profile 2-426
- slot numbers
 - Acct-Src-Port 2-8
 - Auth-Src-Port 2-61
 - Call-Routing-Sort-Method 2-91
 - Digital-Call-Routing-Sort-Method 2-137
 - Slot 2-423
- SNMP
 - Advanced-Agent-Enabled 2-16
 - Alarm-Enabled 2-19
 - Auth-Protocol 2-57
 - configuring 2-427
 - Contact 2-113
 - Enforce-Address-Security 2-158
 - interface 2-427
 - Location 2-263
 - Msg-Proc-Model 2-291
 - Priv-Protocol 2-358
 - Queue-Depth 2-366
 - Read-Access-Hosts 2-373
 - Read-Community 2-373
 - Read-Write-Community 2-374
 - Read-Write-Enabled 2-374
 - Security-Level 2-400
 - Security-Model 2-401
 - Security-Name 2-402
 - SNMP profile 2-427
 - snmpAuthPass 1-122
 - SNMP-Message-Type 2-428
 - snmpPrivPass 1-122
 - SNMPv3-Notification profile 2-428
 - SNMPv3-Target-Params 2-429
 - Write-Access-Hosts 2-522
- SNMP interfaces
 - administration 1-45
 - Admin-State 2-14
 - Desired-State 2-127
 - Desired-Trap-State 2-128
 - Device Address 2-131
 - SNMP-Interface 2-427

-
- snmpAuthPass command 1-122
 - snmpPrivPass command 1-122
 - SNMPv3- Notifications settings
 - Active-Enabled 2-12
 - Msg-Proc-Model 2-291
 - Name 2-301
 - Security-Level 2-400
 - Security-Model 2-401
 - Security-Name 2-402
 - SNMPv3-Notifications 2-428
 - SNMPv3-Target-Params 2-429
 - Tag 2-465
 - SNMPv3-USM settings
 - Active-Enabled 2-12
 - Auth-Key 2-54
 - Auth-Protocol 2-57
 - Name 2-301
 - Password 2-331
 - Priv-Key 2-357
 - Priv-Protocol 2-358
 - Read-Write-Access 2-374
 - SNMPv3-USM-User 2-429
 - software load name 2-259
 - software version 2-431
 - Sonet framer modes 2-181
 - SPI 2-433
 - spoofing, of fax commands 2-109
 - SS7 settings
 - ACK-Threshold 2-10
 - Bay-ID 2-70
 - CL1-Action 2-97
 - CL1-Level 2-98
 - CL2-Action 2-98
 - CL2-Level 2-98
 - Congestion-Control subprofile 2-110
 - Congestion-Control-Type 2-111
 - Control-Protocol 2-114
 - Device-ID 2-132
 - Enabled 2-154
 - Heart-Beat 2-198
 - Interval 2-220
 - NFAS-ID 2-308
 - Primary-IP-Address 2-352
 - Primary-TCP-Port 2-353
 - Secondary-IP-Address 2-397
 - Secondary-TCP-Port 2-398
 - Signaling-Heartbeat subprofile 2-417
 - SS7-Continuity 2-436
 - SS7-Gateway 2-437
 - System-Type 2-454
 - T1-Duration 2-455
 - T2-Duration 2-457
 - T3-Duration 2-461
 - Transport-Options 2-488
 - Type 2-497
 - Use-System-IP-Address-As-Source 2-506
 - Window-Size 2-521
 - stack trace records 2-438
 - stacking
 - Data-IP-Address 2-120
 - Enabled 2-154
 - Multicast-Address 2-292
 - Multicast-Interface-IP-Address 2-296
 - Name 2-301
 - Stacking profile 2-437
 - UDP-Port 2-499
 - Status command 1-123
 - status windows
 - Bottom-Status 2-74
 - changing default contents 1-141
 - connection information 1-15
 - Default-Status 2-126
 - displaying and hiding 1-123
 - Left-Status 2-252
 - line information 1-51
 - log buffer 1-62
 - Status-Length 2-441
 - Top-Status 2-481
 - Up-Status 2-502
 - Use-Scroll-Regions 2-506
 - STM settings
 - Framer-Rate 2-182
 - Loop-Timing 2-266
 - Name 2-301
 - Physical-Address 2-336
 - STM profile 2-441
 - subaddresses
 - Auth-Boot-Host 2-50
 - Auth-Boot-Host-2 2-50
 - Auth-Boot-Port 2-50
 - CLID 2-99
 - Dial-Number 2-135
 - Dirdo-Enabled 2-138
 - Source-Address 2-432
 - Subaddress 2-442
 - T-Online 2-479
 - subnet masks, specifying 2-56
 - subprofiles
 - PSTN-Attribute 2-364
 - supported card, code image in tar file 2-501
 - SVC address type 2-311
 - SVCs
 - Active 2-11
 - Address-Prefix 2-13
 - AESA-Address 2-16
 - AFI 2-17
 - ATM-Address 2-43
 - ATM-Answer 2-44
 - ATM-Interface 2-45
 - ATM-Options 2-45
-

