Lucent Technologies
Bell Labs Innovations

APX™/MAX TNT®

Reference

Part Number: 7820-0805-005
For software version 10.0
August 2002

Notice

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

European Community (EC) RTTE compliance

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

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

Safety, compliance, and warranty Information

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

Security statement

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

Trademarks

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

Ordering Information

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

Feedback

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

Lucent Technologies

Customer Service

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

Finding information and software

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

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

Obtaining technical assistance

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

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

Obtaining assistance through email or the Internet

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

Calling the technical assistance center (TAC)

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

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

Contents

About This Reference

What is in this reference

This reference provides an alphabetic reference to all the profiles, parameters, and commands for APX and MAX TNT units. For complete information about features and configuration tasks, see the product manuals listed under "Documentation set" on page viii. For complete information about how to navigate the command-line interface, refer to the *TAOS Command-Line Interface Guide*.

Note This manual describes the full set of features for units running software version TAOS 10.0. Some features might not be available with earlier versions or specialty loads of the software.

The APX family of products includes multiple platforms that differ in call capacity and hardware, but support the same operating system and similar configuration options. The APX family, which includes the APX 8000 and APX 1000 products, shares many features with its MAX TNT predecessor. For features that are supported with no differences across all the platforms, this manual often refers to your product as a *TAOS unit*.

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

What you need to know

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

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

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that might appear on your computer's screen.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, following). If you can enter the characters but are not specifically instructed to, they do not appear in boldface.

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

Documentation set

The documentation set for APX and MAX TNT products consists of the following manuals, available at `http:www.lucent.com/support` and `http//:www.lucentdocs.com/ins`:

- **Read me first:**
  - *Edge Access and Broadband Access Safety and Compliance Guide*. Contains important safety instructions and country-specific compliance information that you must read before installing a 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:** *Getting Started Guide* or hardware installation guide for your unit. Shows how to install the unit's chassis and hardware, and includes technical specifications. A *Getting Started Guide* also shows you how to provide the basic configuration needed to access the unit on a network.
- **Configuration:**
  - *Physical Interface Configuration Guide* for your unit. Describes how to provision the slot cards supported in the unit, and how to configure the cards' physical interfaces. This guide also describes system allocation of slot card resources, and how to use the supported cards in a variety of data environments.
  - *APX/MAX TNT ATM Configuration Guide*. Describes how to configure Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) and switched virtual circuit (SVC) ATM interfaces. It includes information about ATM direct and ATM-frame relay circuits.
  - *APX/MAX TNT Frame Relay Configuration Guide*. Describes how to configure frame relay operations on a unit. This guide explains physical layer 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/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 unit. This guide includes information about IP routing, Open Shortest Path First (OSPF) routing, Border Gateway Protocol (BGP) routing, Internet Group Management Protocol (IGMP) routing, multiprotocol routers, virtual routers (VRouters), and tunneling protocols.
  - *MultiVoice® for APX/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 unit to use the Remote Authentication Dial-In User Service (RADIUS) server, and contains a complete reference to RADIUS attributes.
- **Administration and troubleshooting:** *APX/MAX TNT Administration Guide*. Describes how to administer a 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/MAX TNT Reference*. An alphabetic reference to all commands, profiles, and parameters supported on a unit.
  - *TAOS Glossary*. Defines terms used in the documentation for a unit.

APX/MAX TNT Command Reference

1

Note All references to redundant shelf controllers apply to APX™ 8000 units only. The information in this chapter is designed for quick reference.

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
hdlc
help
if-admin
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*

Command element	Description
command	Command that supports the `grep` feature.
| **grep**	Display only information that matches the *expression* pattern.
-i	Use pattern matching that is not case sensitive.
-v	Display only information that does *not* match the *expression* pattern.
-c	Count lines containing the *expression* pattern, but don't print them.
expression	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 operation.
[...]	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 field headers and footers might be omitted from the display if they do not match the pattern. However, error messages are exempt from pattern matching.

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
```

Special characters

?

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

Permission level user

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

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

To list all available commands:

```
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]
```

```
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 carry out 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`

A

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 media access control (MAC) address to ARP requests.

Permission level `system`

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

Command element	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 *Displaying the ARP table*

```
admin> arptable
IP Address  MAC Address        Type IF  Retries/Pkts/RefCnt Time Stamp
10.103.0.2  00:C0:7B:7A:AC:54  DYN  0   0/0/552             22760
10.103.0.22 00:C0:7B:71:83:02  DYN  0   0/0/2791            22760
10.103.0.1  08:00:20:7B:24:27  DYN  0   0/0/4296            22811
10.103.0.8  00:00:0C:05:B3:A2  DYN  0   0/0/6493            23058
10.103.0.7  00:00:0C:76:58:4E  DYN  0   0/0/6572            23233
10.103.0.49 00:C0:80:89:19:95  DYN  0   0/0/397             23208
```

The ARP table displays the following information:

Field	Description
IP Address	The address contained in ARP requests.
MAC Address	The MAC address of the host.
Type	How the address was learned, 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.
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 field every time an ARP entry is refreshed.

Example *Adding an entry to the ARP table*

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 atmlines [ds3|oc3|e3] [-a|-d|-f|-u]

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

Field	Description
dvOp	The current operational state of the line (also specified by device-state): ■ 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: ■ Idle indicates that no call is on the line. ■ Busy indicates that the line is handling a call.

Field	Description
dvRq	The required state of the line as specified by reqd-state: ■ 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): ■ 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.
nailg	The dedicated group to which the line has been assigned.

See Also uds3lines

atmsvcroute

Description Displays the switched virtual circuit (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 Asynchronous Transfer Mode (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]

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

Example The following output show a single entry in the routing table:

```
admin> atmsvcroute -d
Prefix=39adfc0102030405050708090O, lnk={{1, 4, 1}0}
```

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`*

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

Example The following command authenticates a login for a user named `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`

B

bgp restart

Description Restarts all Border Gateway Protocol (BGP) sessions for this TAOS unit and its BGP peers, or restarts a session with a specified peer.

Permission level `system`

Usage `bgp restart` [*`ipaddress`*]

Command element	Description
`restart`	Recreates startup conditions for all BGP sessions, or for a session with a specified peer. When entered with no parameters, `bgp restart` causes the TAOS unit to lose all its current BGP information except configuration information.
`ipaddress`	IP address of a BGP peer for which to restart a session, in dotted decimal notation.

Example To restart a BGP session between this TAOS unit and peer at 200.168.1.2:

```
admin> bgp restart 200.168.1.2
```

Dependencies After you use the `bgp restart` command with no options, BGP is in a transient state during which the `bgp show` command is inoperative.

bgp show

Description Displays information about Border Gateway Protocol (BGP) operations on this TAOS unit and its peers.

Permission level `system`

Usage `bgp show global|next-hop|paths [`*`prefix`*`/nm [`*`verbose`*`]]| peers [verbose|packets]|policy[`*`policyname`*`]|summarization`

Command element	Description
`global`	Displays BGP information at the highest level.
`next-hop`	Displays known BGP next-hop addresses and the gateways to them. The `bgp show next-hop` command provides a convenient way to determine where packets go when forwarded. If the next-hop address and the gateway address are the same, the next-hop router is directly adjacent to the TAOS unit interface.
`paths [`*`prefix/nm`* `[`*`verbose`*`]]`	Displays information about BGP paths learned by the TAOS unit, or the paths associated with one IP prefix and subnet mask.
`prefix/nm`	Specifies IP prefix address and subnet mask for which to display BGP path information. The subnet mask indicates the number of high-order bits in the IP prefix. Enter the IP prefix in dotted decimal notation. The subnet mask is a value in the range from 0 through 32 and must be preceded by a slash (`/`)—for example, `/24`.
`verbose`	Displays detailed information about BGP paths or peers. For `bgp show paths`, `verbose` displays the network layer reachability information (NLRI) associated with the paths that the specified prefix address is on.
`peers [verbose|packets]`	Displays a list of BGP peers. Entering `show bgp peers` without either `verbose` or `packets` provides summary information.
`packets`	Displays a summary of packets sent to and received from BGP peers.
`policy [`*`policyname`*`]`	Lists policy names and definitions. Entering `show bgp policy` without *`policyname`* displays only the names of existing BGP policies.
`policyname`	Name of an existing BGP policy for which to display a definition.