Index

S

SVCs (*continued*)

- ATM-Protocol 2-47
 - ATMSVC-Route 2-48
 - Called-Number-Type 2-78
 - Circuit-Type 2-97
 - CLID 2-99
 - Data-Service 2-122
 - Dial-Number 2-135
 - DLCI 2-140
 - DSP-Portion 2-147
 - E164-Native-Address 2-152
 - Encapsulation-Protocol 2-156
 - ESI 2-160
 - Format 2-177
 - FR-Address 2-179
 - HO-DSP 2-201
 - IDI 2-209
 - IDP-Portion 2-211
 - Incoming-Caller-Addr 2-213
 - Insert-Calling-Party-Addr 2-219
 - Interface-Address 2-219
 - Link-Mgmt-DLCI 2-257
 - Max-Cc 2-274
 - Max-Pd 2-277
 - Max-Restart 2-278
 - Max-Stat 2-278
 - Max-Statenoq 2-279
 - Numbering-Plan 2-311
 - Outgoing-Called-Addr 2-325
 - Q93B-Options 2-365
 - QSAAL-Options 2-365
 - SEL 2-402
 - SVC-Address-Info 2-445
 - SVC-Enabled 2-445
 - SVC-Options 2-445
 - T303-ms 2-459
 - T308-ms 2-459
 - T309-ms 2-459
 - T310-ms 2-460
 - T313-ms 2-460
 - T316-ms 2-460
 - T322-ms 2-460
 - Tcc-ms 2-465
 - Tidle-ms 2-477
 - Tkeepalive-ms 2-478
 - Tnoresponse-ms 2-479
 - Tpoll-ms 2-483
 - Window-Size 2-521
- SWAN card, code image in tar file 2-446
- SWAN lines
- Activation 2-11
 - Clocking 2-106
 - Clock-Mode 2-107
 - Divider 2-140
 - Enabled 2-154
 - Error-Count 2-159
 - Exp 2-164
 - internal clock speed 2-164
 - Line-Config 2-252
 - Line-State 2-255
 - Nailed-Group 2-300
 - Name 2-301
 - SWAN profile 2-446
- SWAN statistics
- Error-Count 2-159
 - Line-State 2-255
 - Physical-Address 2-336
 - SWAN-Stat 2-447
- SWANlines command 1-124
- switch types 2-449
- Syslog 1-62
- Auxiliary-Syslog 2-64, 2-342
 - Facility 2-167
 - Log-Software-Version 2-265
 - Port 2-342
 - Syslog-Enabled 2-450
 - Syslog-Format 2-263
 - Syslog-Level 2-451
- Syslog daemon 2-167, 2-450
- Syslog daemon facility code 2-167
- Syslog level 2-451
- system date and time, setting 1-15
- system version, displaying 1-140
- System-level commands
- ARPTable 1-6
 - ATMlines 1-7
 - ATMSVCroute 1-8
 - CLeval 1-13
 - Clr-History 1-14
 - Connection 1-15
 - Dir 1-17
 - Dircode 1-19
 - DNStab 1-20
 - Fanstatus 1-27
 - Fatal-History 1-28
 - Filterdisp 1-31
 - Get 1-38
 - HDLC 1-41
 - IGMP 1-46
 - IPcache 1-48
 - IP-Pools 1-49
 - IProute 1-49
 - Line 1-51
 - List 1-54
 - Log 1-62
 - LS 1-65
 - Mkdir 1-66
 - Modem 1-66
 - MV 1-68
 - Netstat 1-68
 - New 1-75
 - Power 1-98

Quiesce 1-101
Read 1-102
Redundant-Controller-Switch 1-105
Refresh 1-106
Remote 1-107
RM 1-110
Set 1-114
Show 1-116
Status 1-123
SWANlines 1-124
T1channels 1-125
Thermalstatus 1-130
UDS3lines 1-135
Uptime 1-136
Userstat 1-138
Version 1-140
View 1-141

T

T1 card, code image in tar file 2-3
T1 channels 1-125
T1 FrameLine card, code image in tar file 2-508
T1 lines 2-255
 Call-Route-Info 2-89
 Channel-Config 2-93
 Channel-Config N 2-94
 Channel-Usage 2-95
 Clock-Priority 2-107
 Clock-Source 2-108
 Collect-Incoming-Digits 2-108
 CSU-Build-Out 2-117
 Data-Sense 2-121
 default call type 2-124
 DSP-DTMF-Input-Sample-Count 2-147
 DSX-Line-Length 2-149
 Enabled 2-154
 Encoding 2-156
 error condition indicator 2-91
 Error-Count 2-159
 FDL 2-170
 Frame-Type 2-182
 Front-End-Type 2-186
 Hunt-Grp-Phone-Number 2-208
 Idle-Mode 2-210
 Incoming-Call-Handling 2-214
 Incoming-Procedure 2-214
 Internal-Call-Processing 2-220
 ISDN-Emulation-Side 2-241
 Line-Interface 2-253
 Maintenance-State 2-270
 Nailed-Group 2-300
 Name 2-301
 NFAS-Group-ID 2-306
 NFAS-ID 2-308

Outgoing-Procedure 2-326
Overlap-Receiving 2-328
Phone-Number 2-335
Preferred-Source 2-351
PRI-Prefix-Number 2-355
processing incoming calls 2-220
R1-ANIR-Delay 2-367
R1-ANIR-Timer 2-367
R1-First-Digit-Timer 2-367
R1-Modified 2-368
R1-Use-ANIR 2-368
Robbed-Bit-Mode 2-388
SendDisc-Val 2-405
SS7-Continuity 2-436
T1 profile 2-455
T1-Inter-Digit-Timeout 2-456
T302-Timer 2-458
Trailing-Digits 2-486

T1 statistics

AIS-Receive 2-19
BER-Receive 2-70
Carrier-Established 2-91
Channel-State 2-94
Channel-State N 2-95
Error-Count 2-159
Line-State 2-255
Loss-Of-Carrier 2-267
Loss-Of-Sync 2-267
Network-Loopback 2-304
T1-Stat 2-456
Yellow- Receive 2-525

T1-Stats command 1-127

T3 card, code image in tar file 2-457

T3 lines

Enabled 2-154
Frame-Type 2-182
Line-Length 2-255
Line-State 2-255
Loopback 2-266
T3 profile 2-458

T3 statistics

AIS-Receive 2-19
DS2-State 2-145
Line-State 2-255
Loss-Of-Frame 2-267
Loss-Of-Signal 2-267
T3-Stat 2-462
Yellow-Receive 2-525

T391 polling cycles 2-299

TACACS authentication 2-463

Auth-Key 2-54
Auth-Port 2-56
Auth-Server-N 2-60
Auth-Src-Port 2-61
Auth-Timeout 2-62
Auth-Type 2-62