Command element	Description
summarization	Displays the following route summaries configured on the TAOS unit for advertisement to BGP peers: ■ Route summaries that were manually configured with the bgp-summarization profile ■ Static and connected route summaries that are automatically created when you configure the parameters static-route-redist-policy and conn-route-redist-policy in the bgp-global profile

Example *Displaying global BGP information*

To display global BGP information:

```
admin> bgp show global
BGP       :enabled
BGP ID[AS]:200.168.30.10[60001]
BGP timers:Connect 120 Keepalive 30 Hold 90
BGP IGP Lockstep:off
BGP Max multipath 0
```

Example *Displaying BGP next-hop information*

The following example shows the next-hop count for two interfaces (172.16.95.1 and 172.16.96.1) on a TAOS unit:

```
admin> bgp show next-hop
Next Hop      Gateway      Src Addr to it Flag Metric Interface
------------  ----------   -------------- ---- ------ ---------
21.21.21.32   10.10.10.32  100.100.100.31      1      ie1-6-1
10.105.0.16   10.105.0.16  100.105.0.31        0      ie1-15-1
32.32.32.32   10.10.10.32  100.100.100.31  M   8      ie1-6-1
32.32.32.32   10.10.0.32   100.100.100.31  M   8      ie1-6-1
10.10.10.11   10.10.10.11  100.100.100.31      0      ie1-6-1
```

Example *Displaying BGP path information*

The following example shows a simple path:

```
admin> bgp show path
0: IGP
Sequence:  200
NH: 32.32.32.32     LP: not present MED Learned/Used:    0/          0
Metrics to NH: 60/2/8/4/2  Gateway to NH: 100.100.100.32
^
|--------No. of equal cost gateways.
NLRI:  32.32.32.32/32/1/1 +210.210.210.0/24/1/0
       10.105.0.0/16/1/1
```

Example *Displaying a list of BGP peers*

In the following example, BGP peer 200.168.1.2 is a member of autonomous system 2 and is a route-reflector client of the TAOS unit. It is configured to accept, inject, and advertise BGP policy `only207`.

```
admin> bgp show peers
Remote IP     AS    Fl    DM   Up    Accept    Inject    Advertise
-------------------------------------------------------------------
200.168.1.2   2     RN     2   Up    only207   only207   only207
200.168.1.3   3     C     --   Dn    all       all       all
```

In the flags (`Fl`) field, the `R` flag in this example identifies this peer as a route-reflector client to the TAOS unit. The `N` flag indicates that this peer is configured to always consider the TAOS unit as the next hop for any update packet sent by the TAOS unit.

Example *Displaying BGP route summaries*

The following example shows a summary configured for a route to an IP address with a prefix of 10.0.0.0, a subnet mask of /8, and a multiexit discriminator of 5:

```
admin> bgp show summarization
10.0.0.0/8/C Bad Count of Supporting Routes: 0
LP: 0           MED: 5   CAS no-advertise
```

Example *Displaying a BGP policy*

The following example shows the definitions for a policy called `test`:

```
admin> bgp show policy test
1 permit
  then local-pref 333 output-multi-exit-disc 444 community add no-advertise
```

C

callroute

Description Displays the call-routing database (the total set of all `call-route` profiles).

Permission level `diagnostic`

Usage `callroute -ah|-an|-ad|-d|-o|-?`

Command element	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.
`-o`	List output available for call routing entries.
`-?`	Display a usage summary.

Example To list available host-side call-routing entries:

```
admin> callroute -ah
slot        #   cost source       type            tg sa phone
1:08:00/0   3   20   0:00:00/0    voip-call-type  0  0
1:08:00/0   7   20   0:00:00/0    g729-call-type  0  0
```

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

Field	Description
Slot	Interface address to which the TAOS routes the incoming or outgoing call. Host-side addresses show incoming-call routes, while network-side addresses show outgoing-call routes. When the TAOS 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 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.
Cost	Using `cost` parameter settings in the `call-route` profile, the system routes calls to a card according to its `cost` value. The lower the `cost` value of a call route, the higher its priority for selection as the destination slot card for a call.
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.

See Also `modem, hdlc, show, t1channels`

cat

Description Prints a file to the screen.

Permission level `system`

Usage `cat` *`socketnumber/pathname`*

Command element	Description
`socketnumber`	Socket number
`pathname`	Full path and filename

Example To print the file doc.txt to the screen, enter the following:

```
admin> cat c:\docs\doc.txt
```

cgCtrl

Description Displays the number of packets dropped because of traffic congestion, and enables you to change the traffic-congestion threshold. You can enter the cgCtrl command for the shelf controller or for an individual slot card.

Permission level system

Usage cgCtrl -s | -c [*parameter* = *value*]

Command element	Description
-s	Display the number of packets dropped because of traffic congestion.
-c [*parameter=value*]	Change the traffic-congestion threshold. The *parameter* value can be one of the following: ■ i—packets per interface ■ p—packets from the Packet Bus Transport Layer (PBTL) ■ t—total packets ■ b—backlog in milliseconds ■ m—available memory in kilobytes

Example To display the number of packets dropped because of traffic congestion:

```
madd-1/4> cgctrl -s
Congestion Control, packets discarded:
0 based on max #pkts/if now=0 thresh=20 pkts
0 based on max #pkts from pbtl now=0 thresh=256 pkts
0 based on max total #pkts now=0 thresh=80 pkts
0 based on max backlog now=0 thresh=0 OFF
0 based on low memory now=26783 thresh=0 OFF
0 dropped continuously (FE41 after doing so for 180 sec)
```

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]

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

Example admin> **clear**

cleval

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

Permission level `system`

Usage `cleval`

Example To enable the call-logging evaluation license:

```
admin> cleval
Date: 04/12/2001. 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: 05/12/2001. 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 carry out this command on the shelf controller or on an individual T1, E1, T3, or FrameLine card. You must first carry out 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]`

Command element	Description
No options	Clear the primary controller's fatal-error log.
`-f` (APX 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 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 To display connection status information:

```
admin> connection
```

```
 2 Connections                  Status
001 tomw PPP 1/7/14 19200       Serial number: 6201732    Version: 10.0
002 timl MP  1/7/3  56000
                                 Rx Pkt:    11185897
                                 Tx Pkt:       42460
                                    Col:         129

                                09/27/2001 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, 09/27/2001
[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

D

date

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

Permission level user

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`

Command element	Description
`on`	Enables diagnostic output.
`off`	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 memory space that was used by the profile becomes available to the system.

Permission level `update`

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

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

Example To delete a `connection` profile named `tlynch`:

```
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 restart. If a system restart 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`

Command element	Description
`-d`	Bring the specified device down.
`-t`	Toggle debug output level.
`-u`	Bring the specified device up.
`-?`	Display a usage summary.
interface_address	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]]`

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

Example *Listing all profiles*

To list all the profiles on the system:

```
admin> dir
ADMIN-STATE-PERM-IF   SNMP Permanent Interface Admin State
ADMIN-STATE-PHYS-IF   SNMP Physical Interface Admin State
ANSWER-DEFAULTS       Answer profile
ATMP                  ATMP profile
BASE                  System version and enabled features
CALL-LOGGING          Call logging
CALL-ROUTE            Call routing attributes
CONNECTION            Connection (WAN) profiles
DEVICE-STATE          Device Operational State
DEVICE-SUMMARY        Device availability summary information
ETHER-INFO            Ethernet Interfaces Information
ETHERNET              Ethernet Interfaces Configuration
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
VROUTER               Virtual Router
```

Example *Listing all profiles of a particular type*

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

```
admin> dir conn
169  08/31/2001 22:21:07  dallas
195  09/12/2001 10:14:08  chicago
189  09/14/2001 09:34:44  nyc1
177  09/14/2001 11:38:09  nyc2
187  10/22/2001 15:34:53  la
201  10/14/2001 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.

Example *Listing information about a specific profile*

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

```
admin> dir conn dallas
169  08/31/2001 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 nonvolatile RAM (NVRAM).

Permission level `system`

Usage `dircode`

Example To display the contents of the flash-card code directory:

```
admin> dircode flash-card-2
Card 2, format FTL/FAT, capacity 8MB
/current:
shelf controller   1231877 Tue Oct 16 17:17:22 2001 9.1
8t1-card            209191 Tue Oct 16 17:17:42 2001 9.1
4ether2-card        180385 Tue Oct 16 17:17:56 2001 9.1
hdlc2-card          588610 Tue Oct 16 17:18:38 2001 9.1
```

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:

Error message	Explanation
`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, fsck, load`

dnscache

Description Enables you to display, clear, and refresh Domain Name System (DNS) cache entries. You can enter the `dnscache` command for the shelf controller or for an individual slot card.

Permission level `system`

Usage `dnscache [-v VRoutername] [-l] [-s] [-c] [-f]`

Command element	Description
`-v VRoutername`(shelf controller only)	Act upon the DNS cache for a specific virtual router (VRouter). By default, the global VRouter is used.
`-l`	List DNS cache entries.
`-s`	Display DNS cache statistics.
`-c`	Clear temporary entries in the DNS cache.
`-f`	Refresh all permanent entries in the DNS cache.

Example *Listing DNS cache entries*

To list DNS cache entries:

```
admin> dnscache -l
Host: syslog.newyork.com
        Type: Permanent    Status: Valid    TTL: 575 sec
        Ip Address
        77.77.76.174
        77.77.76.175
        77.77.76.172
        77.77.76.173
Host: sigma.newyork.com
        Type: Temporary    Status: Valid    TTL: 296 sec
        Ip Address
        77.77.77.184
        77.77.77.185
        77.77.77.182
        77.77.77.183
```

Example *Displaying DNS cache statistics*

To display DNS cache statistics:

```
admin> dnscache -s
       Number of Permanent entries:     1
       Number of Temporary entries:     1
     Total number of cache entries:     2
```

Example *Clearing temporary entries from the DNS cache*

To clear temporary entries from the DNS cache:

```
admin> dnscache -c
Flushing all temporary entries from DNS cache...done
```

Example *Refreshing permanent entries in the DNS cache*

To refresh all permanent entries in the DNS cache:

```
admin> dnscache -f
Refreshing all Permanent entries...
done
```

See Also dnstab

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*]

Command element	Description
-s	Display the local DNS table. This option 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 through 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 01
 2: "rafael"         200.65.212.23    3      Feb 10  9:30:00 01
 3: "donatello"      200.65.212.67    1      Feb 11 11:41:33 01
 4: "wheelers"       200.65.212.9     1      Feb 12  8:35:22 01
```

The output contains the following fields:

Field	Description
Local DNS Table	Specifies whether enabled is set to yes in the dns-local-table subprofile of the ip-global profile.
AutoUpdate	Specifies whether auto-update is set to 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 Simple Network Time Protocol (SNTP) is not in use, the field contains hyphens.

See Also dnscache

dtunnel

Description Display information about established tunnels on the shelf controller or on an individual slot card.

Permission level user

Usage dtunnel full | summary | ipx | route | home [-m | *home_network*] | counts | *tunnelnumber*

Command element	Description
full	Print full tunnel details.
summary	Print tunnel summary.
ipx	Print IPX server information.
route	Print home network route information.
home [-m | *home_network*]	Print home network information. When you include the -m option, the dtunnel command prints home network information that includes all registered mobile clients. When you specify a home network name, the unit displays information about the specified home network and includes information about associated mobile clients and a home network backup (if any).
counts	Print tunnel counts. (This argument requires debug permission.)
tunnelnumber	Print details for tunnel *tunnelnumber*.

Example *Printing full tunnel details*

To print full tunnel details:

```
admin> dtunnel full
Agent Mode  HA Type  IPX sap   UDP   password
----------  -------  -------   ----- --------
Home-Agent  Gateway  disabled  5150  ascend

vRouterID Socket
--------- ------
0         6007
Tunnels:
-------------------------------------------------
Tunnel 2 IfNum 65535 Agent Address 87.99.99.9:5150
Ident=0x1 TN=0x1 DnsSN=0
ATMP Home-Agent
Primary home interface: 11
State 5 (UP) Gateway Mode Home Network Name maxsan1
Remote client
Client IP Address 181.181.181.181/16
Home: Slot=1/1 rtIf=1/1/1/e05109f8
VrouterID: 0, Vrouter: main
-------------------------------------------------
```

Example *Printing a tunnel summary*

To print a tunnel summary:

```
admin> dtunnel summary
Agent Mode   HA Type  IPX sap  UDP   password
----------   -------  -------  ----- --------
Home-Agent   Gateway  disabled 5150  ascend

vRouterID Socket
--------- ------
0         6007
SN IfNum  Tunn Id  VR  St Mode  Agent Address  Mobile Client
-- -----  -------- --- -- ----  -------------  ---------------
2  65535   00000001 0   5   - H   87.99.99.9      181.181.181.181/16
maxsan1
```

Example *Displaying home network information*

To display home network information:

```
admin> dtunnel home
Home Network Name ifNum/mpID MC cnt maxMC
----------------- ---------- ------ -----
hr1               2/-             3     0
hr2-mp            -/2             2     0
hr3               8/-             0     0
```

Following are the fields in the output:

Field	Description
Home Network Name	Name of the home network.
ipNum/mpID	Interface number, MP identifier, or both.
MC cnt	Number of mobile clients using the home network.
maxMC	Maximum number of mobile clients that can use the home network. On MAX TNT units, this field applies only to slot cards.

Example *Displaying home network information with mobile clients*

To display home network information that includes all registered mobile clients:

```
admin> dtunnel home -m
Home Network Name ifNum/mpID MC cnt maxMC
----------------- ---------- ------ -----
hr1               2/-             3     0
     17: 10.2.1.135/24, 18: 10.3.1.130/24, 20: 10.3.2.14/32
hr2-mp            -/2             2     0
     151: 11.2.1.15/24, 150: 11.3.1.16/24
hr3               8/-             0     0
```

Example *Displaying home network route information*

To display home network route information:

```
admin> dtunnel route
HN 'maxsan1' ifId 11 MC Route Info:
     181.181.181.181/16
```

Example *Displaying tunnel counts*

To display tunnel counts:

```
admin> dtunnel counts
Tunnels: UP=1 Connecting=0 Disconnecting=0
FA=0 HA=1 FA+HA=0
Home Networks: 1
```

Example *Displaying information about a particular tunnel*

To display information about tunnel 2:

```
admin> dtunnel 2
Tunnel 2 IfNum 65535 Agent Address 87.99.99.9:5150
Ident=0x1 TN=0x1 DnsSN=0
ATMP Home-Agent
Primary home interface: 11
State 5 (UP) Gateway Mode Home Network Name maxsan1
Remote client
Client IP Address 181.181.181.181/16
Home: Slot=1/1 rtIf=1/1/1/e05109f8
VrouterID: 0, Vrouter: main
-------------------------------------------------
```

dumpcachestat

Description Displays cache statistics.

Permission level code

Usage dumpcachestat

Example To display cache statistics:

```
admin> dumpcachestat
Cache Updates 32 total 7554
Cache Attempts 32 total 8852
Cache Hits 0 total 1298
Add count 54264 Del count 53795
Array Add count 0 Del count 0
Number of flash devices created 0 deleted 0
```

Dependencies The dumpcachestat command requires that you enable diagnostic output.

E

e1sig

Description Displays the state of all E1 channels. You must first carry out the `open` command to open a session with the E1 card.

Permission level `diagnostic`

Usage `e1sig`

Example To display the state of the card in slot 10:

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

e1-1/10> e1sig
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 carry out the `open` command to open a session with the card.

Permission level `diagnostic`

Usage `e1-stats [-c] line`

Command element	Description
`-c`	Display statistics for the line, and reset the statistics to 0 (zero).
line	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.

Field	Description
Line Code Violations	The TAOS unit detected either a bipolar violation or excessive zeroes, 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 –c option.

ether-display

Description Displays the contents of Ethernet packets.

Permission level diagnostic

Usage ether-display *port# n*

Command element	Description
port#	The Ethernet port on which the packets are received or transmitted. If you specify 0 (zero) for the port number, the 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 267 octets
10790840: 00 20 af f8 0f 1d 00 c0  7b 5e ad 3c      . ..... {^.<
```

To stop displaying the Ethernet statistics:

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

Dependencies You must set `debug on` for `ether-display` to have any effect.

See Also `debug`

F

fanstatus

Description Displays fan tray status information, such as the fan's revolutions per minute (RPM) and status, and the unit's ambient temperature.

Permission level `system`

Usage `fanstatus`

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 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.

Permission level `system`

Usage `fatal-history`

Example *Displaying the fatal-error log on an APX unit*

When you display the fatal-error log on an APX unit, information similar to the following appears:

```
admin> fatal-history
SYSTEM IS UP:  Index: 100  Revision: 9.1  Slot 1/41 (apxsre)
        Date: 10/07/2001.       Time: 12:07:39
PRIMARY SELECTED:  Index:  98  Revision: 9.1  Slot 1/41 (apxsre)
        Date: 10/07/2001.       Time: 12:07:52
OPERATOR RESET:  Index:  99  Revision: 9.1  Slot 1/41 (apxsre)
        Date: 10/07/2001.       Time: 12:20:02
        Reset from 172.31.1.254, user profile admin.
SYSTEM IS UP:  Index: 100  Revision: 9.1  Slot 1/41 (apxsre)
        Date: 10/07/2001.       Time: 12:22:06
PRIMARY SELECTED:  Index:  98  Revision: 9.1  Slot 1/41 (apxsre)
        Date: 10/07/2001.       Time: 12:22:19
```

Example *Displaying the fatal-error log on a MAX TNT unit*

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: 09/20/2001.       Time: 16:56:01
        Reset from unknown, user profile super.
OPERATOR RESET:  Index:  99  Revision: 1.3Ap6  Shelf 1 (tntsr)
        Date: 09/24/2001.       Time: 11:56:10
        Reset from unknown, user profile super.
```

Dependencies 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.