Index

T

- TACACS authentication (*continued*)
 - External-Auth 2-164
 - Tac-Auth-Client 2-463
 - Use-Answer-For-All-Defaults 2-502
- TACACS+ accounting 2-464
 - Acct-Key 2-5
 - Acct-Port 2-6
 - Acct-Server-N 2-7
 - Acct-Src-Port 2-8
 - TacPlus-Acct-Client 2-464
- TACACS+ authentication 2-464
 - Auth-Key 2-54
 - Auth-Port 2-56
 - Auth-Retries 2-59
 - Auth-Server-N 2-60
 - Auth-Src-Port 2-61
 - Auth-Timeout-Time 2-62
 - External-Auth 2-164
 - Pool-Name 2-340
 - TacPlus-Auth-Client 2-464
- tagging
 - route 2-47
 - routes 2-386
 - TOS 2-31
- tags
 - ASE 2-34
 - LSA 1-89
 - MIB 1-111
 - RIP 2-386
- TCP
 - configuring for a WAN link 2-466
 - defaults for answering calls 2-466
 - immediate logins 2-412
 - port for immediate logins 2-342
 - TCP-Estab 2-467
 - TCP-Timeout 2-468
 - timeout 2-468
- TCP connections
 - Clear-Call 2-99
 - Detect-End-Of-Packet 2-131
 - Encap-Mode 2-155
 - Encapsulation-Protocol 2-156
 - End-Of-Packet-Pattern 2-157
 - Flush-Length 2-175
 - Flush-Time 2-176
 - Host 2-203
 - Host2 2-204
 - Host3 2-204
 - Host4 2-205
 - maximum buffered bytes 2-175
 - maximum buffering time 2-176
 - Port 2-342
 - Port2 2-343
 - Port3 2-344
 - Port4 2-345
 - Primary-TCP-Port 2-353
 - Secondary-TCP-Port 2-398
 - TCP 2-466
 - TCP-Clear-Answer 2-466
 - TCP-Clear-Options 2-466
 - TCP-Timeout 2-468
- TCP/IP, global settings 2-224
- TE line numbers 2-480
- Telco settings
 - Answer-Originate 2-30
 - Billing-Number 2-72
 - Callback 2-75
 - Call-By-Call 2-75
 - Data-Service 2-121
 - Delay-Callback 2-127
 - Dialout-Allowed 2-135
 - Expect-Callback 2-164
 - FDL 2-170
 - Force-56Kbps 2-176
 - FT1-Caller 2-188
 - NAS-Port-Type 2-302
 - Telco-Options 2-468
 - Transit-Number 2-488
- telephone numbers 2-335
 - billing 2-72
 - called 2-80
 - calling 2-80
 - CLID 2-99
 - DNIS number associated with 2-190
 - hunt group 2-208
 - matching called-party number 2-355
 - outbound calls 2-135
 - prefixes 2-209
 - remote device 2-168
 - required number of digits 2-311
 - types of 2-77
- Telnet 2-469
 - Auto-Telnet 2-63
 - Clear-Call 2-99
 - Enable-Permit 2-155
 - hosts displayed in menu 2-206
 - immediate logins 2-412
 - maximum number of seconds for idle session 2-210
 - mode in use 2-469
 - port for host 2-345
 - Port-For-Direct-Access 2-346
 - quitting 1-102
 - TACL profile 2-463
 - Telnet-Host-Auth 2-469
 - Telnet-Mode 2-469
 - Telnet-Options 2-470
 - Telnet-Password 2-471
 - User-Profile 2-504
 - using the Telnet command 1-128
- Telnet command 1-128
- temperature threshold settings 2-20

- hr/>
- terminal server
 - 7-Even 2-2
 - AT-Answer-String 2-42
 - Auth-TS-Secure 2-61
 - Auto-Telnet 2-63
 - Banner 2-68
 - Banner N 2-68
 - Buffer-Chars 2-74
 - Cell-Level 2-92
 - Cell-Mode-First 2-93
 - Clear-Call 2-99
 - Clear-Screen 2-99
 - Delay 2-127
 - dialout 2-136
 - Direct 2-138
 - Enabled 2-154
 - enabling Telnet 2-469
 - highest Rlogin source port value 2-278
 - hostnames in menu 2-207
 - immediate login host 2-203
 - Immediate-Mode-Options 2-213
 - Info 2-216
 - IP addresses in menu 2-207
 - IP-Add-Msg 2-221
 - Local-Echo 2-261
 - Login-Prompt 2-264
 - Login-Timeout 2-265
 - lowest Rlogin source port value 2-284
 - maximum baud rate 2-272
 - menu mode 2-282, 2-438
 - modem configuration 2-285
 - modem modulation 2-287
 - modem transmit level 2-287
 - monitoring idle time 2-493
 - obtaining menu from RADIUS 2-379
 - Password-For-Direct-Access 2-332
 - passwords 2-454
 - Port 2-342
 - Port2 2-343
 - Port3 2-344
 - Port4 2-345
 - Port-For-Direct-Access 2-346
 - Port-N 2-345
 - PPP command 2-347
 - PPP sessions 2-349
 - Prompt 2-361
 - Prompt-Format 2-361
 - remote configuration 2-379
 - Rlogin command 2-387
 - Rlogin options 2-387
 - security for direct access 2-400
 - Security-Mode 2-401
 - Service 2-412
 - Service-N 2-413
 - Silent-Mode 2-420
 - SLIP 2-422
 - SLIP configuration 2-422
 - SLIP-BOOTP 2-422
 - TCP command 2-466
 - Telnet hosts 2-206
 - Telnet mode 2-469
 - Telnet-Host-Auth 2-469
 - Terminal-Mode-Configuration 2-471
 - Terminal-Server profile 2-472
 - Terminal-Type 2-473
 - Text-N 2-473
 - Third-Prompt-Sequence 2-476
 - Toggle-Screen 2-479
 - Traceroute 2-484
 - TS-Idle-Timer 2-493
 - User-N 2-504
 - Termserve-level commands, Terminal-Server 1-129
 - Thermalstatus command 1-130
 - Tokencount command 1-131
 - T-Online settings
 - T-Online 2-479
 - T-Online-Most-Avail-Chan 2-480
 - T-Online-Offset 2-480
 - T-Online-Type 2-481
 - TOS filters 2-482
 - Dest-Address 2-128
 - Dest-Address-Mask 2-129
 - Dest-Port 2-130
 - Dst-Port-Cmp 2-148
 - Precedence 2-350
 - Protocol 2-361
 - Source-Address 2-432
 - Source-Address-Mask 2-432
 - Source-Port 2-433
 - Src-Port-Cmp 2-435
 - TOS-Filter subprofile 2-482
 - Type 2-497
 - Type-Of-Service 2-498
 - Type-of-Service 2-498
 - TOS settings
 - Active 2-11
 - Apply-To 2-31
 - Precedence 2-350
 - TOS-Options 2-483
 - Type-of-Service 2-498
 - Traceroute command 1-133
 - traffic shapers 2-484
 - Aggregate 2-18
 - Bit-Rate 2-72
 - Max-Burst-Size 2-273
 - Peak-Rate 2-333
 - Priority 2-355
 - Traffic-Shaper 2-484
 - Traffic-Shapers 2-484
 - Traffic-Shapers N 2-485
-

Index

U

transaction-server settings

- Available-Metric 2-65
- Call-Ack-Decrement 2-75
- Call-Reject-Increment 2-88
- Congested-Metric 2-110
- Data-Ack-Timeout 2-119
- Enabled 2-154
- Hunting-Mechanism 2-208
- Keep-Alive-Timeout 2-243
- Max-QTP-PDU-Size 2-277
- Metric-Max 2-283
- No-Conn-Ack-Increment 2-309
- No-First-Status-Metric 2-309
- No-Second-Status-Metric 2-310
- Partly-Congested-Metric 2-331
- QTP-Port 2-366
- Selection-Timeout 2-402
- Shutdown-Metric 2-416
- Transaction-Server profile 2-486