See Also `clr-history`

fe-loop

Description Performs a line loopback test at the transceiver of a T1, E1, or T3 card. You must first carry out the `open` command to open a session with the card.

Permission level `diagnostic`

Usage fe-loop *line* in|out on|off

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

Example To loop the channel service unit (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
```

filtcache

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

Permission level user

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

Command element	Description
-s [*filtername*]	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.
-f [-f]	Flush all cached filters. The second -f flag specifies that all filters are flushed without a prompt for confirmation being displayed.

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

```
admin> filtcache -s myfilter
Filter Name  Time Created    Exp After(min)  Use Cnt Refresh   Cache
_____________________________________________________________________
myfilter     18:44:30       10              2       No
```

The following command flushes all cached filters:

```
admin> filtcache -f
Flush all cached filter profiles? [y/n] y
All 3 cached RADIUS filter profiles flushed.
```

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

```
admin> filtcache -s
Filter Name      Time Created    Exp After(min)  Use Cnt Refresh Cache
_____________________________________________________________________
myfilter         20:01:50        1440            3       Yes
filter-b         21:03:34        10              2       No
filter-c         21:10:32        8               14      Yes
```

See Also filterdisp

filterdisp

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

Permission level system

Usage filterdisp [*sessNum*]

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

Example *Displaying all active sessions*

To display all active sessions and their filter names:

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

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

Field	Specifies
`ID`	Identification number for the session.
`Username`	Name of the authenticated profile.
`Src`	Whether the profile is downloaded through RADIUS (`ext`) or recognized as a local profile (`loc`).
`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, `<filters present>` 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, `<filters present>` indicates that a data filter has been applied. If blank, no data filter applies.
`Call-Filter`	Whether a call filter has been applied to the session. F or 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, the label `<filters present>` indicates that a TOS filter has been applied. If blank, no TOS filter applies.

Example *Displaying filter details for a particular session*

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
```

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

See Also `filtcache`

format

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

Permission level `code`

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

Command element	Description
`-f`	Force format without asking for verification.
`-o`	Format the flash card using the version 2 (old) format. By default, the card is formatted using the newer FAT format.
`-e`	Erase the entire flash card.
`-b`	Format the flash card and reserve space for the boot region.
`-x`	For ATA flash cards, format without a master boot record.
`-e -b`	Erase the boot region of the flash card.
`device`	The name of the flash card to be formatted. The following are valid names: ■ `[flash-card-]1` ■ `[flash-card-]2` Device names can be abbreviated as 1 and 2.

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

Error message	Explanation
`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 message	Explanation
`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 memory card in the second (rightmost) slot on the shelf controller, you format it as follows:

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

Dependencies You cannot format a 32MB ATA flash card using the `-o` option. You must format a 32MB ATA flash card using default newer FAT format.

See Also `dircode, fsck, load`

fsck

Description Audits inconsistent file conditions (which can include file contents) on a PCMCIA flash memory card. For each file found, the command displays the type-name, type-number, decimal and 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`

Command element	Description
`-b`	Ignore invalid identifiers. If `fsck` finds no valid directory block but does find a candidate directory block, the `-b` option causes it to ignore any invalid identifiers for the candidate directory block and use that block. 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 cyclic redundancy check (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.

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

Example To check flash card 1:

```
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

ftp

Description Provides File Transfer Protocol (FTP) client functionality.

An FTP client enables you to transfer files larger than the Trivial File Transfer Protocol (TFTP) limit of 16MB and provides a more reliable file transfer protocol. You can start up the FTP client by entering an ftp command and a set of related service commands. Or you can initiate FTP from a command line by means of a set of FTP URLs.

The command interface to the TAOS FTP client consists of a subset of the FTP service commands defined in RFC 959, *File Transfer Protocol (FTP)*. You use these commands to set the FTP file transfer type and working directory, to transfer files, and to otherwise manipulate FTP as you require.

Permission level system

Usage `ftp [hostname | ipaddress]`

Command element	Description
hostname | *ipaddress*	Symbolic hostname or IP address of an FTP server.

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

```
ftp>
```

At this prompt, you can enter the FTP service command `open` to connect to a particular FTP host.

FTP service commands

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

Command	Description
`ascii`	Sets the file transfer type for ASCII files.
`binary`	Sets the file transfer type so that files containing non-ASCII characters can be transferred correctly.
`cd [`*`directory`*`]`	Accesses a working directory named *directory* on the remote system.
`close`	Closes the connection with the remote system without exiting from FTP.
`debug`	Toggles debug output on and off.
`dir [`*`directory`*`]`	Synonym for `ls`. Displays a listing of *directory* on the remote system.
`exit`	Synonym for `quit`. Ends the FTP session and closes any open connections.
`get [`*`remote filename`*`] [`*`local filename`*`]`	Transfers a file named *remote filename* from the remote system to the local system. You can provide a remote file's pathname as a valid remote filename. If you do not enter a *local filename* value, FTP transfers the file to the local current directory (LCD), using the remote filename. If you do not enter either a remote or local filename, you are prompted for both.
`help`	Displays a list of commands recognized by the FTP client.
`lcd [`*`directory`*`]`	Sets the local current directory (LCD) to *directory*. If you do not enter a directory, the TAOS unit displays the current LCD to you.
`ls [`*`directory`*`]`	Synonym for `dir`. Displays a listing of *directory* on the remote system.

Command	Description
`open [hostname]`	Opens a connection to a remote system named *hostname*. If you do not specify a hostname, you are prompted for one.
`put [local filename] [remote filename]`	Transfers a file named *local filename* from the local system to the remote system. You can provide a local file's pathname as a valid local filename. If you do not enter a *remote filename* value, FTP transfers the file to the remote system's current working directory (CWD) using the local filename. If you do not enter either a local or remote filename, you are prompted for both.
`pwd`	Displays the pathname of the working directory on the remote system.
`quit`	Synonym for `exit`. Ends the FTP session and closes any open connections.
`user [username] [password]`	Initializes a login to the host to which the FTP client is connected. If you do not enter a username or password, you are prompted to do so. For more information, see "Username and password details" on page 1-43.

FTP URL interface

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

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

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

Command element	Description
username	Optional username. If the remote server requires a username, the TAOS unit prompts you to enter one. Be sure to enter a colon (:) after any username you enter, and to omit the colon if you omit the username.
password	Optional password. If the remote server requires a password, the TAOS unit prompts you to enter one. You must first enter a username to specify a password. For more information, see "Username and password details" on page 1-43.

Command element	Description
hostname	Fully qualified domain name of a network host, or the host's IP address in dotted decimal notation. If you use a domain name, use a fully qualified one as specified in Section 3.5 of RFC 1034, *Domain Names—Concepts and Facilities*, and Section 2.1 of RFC 1123, *Requirements for Internet Hosts—Application and Support*. A domain name is a sequence of domain labels separated by periods (.), starting and ending with an alphanumeric character, and optionally containing hyphens (-). In contrast to an IP address, the rightmost label can never start with a number.
port	Number of the port, in decimal notation, on an FTP host to which to connect. If you do not enter a port number, *port* defaults to 21. Be sure to enter a colon (:) before any port number you enter, and to omit the colon if you omit the port number.
url-path	Path on the remote system of one or more directory names to the file that you want to transfer. The slashes (/) that precede and follow the path are not part of the pathname(s). If you omit the path, be sure to retain both slashes.
filename	Name of the file on the remote host to transfer.
type=a|i	Optional file transfer type: ■ Enter **;type=a** to transfer ASCII files. ■ Enter **;type=i** to transfer files containing non-ASCII characters, in binary mode. If you do not enter a type, the file transfer type defaults to binary mode. Be sure to enter a semicolon (;) before **type**, and to omit the semicolon if you do not enter a file transfer type.
local-dir	Optional path of one or more names to the local directory of flash memory where the TAOS unit is to store the transferred file. You can enter a PCMCIA slot number and a directory name (for example, **1/current**). If you enter only a directory name, the unit uses the first slot with a FAT-formatted PCMCIA flash memory card. Be sure to include a space before *local-dir*. If you omit *local-dir*, the TAOS unit stores the file in the **root** directory of the first PCMCIA slot that contains a FAT-formatted flash card.

Username and password details

If a username or password includes any of the following characters, you must encode them:

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

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

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

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

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

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

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

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

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

URL path details

The URL path includes the following FTP URL elements:

url-path/*filename*;type=a|i

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

To represent a slash, use the following code:

```
%2F
```

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

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

Example *Connecting to an FTP server*

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

```
admin> ftp 111.11.26.12
220 ds2 FTP server (SunOS 5.6) ready.
```

```
Name:ddoug
331 Password required for ddoug.
Password:
230 User ddoug logged in.

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

ftp> lcd current
Local directory now 1/current

ftp> binary
200 Type set to I.