transparent modem mode 2-189

traps

- Alarm-Enabled 2-19
- Ascend-Enabled 2-34
- Authentication-Enabled 2-51
- Call-Log-Dropped-Pkt-Enabled 2-81
- Call-Log-Serv-Change-Enabled 2-86
- Coldstart-Enabled 2-108
- Community-Name 2-109
- Config-Change-Enabled 2-110
- Console-Enabled 2-113
- Dirdo-Enabled 2-138
- Event-Overwrite-Enabled 2-163
- FR-LinkDown-Enabled 2-185
- FR-LinkUp-Enabled 2-185
- Host-Address 2-206
- Host-Name 2-206
- Host-Port 2-207
- LAN-Modem-Enabled 2-250
- LinkDown-Enabled 2-257
- LinkUp-Enabled 2-259
- Mcast-Monitor-Enabled 2-280
- Megaco-Link-Status-Enabled 2-281
- Notify-Tag-List 2-310
- OSPF-Approaching-Overflow-Enabled 2-315
- OSPF-Enabled 2-316
- OSPF-IF-Auth-Failure-Enabled 2-317
- OSPF-IF-Config-Error-Enabled 2-318
- OSPF-IF-RX-Bad-Packet 2-318
- OSPF-IF-State-Change-Enabled 2-319
- OSPF-LSDB-Overflow-Enabled 2-319
- OSPF-MaxAgeLSA-Enabled 2-319
- OSPF-NBR-State-Change-Enabled 2-320
- OSPF-OriginateLSA-Enabled 2-321
- OSPF-TX-Retransmit-Enabled 2-322
- OSPF-Virt-IF-Auth-Failure-Enabled 2-323
- OSPF-Virt-IF-Config-Error-Enabled 2-323
- OSPF-Virt-IF-RX-Bad-Packet 2-324

- OSPF-Virt-IF-State-Change-Enabled 2-324
- OSPF-Virt-IF-TX-Retransmit-Enabled 2-324
- OSPF-Virt-NBR-State-Change-Enabled 2-325
- Password-Enabled 2-332
- Port-Enabled 2-346
- Power-Supply-Enabled 2-347
- RADIUS-Change-Enabled 2-371
- Secondary-Controller-State-Change-Enabled 2-397
- Security-Enabled 2-399
- Slot-Enabled 2-424
- Slot-Profile-Change-Enabled 2-424
- Suspect-Access-Resource-Enabled 2-444
- Trap profile 2-489
- Use-Exceeded-Enabled 2-502
- VoIP-GK-Change-Enabled 2-516
- WAN-Line-State-Change-Enabled 2-521
- Warmstart-Enabled 2-521

trunk groups

- Num-Digits-Trunk-Groups 2-312
- Trunk-Group 2-491
- Trunk-Group-Callback-Control 2-492
- Trunk-Prefix-Enable 2-492
- Use-Trunk-Groups 2-507

U

UDP packets

- enabling reception 2-476
- UDP-Cksum 2-499

UDP ports 2-499

UDP queue length 2-500

UDS3lines command 1-135

unchannelized DS3 card, code image in tar file 2-500

unnumbered interfaces 2-310

Update-level commands

- Date 1-15
- Delete 1-16
- Load 1-56
- NVRAM 1-78
- PrtCache 1-100
- Reset 1-108
- Save 1-111
- Screen 1-113
- snmpAuthPass 1-122
- snmpPrivPass 1-122
- Write 1-142

Uptime command 1-136

User-level commands

- ? 1-4
- Auth 1-9
- Clear 1-12
- Filtcache 1-30
- Help 1-44
- Netware 1-74

Quit 1-102
Whoami 1-142
Userstat command 1-138, 2-504
UTP 2-161

V

V.120 settings
 Frame-Length 2-179
 V120-Answer 2-509
Van Jacobsen header prediction 2-513
VCI 2-511
Version command 1-140
View command 1-141
virtual IPX network, specifying 2-232
Visa2 settings
 1-Char-Sequence 2-2
 2-Char-Sequence 2-2
 Encapsulation-Protocol 2-156
 First-Data-Forward-Character 2-174
 Fourth-Data-Forward-Character 2-178
 Idle-Character-Delay 2-210
 SDTN-Packets-Server 2-396
 Second-Data-Forward-Character 2-399
 Third-Data-Forward-Character 2-475
 Visa2-Answer 2-512
 Visa2-Options 2-512
VoIP network-management license, enabled 2-305
VoIP settings 2-517
 Active 2-11
 Allow-Coder-Fallback 2-23
 Allow-G711-Fallback 2-25
 Apply-To 2-31
 Call-Hairpin 2-79
 Call-Inter-Digit-Timeout 2-80
 Call-Keep-Alive-Timeout 2-81
 CLID-Suppress 2-102
 Command-Spoof 2-109
 Cut-Thru-Enable-Nearend 2-118
 DTMF-Tone-Passing 2-149
 Early-Ringback-Enable 2-152
 ECM-Enable 2-153
 Ena-Adap-Jitter-Bugger 2-153
 Far-End-Number 2-168
 Fixed-Packets 2-175
 Frames-Per-Packet 2-182
 G711-Transparent-Data 2-189
 Gatekeeper-IP 2-189
 Gatekeeper-IP-Sec 2-190
 Gatekeeper-Keepalive 2-190
 Gateway-Access-Number 2-190
 Gk-Mlg-Control 2-192
 H323-Voice-Ann-Enabled 2-196
 Initial-Jitter-Buffer-Size 2-217

Local-Retransmit-LSF 2-262
Low-Latency-Mode 2-268
Maxcalls 2-274
Max-Dialout-Time 2-275
Max-Jitter-Buffer-Size 2-276
Max-Rate 2-277
Packet-Audio-Mode 2-329
Packet-Redundancy 2-330
Precedence 2-350
Primary-Retrieves 2-353
PSTN-Attribute subprofile 2-364
Registration-Retrieves 2-378
Registration-Retry-Timer 2-379
RT-Fax-Enable 2-391
RT-Fax-Options 2-392
Send-ICMP-Dest-Unreachable 2-406
Sequential-Calls-Enable 2-407
Silence-Det-Cng 2-419
Silence-Threshold 2-420
Single-Dial-Enable 2-421
Transfer-to-Operator 2-487
True-Connect-Enable 2-490
Trunk-Prefix-Enable 2-492
Trunk-Quiesce-Enable 2-492
Type-of-Service 2-498
Voice-Ann-Dir 2-513
Voice-Ann-Enc 2-514
VoIP profile 2-514
VoIP-Enabled 2-515
VoIP-Index 2-516
VPN-Mode 2-518
VoIP-Max-Capacity-Allowed 2-517
VPI 2-517
VRouters
 Active 2-11
 address pools 2-339, 2-340
 Allow-As-Client-DNS-Info 2-22
 Assign-Count 2-35
 client DNS configuration 2-22, 2-104
 Client-Primary-DNS-Server 2-104
 Client-Secondary-DNS-Server 2-104
 DNS-Primary-Server 2-143
 DNS-Secondary-Server 2-143
 Domain-Name 2-144
 global 2-192
 Global-VRouter 2-192
 IPX-Dialin-Pool 2-232
 IPX-Routing-Enabled 2-238
 Name 2-301
 name of defined 2-518
 next hop 2-220
 pool summarization 2-342
 Pool-Base-Address 2-339
 Pool-Name 2-340
 Pool-Summary 2-342
 RIP-Policy 2-385

Index

W

VRouters (*continued*)

- RIP-Trigger 2-386
- Sec-Domain-Name 2-397
- Summarize-RIP-Routes 2-443
- System-IP-Addr 2-452
- TCP connections, and 2-467
- VRouter 2-518
- VRouter profile 2-519
- VRouter-IP-Address 2-520

VSA compatibility mode

- Acct-RADIUS-Compat 2-6
- Auth-RADIUS-Compat 2-57
- Call-Log-RADIUS-Compat 2-85
- RADIUS-Server-Compat 2-371

VT100 session 1-12

W

Whoami command 1-142

Write command 1-142

X

X.75

- configuring for a WAN link 2-523
- defaults when answering calls 2-523
- Frame-Length 2-179
- K-Frames-Outstanding 2-244
- N2-Retransmissions 2-299
- T1-Retrans-Timer 2-456

XON-XOFF (serial port) 2-175

Z

zones

- Atalk-Default-Zone 2-36
- Atalk-Static-ZoneName 2-41
- Atalk-Zone-List 2-42