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

ftp> quit
221 Goodbye.
```

Example *Specifying a URL with complete syntax*

```
ftp //samwise:chey3nne@149.52.12.35/%2Fhome%2Ftest/ftptest.txt;type=a current
```

This URL performs the following tasks:

1. Changes the directory on the TAOS unit to `current` in the first PCMCIA slot with a FAT-formatted flash card
2. Opens an FTP session with host 149.52.12.35
3. Logs in with username `samwise` and password `chey3nne`
4. Changes the remote system's directory to `/home/test/`
5. Switches to ASCII mode
6. Downloads file `ftptest.txt` to `current`
7. Exits FTP

Example *Specifying a URL without a path or local directory name*

```
ftp //samwise:chey3nne@149.52.12.35//ftptest.txt;type=a
```

This URL performs the following tasks:

1. Opens an FTP session with host 149.52.12.35
2. Logs in with username `samwise` and password `chey3nne`
3. Switches to ASCII mode
4. Downloads file `ftptest.txt` to the `root` directory of the first PCMCIA slot that contains a FAT-formatted flash card on the TAOS unit
5. Exits FTP

Example *Specifying a URL without a username or password*

```
ftp //@149.52.12.35/%2Fhome%2Ftest/tntsr.ffs;type=i current
```

This URL performs the following tasks:

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

2 Opens an FTP session with host 149.52.12.35

3 Logs in, prompting for a username and password.

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

5 Switches to binary mode

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

7 Exits FTP

Dependencies Consider the following:

- To use the FTP client capability, your TAOS unit must have a file allocation table (FAT)-formatted flash memory card in its PCMCIA slot.
- The FTP client supports active connections only.
- You cannot cancel an FTP download or upload that is already in progress.
- The FTP client uses the IP address specified for the Ethernet port in use.

G

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 1-122.

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

Permission level `system`

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

Command 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.

Command element	Description
param-index	Complex parameters have an index. For example, the `interface-address` parameter contains both the `physical-address` and `logical-item` indexes.

Example *Displaying the contents of a profile*

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

```
admin> get connection dallas
[in CONNECTION/dallas]
station* = dallas
active = 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 0.0.0.0 +
ipx-options = { no router-peer both both no 00:00:00:00 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 "" "" no +
ppp-options = { no-ppp-auth none "" "" "" "" stac 1524 no 600 600 no+
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 }
x75-options = { 7 10 1000 1024 }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
dhcp-options = { no 1 4 }
shared-prof = no
max-shared-users = 0
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 }
sdtn-packets-server = no
AT-string = ""
port-redirect-options = { none 0 0.0.0.0 }
modem-on-hold-timeout = conn-profile-use-global
```

Example *Displaying the contents of a subprofile*

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 = ascend0
key-id = 0
cost = 10
down-cost = 1000
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no
network-type = Point-to-Point
poll-interval = 10
md5-auth-key = ascend0
```

Example *Displaying the contents of the current location*

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 = ascend0
key-id = 0
cost = 10
down-cost = 1000
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no
network-type = Point-to-Point
poll-interval = 10
md5-auth-key = ascend0
```

Example *Displaying a higher context than the current location*

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
remote-address = 0.0.0.0/0
local-address = 0.0.0.0/0
routing-metric = 1
preference = 60
down-preference = 120
private-route = no
multicast-allowed = no
address-pool = 0
ip-direct = 0.0.0.0
rip = routing-off
route-filter = ""
source-ip-check = no
ospf-options = { no 0.0.0.0 normal 30 120 5 simple ascend0 0 10 1000 type-1 +
multicast-rate-limit = 100
multicast-group-leave-delay = 0
client-dns-primary-addr = 0.0.0.0
client-dns-secondary-addr = 0.0.0.0
client-dns-addr-assign = yes
client-default-gateway = 0.0.0.0
tos-options = { no 000 normal incoming precedence-tos 00 }
tos-filter = ""
client-wins-primary-addr = 0.0.0.0
client-wins-secondary-addr = 0.0.0.0
client-wins-addr-assign = yes
private-route-table = ""
private-route-profile-required = no
```

Example *Displaying a deeper context than the current location*

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 = ascend0
key-id = 0
cost = 10
down-cost = 1000
ase-type = type-1
```

```
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no
network-type = Point-to-Point
poll-interval = 10
md5-auth-key = ascend0
```

Example *Using the* get *command on an APX unit*

The following example shows how to use the *param-name* argument for the IP address of an Ethernet interface on an APX 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 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-1 left-controller 1} 0}
shelf = shelf-1
slot = left-controller
item-number = 1
```

Example *Using the* get *command on an MAX TNT unit*

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-1 controller 1} 0}
shelf = shelf-1
slot = controller
item-number = 1
```

See Also read, write, list

gre

Description Displays Generic Routing Encapsulation (GRE) statistics.

Permission level `diagnostic`

Usage `gre c | z | k | s`

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

Example *Displaying GRE counters*

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

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


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


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


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

Example *Displaying the slots for which GRE is enabled*

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

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

H

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`

Command element	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 *Displaying information about all available HDLC channels*

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:

Field	Description
dvOp	The current operational state of the channel (also specified by the device-state setting): ■ Down indicates that the channel is in a nonoperational state. ■ Up indicates that the channel is in normal operations mode.
dvUpSt	The status of the channel in normal operations mode: ■ Idle indicates that no call is on the line. ■ Active indicates that the channel is handling a call.
dvRq	The required state of the channel as specified by reqd-state: ■ 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	The desired administrative state of the channel (also specified by the desired-state setting): ■ 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.

Example *Displaying information about all possible HDLC channels*

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 recv sndq rcvq  dscr  bufr crc long ovrun 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.
recv	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 cyclic redundancy check (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`*`]`

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

Example *Listing all commands authorized by the current* `user` *profile*

To list all commands authorized by the current `user` profile:

```
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]
```

Example *Displaying help text*

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 carry out 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`

I

if-admin

Note Use of the `if-admin` command is no longer recommended. The functionality that was provided by the `-d` (down) and `-u` (up) options of the command is now provided by `read`, `set`, and `write` operations on one of the following profiles:

- The `admin-state-perm-if` profile for permanent interfaces, such as a nailed interface
- The `admin-state-phys-if` profile for physical interfaces, such as a T1 line

The other options of the `if-admin` command are not supported.

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 nonvolatile RAM (NVRAM), which is not affected by system restarts, so a physical device keeps the same interface number across system restarts or power failures.

Permission level `diagnostic`

Usage `if-admin -a|-d` *`interface`*`|-l|-u` *`interface`*`|-r` *`interface`*`|-?`

Command element	Description
`-a`	List available SNMP interface numbers.
`-d` *`interface`*	Administratively down a specified SNMP interface.
`-l`	List SNMP interface and device address mappings.
`-u` *`interface`*	Administratively bring up a specified SNMP interface.
`-r` *`interface`*	Restart 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
```

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

```
admin> if-admin -l
SNMP-IF   DEVICE ADDRESS
  101   -   { 1 11 32 }
    1   -   { 1 17 1 }
  102   -   { 1 11 33 }
    2   -   { 1 3 1 }
  103   -   { 1 11 34 }
    3   -   { 1 3 2 }
  104   -   { 1 11 35 }
    4   -   { 1 3 3 }
  105   -   { 1 11 36 }
    5   -   { 1 3 4 }
  106   -   { 1 11 37 }
    6   -   { 1 3 5 }
  107   -   { 1 11 38 }
    7   -   { 1 3 6 }
  108   -   { 1 11 39 }
    8   -   { 1 3 7 }
[More <ret>=next entry, <sp>=next page, <^C>=abort]
```

To bring up SNMP interface number 111:

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

igmp

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

Permission level `system`

Usage `igmp clients|groups|mbone`

Command element	Description
`clients`	Display multicast clients.
`groups`	Display active multicast group addresses and interfaces.
`mbone`	Display multicast backbones (MBONEs).

Example *Displaying multicast clients*

To display all multicast clients:

```
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 ALU	CLU is current line utilization, and ALU is average line utilization. Both indicate the percentage of bandwidth used across this interface. If bandwidth utilization is high, some IGMP packet types are not forwarded.

Example *Displaying active multicast group addresses and interfaces*

To display information about all active multicast group addresses and interfaces:

```
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.
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.

Field	Description
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.

Example *Displaying MBONEs*

To display information about all MBONEs:

```
admin> igmp mbone
Pri  Slot   IfNum  Mbone                  Status
-----------------------------------------------
1    1:4    14     { shelf-1 slot-4 1 }   Active
2    -:-    -      test1                  Down
3    1:2    15     { shelf-1 slot-2 1 }   Up (timeout)
```

The output contains the following fields:

Field	Description
Pri	Priority of MBONE [shelf only].
Slot	Slot card that MBONE connection is on.
IfNum	Interface number of connection.
Mbone	Mbone name (for WAN MBONEs) or interface name (LAN MBONEs).
Status	■ Active—Interface is the current MBONE ■ Up—Interface is up but higher priority MBONE is active ■ Down—Interface is down In addition to the status, the message timeout might appear, indicating that the MBONE has had an IGMP HMQ time-out.

Dependencies The igmp command applies only if the TAOS unit forwards multicast packets to members of multicast groups. 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`

Command 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.
`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 *Displaying IP route cache information on the shelf controller*

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
```

Example *Displaying IP route cache information on a slot card*

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

ip-pool-addr

Description Disables or enables an IP pool address.

Permission level system

Usage ip-pool-addr [-d | -e | -l | -?] [*VRoutername*] *ipaddress*

Command element	Description
-d	Disable pool address.
-e	Enable pool address.
-l	List disabled addresses.
-?	Display command summary.
vRoutername	Act on a specific virtual router (VRouter). By default, the global VRouter is used.
ipaddress	IP pool address to be disabled.

Example *Disabling an IP pool address*

To disable an IP pool address, enter the ip-pool-addr -d command. For example:

```
admin> ip-pool-addr -d 10.10.10.1
Disabling 10.10.10.1 pool address
LOG notice, Shelf 1, Controller, Time: 05:56:21--
Disabling 10.10.10.1 pool address
```

Example *Listing all disabled IP addresses*

To list disabled addresses, enter the ip-pool-addr -l command. For example:

```
admin> ip-pool-addr -l
Disabled ippool addresses:
10.10.10.
```

Example *Enabling an IP pool address*

To enable an IP pool address, enter the ip-pool-addr -e command. For example:

```
admin> ip-pool-addr -e 10.10.10.1
Enabling 10.10.10.1 pool address
LOG notice, Shelf 1, Controller, Time: 05:57:42--
Enabling 10.10.10.1 pool address
```

See Also ip-pools

ip-pools

Description Displays the status of the IP address pools configured in the `ip-global` profile.

Permission level `system`

Usage `ip-pools [VRoutername]`

Command 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.

Example To display the status of global address pools:

```
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.

See Also `ip-pool-addr`

ipportmap

Description Displays active UDP and TCP port mappings.

Permission level `system`

Usage `ipportmap -c | -m`

Command element	Description
`-c`	Display the cache state.
`-m`	Display current mappings.

Example *Displaying the cache state*

To display the number of active ports, enter the `ipportmap -c` command:

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

Example *Displaying current mappings*

To display the protocol, IP address, shelf number, and slot number for each port, enter the `ipportmap -m` command:

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

iproute add

Description Enables you to manually add IP routes. 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. Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) updates can change the metric for the route.

Any routes you add with the `iproute add` command are lost when you restart the TAOS unit.

Permission level `system`

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

Command element	Description
`-r` *VRoutername*	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`.

Command element	Description
pref	Route preference. The default is 100.
metric	Virtual hop count of the route. You can enter a value between 1 and 15. The default is 1.

Example To add a route to the 10.1.2.0 network through the IP router located at 10.0.0.3/24, with a metric of 1:

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

iproute delete

Description Enables you to manually delete IP routes. Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) updates can add back any route you remove with `iproute delete`. The TAOS unit restores all routes listed in the `ip-route` profile after a system restart.

Permission level `system`

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

Command element	Description
`-r` *VRoutername*	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.

Example To delete a route to the 10.1.2.0 network through the IP router located at 10.0.0.3/24:

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

L

l2tp

Description Displays information about the Layer 2 Tunneling Protocol (L2TP) configuration of a TAOS unit.

Permission level `user`

Usage `l2tp -[a|v|d|t[s r c t]|c[i s n m]]`

Command element	Displays
`-a`	L2TP administrative status.
`-v`	L2TP version information.
`-d`	L2TP domain statistics table.
`-t`	Tunnel statistics table. Following are additional arguments for use with this option: ■ `s`—Display tunnel states. ■ `r`—Display remote information. ■ `c`—Display capability information. ■ `t`—Display totals/active session.
`-c`	Call statistics table. Following are additional arguments for use with this option: ■ `i`—Display username and call serial number. ■ `s`—Display call state, connection speed, and capability. ■ `n`—Display DNIS, CLID, and subaddress. ■ `m`—Display proxy Link Control Protocol (LCP), authentication method, and sequencing state.

Example *Displaying information about the enabled L2TP mode*

When you enter the `l2tp` command with the `-a` option, the unit displays information about which L2TP mode is enabled. One of the following messages can appear:

```
L2TP is disabled on this unit.
```

```
L2TP LAC mode is enabled on this unit.
```

```
L2TP LNS mode is enabled on this unit.
```

```
L2TP LAC and LNS modes are enabled on this unit.
```

If L2TP is not enabled in the security PROM, the following message is displayed:

```
The L2TP software option is not installed on this unit. For additional
information see the 'base' profile or the 'update' command.
```

Example *Displaying L2TP version information*

When you enter the `l2tp` command with the `-v` option, version information is displayed. For example:

```
admin> l2tp -v
L2TP Protocol Version: 1.0
L2TP Firmware Revision: 1.0
Vendor name: Ascend
```

Example *Displaying the L2TP domain statistics table*

An L2TP domain is equivalent to a virtual router (VRouter). The `l2tp -d` command displays the following information:

```
admin> l2tp -d
    Total     Failed    Failed    Active     Total   Failed  Active
ID  Tunnels   Tunnels   Auth      Tunnels    Calls   Calls   Calls
0   4         0         1         2          42      7       11
1   6         1         2         3          62      3       9
```

Example *Displaying L2TP tunnel information*

When you enter the `l2tp` command with the `-t` option, the unit displays data about each tunnel. For example:

```
admin> l2tp -t
Shelf/
Slot   LocalTID   RemoteTID
1/ 3   1          1
```

Example *Displaying L2TP tunnel-state information*

The `-ts` option displays tunnel states. For example:

```
admin> l2tp -ts
Shelf/
Slot   LocalTID   RemoteTID  State   Initiated
1/ 3   1          1          Estab   Locally

State: Idle, Conn, Estab, Disconn, Dstroyd
Initiated: Locally, Remotely
```

Example *Displaying L2TP remote capability information*

The `-tc` option displays remote capability information. For example:

```
admin> l2tp -tc
Shelf/                        Bearer Framing
Slot   LocalTID   RemoteTID   Cap.   Cap.
1/ 3   1          1           AD     SA

Bearer Cap: "A" = Analog, "D" = Digital
Framing Cap: "S" = Sync, "A" = Async
```

Example *Displaying active L2TP sessions*

The `-tt` option displays totals. For example:

```
admin> l2tp -tt
Shelf/                          Total    Active
Slot   LocalTID   RemoteTID     Calls    Calls
1/ 3   1          1             1        1
```

Example *Displaying L2TP call-level statistics*

When you enter the `l2tp` command with the `-c` option, the unit displays call-level statistics. For example:

```
admin> l2tp -c
Shelf/ Local     Local      Remote
Slot   TID       CID        CID
1/ 3   2         2          2
```

Example *Displaying L2TP call information*

The `-ci` option displays call information. For example:

```
admin> l2tp -ci
Shelf/ Local    Local      Remote    User             Call
Slot   TID       CID        CID        Name             Serial #
1/ 3   2         2          2          max6k            2
```

Example *Displaying L2TP call-state information*

The `-cs` option displays call state information. For example:

```
admin> l2tp -cs
Shelf/ Local  Local Remote   Call  Call   Tx Conn. Rx Conn.  Bearer/
Slot   TID    CID   CID      State Type   Speed    Speed     Framing
1/ 3   2      2     2        Estab LAC/In 56000    56000     D/S
Call State: Idle, Conn, Estab, Dconn, Dstry
Call Type: LAC/In, LAC/Out, LNS/In, LNS/Out
Bearer: D or S
Framing: A or S
```

Example *Displaying DNIS, CLID, and subaddress information*

The `-cn` option displays DNIS, CLID, and subaddress information. For example:

```
admin> l2tp -cn
Shelf/ Local   Local   Remote
Slot   TID     CID     CID    DNIS         CLID          SubAddress
1/ 3   2       2       2      800-555-1212 877-555-1212  123456
```

See Also `l2tpcards`

l2tpcards

Description Displays the slot cards capable of handling Layer 2 Tunneling Protocol (L2TP) tunnels.

Permission level `user`

Usage `l2tpcards`

Example To display slot cards for L2TP tunnels:

```
admin> l2tpcards
L2TP Control Cards (Shelf:Slot):
Enabled slots:   1/7    1/13
```

See Also l2tp

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]

Command element	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 *Displaying the upper portion of the status window*

To display the line status in the upper portion of the status window:

```
admin> line top
```

```
 2 Connections
001 tomw PPP 1/7/14 19200
002 timl MP  1/7/3  56000
                                  SanFran+ 1/13/8  RA I........ ........ ......
                                  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, 09/27/2001

[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 (unchannelized DS3 lines)	Loss of signal. No signal has been detected.
LF (unchannelized DS3 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 signal. The TAOS unit is receiving a Yellow Alarm signal 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 Primary Rate Interface (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: ■ 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.

Code	Description
-	The channel is currently idle (but in service).
@	The channel is disabled.
b	The channel is a backup non-facility associated signaling (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. This code applies to Integrated Services Digital Network (ISDN) and Signaling System 7 (SS7) only.
n	The channel is dedicated.
o	The channel is out of service (ISDN and SS7 only).
s	The channel is an active D channel (ISDN only).
h	The channel is on hold.
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	Description
(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 signal receive.
`1S`	Alarm Indication signal (AIS) receive.

Following are the status indications for OC3-ATM lines:

Status indicator	Description
(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 signal receive
`1S`	Alarm Indication signal (AIS) receive.

Example *Displaying line status information directly to screen*

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 DSO 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---e1-indian-signal
1/14/02 RED ALARM  LOC   --  ........ ......... e1-dpnss-signal
1/14/03 ACTIVE      --   --  .------- ------s---e1-indian-signal
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:

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 `fe-loop` command.
`CARR`	Carrier. If the system detects a loss of carrier on a line, `LOC` is displayed. If the line sees a carrier, it displays dashes (`--`).
`LOOP`	Loopback status. If the line is locally looped, `LOOP` is displayed. Otherwise, the field 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*`]]`

Command element	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.

Command element	Description
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 *Listing the contents of a profile*

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 = 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 0.0.0.0 +
ipx-options = { no router-peer both both no 00:00:00:00 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 "" "" no +
ppp-options = { no-ppp-auth none "" "" "" "" stac 1524 no 600 600 no+
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 }
x75-options = { 7 10 1000 1024 }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
dhcp-options = { no 1 4 }
shared-prof = no
max-shared-users = 0
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 }
sdtn-packets-server = no
AT-string = ""
port-redirect-options = { none 0 0.0.0.0 }
modem-on-hold-timeout = conn-profile-use-global
```

Example *Listing the contents of a subprofile*

To list the ppp-options subprofile:

```
admin> list ppp
[in CONNECTION/dallas:ppp-options]
send-auth-mode = no-ppp-auth
bi-directional-auth = none
send-password = ""
substitute-send-name = ""
recv-password = ""
substitute-recv-name = ""
link-compression = stac
mru = 1524
lqm = no
lqm-minimum-period = 600
lqm-maximum-period = 600
cbcp-enabled = no
mode-callback-control = cbcp-no-callback
delay-callback-control = 0
trunk-group-callback-control = 4
split-code-dot-user-enabled = no
mtu = 1524
```

Example *Returning to the top-level context of a profile*

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

```
admin> list ..
```

To use the list command to display the x75-options subprofile:

```
admin> list .. x75-options
[in CONNECTION/dallas:x75-options]
k-frames-outstanding = 7
n2-retransmissions = 10
t1-retran-timer = 1000
frame-length = 1024
```

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 Trivial File Transfer Protocol (TFTP).

Permission level update

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

Command element	Description
`-v`	Display verbose output for configuration loads.
`-l` (APX 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 units only)	Transfer the image from this controller to the peer controller after the download is complete.
`-e password`	Use encryption. The *password* 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 Data Encryption Standard (DES) or message-digest algorithm 5 (MD5).
load-type	■ `amdm`—code for an Analog Modem card ■ `boot-sr`—shelf-router boot load ■ `config`—configuration file ■ `csmx`—code for a Series56™ II card ■ `csmv`—code for a Series56™ III card ■ `ds3-atm`—code for a DS3-ATM card ■ `ds3-atm2`—code for a DS3-ATM2 card ■ `e1-8`— code for an E1 card ■ `enet2`—code for an Ethernet-2 card ■ `enet3`—code for an Ethernet-3 card ■ `hdlc2`—code for a Hybrid Access II card ■ `hdlc2ec`—code for a Hybrid Access III card ■ `madd`—code for a 48-port MultiDSP card ■ `pctfit`—code for a Peripheral Control Timing Facilities Interface (PCTFI) card with a T1 line ■ `pctfie`—code for a PCTFI card with an E1 line ■ `sr`— shelf-router runtime load (resides in onboard flash memory) ■ `stm0`—code for an STM-0 card ■ `swan`—code for a Serial WAN (SWAN) card ■ `swan2`—code for a SWAN2 card

Command element	Description
	■ t1-8—code for aT1 card ■ t3—code for a T3 card ■ tar—tar file containing all slot card code images ■ uds3—code for an unchannelized DS3 card ■ ue1—code for an E1 FrameLine card ■ unchan-t1—code for a T1 FrameLine card
-subtype	The subtype of the image: ■ –normal (for regular image, the default) ■ –debug (for debugging image) ■ –diagnostic (for diagnostic image) 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 –debug subtype, the image saved in flash memory has a subtype of debug instead of normal.
source	The location from which the file will be loaded: ■ network *host filename*—After typing the word network, 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. ■ console—The PC connected to the TAOS unit by means of the serial port.
device	The name of the flash card to load. Following are the valid device names: ■ [flash-card-]1 ■ [flash-card-]2 The [flash-card-]1 value is the default. 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. 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 tntrel.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 tntrel.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 *Loading a configuration file*

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
```

Example *Loading a software update*

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
```

Example *Loading a* `tar` *file*

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 tntrel.tar
file tntrel.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.
```

Example *Loading a new boot loader to both APX controllers*

With the following command, the system loads the new boot loader to both controllers on an APX 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.
```

Example *Loading a new boot loader to the local APX controller*

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.
```

Example *Error messages that can appear when you use the* `load` *command*

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:

Error message	Explanation
`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:

Error message	Explanation
`-e option:unknown encryption method` *`method`*	You specified an incorrect encryption method when you saved the configuration.
`File is corrupted, Encryption tag not found`	The configuration file is corrupted.
`File is corrupted, Version tag not found`	

Error message	Explanation
`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, fsck, 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]]`

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

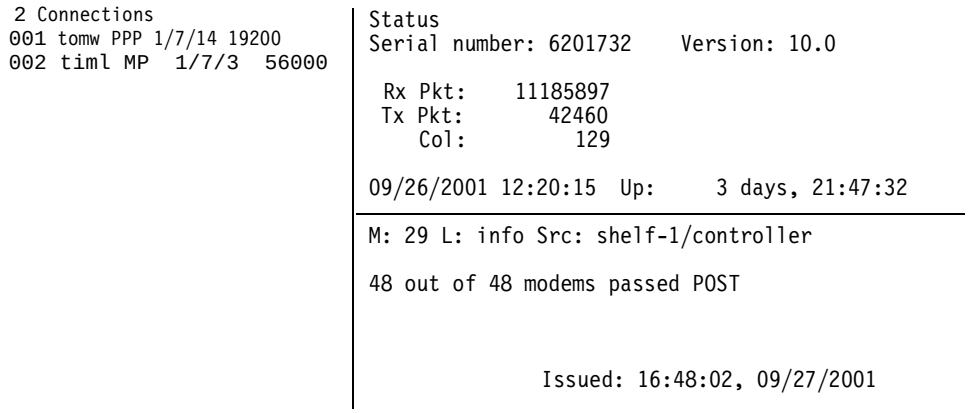
Example *Printing log contents to the screen*

To print log contents to the screen with the most recent entry first:

```
admin> log -p
Time     Date        Source              Level   Description
11:11:25 10/16/2001  shelf-1/controller  notice  Slot 1/10, state UP 2
11:11:20 10/16/2001  shelf-1/slot-10     info    Software version 9.1
11:11:20 10/16/2001  shelf-1/slot-10     info    Card serial number 91464
11:10:15 10/16/2001  shelf-1/controller  notice  Slot 1/5, state UP 2
11:10:10 10/16/2001  shelf-1/slot-5      notice  100BaseT: Link down
11:10:10 10/16/2001  shelf-1/slot-5      notice  ie1-5-3: Link down
11:10:10 10/16/2001  shelf-1/slot-5      notice  ie1-5-2: Link down
11:10:10 10/16/2001  shelf-1/slot-5      notice  ie1-5-1: Link down
```

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

```
admin> log bottom
```



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.
`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.

Level	Description
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.

Example *Informational messages*

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 (POST).
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.

Example *Warning messages*

Following are some sample warning messages:

Warning message	Description
`Busy`	The telephone 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 glare signal from the switch. 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.

Example *Closing the status window*

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`*`]]`

Command element	Description
`socket`	Specify the flash card number.
/`path`	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.ffs          1859325 Mon Oct 15 11:29:26 2001 Version 10.0
  tnt8t1.ffs         272179 Mon Oct 15 11:29:32 2001 Version 10.0
```

See Also mkdir, mv, rm

M

mkdir

Description Creates a new directory.

Permission level system

Usage mkdir *socket/path*

Command element	Description
socket	Specify the flash card number.
path	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|-p|-s

Command element	Display
-a	Available digital modems.
-d	Disabled digital modems.
-f	Failed or nonexistent digital modems.
-g	Operational digital modems.
-i	In-use digital modems.
-m	All possible digital modems.
-p	Summary of all digital modems.
-s	Suspect digital modems.

Example *Listing all nonsuspect modems*

To list all nonsuspect modems:

```
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  )
<end modem list>  Total number of Non-Suspect Modems: 14
```

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

Field	Description
dvOp	The current operational state of the modem (also specified by device-state): ■ Down indicates that the modem is in a nonoperational state. ■ Up indicates that the modem is in normal operations mode. ■ None indicates that the modem does not currently exist. ■ Restart indicates that the modem is being restarted.
dvUpSt	The status of the modem in normal operations mode: ■ Idle indicates that the modem is not handling a call. ■ Reserve indicates that the modem is not currently in use, but should not be used until all idle devices are in use. ■ Assign indicates that the modem is handling a call.
dvRq	The required state of the modem as specified by the reqd-state setting: ■ 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.

Field	Description
SAdm	The desired administrative state of the modem (also specified by `desired-state`): ■ `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. 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.
mDis	Modem disable mode (as indicated by the `lan-modem` profile): ■ `Enable` specifies that the modem is operational. ■ `Disable` specifies that the modem has been disabled.

Example *Displaying a summary of all digital modems*

To display a summary:

```
admin> modem -p
Number of available modems: 192
Number of disabled modems: 0
Number of failed/non-existent modems: 0
Number of available good modems: 192
Number of in-use modems: 0
Number of all possible modems: 192
```

See Also `open, show, slot`

mprt

Description Displays multipath routes.

Permission level `system`

Usage `mprt [-l]`

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

Example To display a page-by-page output of multipath routes:

```
ether2-1/10> mprt -l
MP Route Gateway        Shelf/Slot IF Addr          Mtu  Switched
1.1.1.1/32
         200.200.200.3  ( 1/17)    200.200.200.230  1500  0
         200.200.200.2  ( 1/17)    200.200.200.230  1500  0
         200.200.200.4  ( 1/17)    200.200.200.230  1500  0
         200.200.200.5  ( 1/17)    200.200.200.230  1500  0
         200.200.200.6  ( 1/17)    200.200.200.230  1500  0
         200.200.200.7  ( 1/17)    200.200.200.230  1500  0
         200.200.200.8  ( 1/17)    200.200.200.230  1500  0
         200.200.200.9  ( 1/17)    200.200.200.230  1500  0
         200.200.200.10 ( 1/17)    200.200.200.230  1500  0
         200.200.200.11 ( 1/17)    200.200.200.230  1500  0
         200.200.200.12 ( 1/17)    200.200.200.230  1500  0
         200.200.200.13 ( 1/17)    200.200.200.230  1500  0
         200.200.200.14 ( 1/17)    200.200.200.230  1500  0
         200.200.200.15 ( 1/17)    200.200.200.230  1500  0
         200.200.200.16 ( 1/17)    200.200.200.230  1500  0
         200.200.200.17 ( 1/17)    200.200.200.230  1500  0
         200.200.200.18 ( 1/17)    200.200.200.230  1500  0
         200.200.200.19 ( 1/17)    200.200.200.230  1500  0
         200.200.200.20 ( 1/17)    200.200.200.230  1500  0
         200.200.200.1  ( 1/17)    200.200.200.230  1500  0
         200.200.200.21 ( 1/17)    200.200.200.230  1500  0
         200.200.200.22 ( 1/17)    200.200.200.230  1500  0
```

mv

Description Moves a file or directory.

Permission level system

Usage mv *socket1*/*path1* *socket2*/*path2*

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

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

N

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]`

Command element	Description
No options	Display UDP and TCP statistics.
VRoutername	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.
`-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 `udp`, `tcp`, `icmp`, `ip`, `igmp`, and `mcast`. There is no support for IP multicast on a per-VRouter basis, so the IGMP and MCast statistics relate only to the global VRouter.
`-z`	Display zombie routes created for Routing Information Protocol (RIP). Zombie routes are those that have been deleted from the main routing table and are advertised with an infinite metric (16) for a period of 2 minutes to cause neighboring router to flush this route from their tables.

Example *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   PreQDrops   Total Rx  Service
1/c   0   1023       0      1        0          0           0
1/c   1   route      0      0        0          0           25
1/c   2   echo       0      32       0          0           0
1/c   3   ntp        0      32       0          0           1
1/c   4   1022       0      128      0          0           0
1/c   5   snmp       0      128      0          0           0
1/1   0   1          0      256      0          0           0
1/1   1   1018       0      128      0          0           0
1/3   0   3          0      256      0          0           0
1/3   1   1021       0      128      0          0           0
1/5   0   5          0      256      0          0           0
1/5   1   1020       0      128      0          0           0
1/8   0   8          0      256      0          0           0
1/8   1   1019       0      128      0          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:

Field	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.
`InQDrops`	The number of packets dropped from the input queue because the value of `InQMax` was reached.
`PreQDrops`	The number of unauthorized requests dropped for a particular socket before being queued.
`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.

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

For UDP, netstat reports the following services:

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

For TCP, netstat reports the following services:

Service	TCP port number
Telnet	23
TACACS+	49
Finger	79

Example *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 fields in the interface table contain the following information:

Field	Description
`Name`	The name of the interface: ■ `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.
`MTU`	The maximum packet size allowed on the interface.
`Net/Dest`	The network or the target host this interface can reach. For Ascend Tunnel Management Protocol (ATMP) interfaces, the unit displays a subnet mask of /32.
`Address`	The address of this interface. For ATMP interfaces, the unit displays an IP address of 127.0.0.5.
`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.

Example *Displaying the routing table*

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

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

Field	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 field.
`IF`	The name of the interface through which to send packets over this route: ■ `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.

Field	Description
Flg	One or more of the following flags: ■ 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 Open Shortest Path First (OSPF) ■ R—a route learned from Routing Information Protocol (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
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 through 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.

Example *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
```

```
admin> netstat -s udp
udp:
   46 packets received
   34 packets received with no ports
   12 packets dropped pre-Queuing check
   14 packets transmitted
```

See Also nslookup, ping, traceroute

netware

Description Displays Internetwork Packet Exchange (IPX) network and server information, data on IPX pings, and IPX statistics.

Permission level user

Usage netware [*VRoutername*] [-n | -p | -s | -t]

Command element	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:

```
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 1-94.)

Permission level system

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

Command 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 and write a connection profile named `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 = ""
sub-address = ""
clid = ""
ip-options = { yes yes 0.0.0.0/0 0.0.0.0/0 1 60 120 no no 0 0.0.0.0 +
ipx-options = { no router-peer both both no 00:00:00:00 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 "" "" no +
ppp-options = { no-ppp-auth none "" "" "" "" stac 1524 no 600 600 no+
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 }
x75-options = { 7 10 1000 1024 }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
dhcp-options = { no 1 4 }
shared-prof = no
max-shared-users = 0
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 }
sdtn-packets-server = no
AT-string = ""
port-redirect-options = { none 0 0.0.0.0 }
modem-on-hold-timeout = conn-profile-use-global

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
idle-logout = 0
prompt = *
default-status = no
top-status = general-info
bottom-status = log-window
left-status = connection-list
screen-width = 80
screen-length = 24
status-length = 18
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 = Ascend
active-enabled = yes
allow-termserv = yes
allow-system = yes
allow-diagnostic = yes
allow-update = yes
allow-password = no
allow-code = yes
idle-logout = 0
prompt = *
default-status = no
top-status = general-info
bottom-status = log-window
left-status = connection-list
screen-width = 80
screen-length = 24
status-length = 18
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*

Command element	Description
-r *VRoutername*	Specifies the VRouter for which you want to obtain an IP address.
-s *DNS_server*	Specifies the IP address of the DNS server that the unit uses to resolve the hostname or VRouter name. If you do not specify this option, the system uses the DNS server you configured locally.
-v	Specifies that the unit prints the details of the packet received from the DNS server.
hostname	Specifies the 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 RAM (NVRAM), and restarts 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 `nvram [-f|-t|-u|-c|-e|-?][-r controller]`

Command element	Description
No options	Clear NVRAM. On an APX 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.
`-e`	Enable extended profiling.
`-?`	Display a usage summary.
`-r` *`controller`*	Clear NVRAM and reboot one or both redundant controllers. For *`controller`*, 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.

Warning If you enable extended profiling by means of the `nvram -e` command, your boot load must support extended profiles and you must use a 32M memory card. If you use the `nvram -e` command without first meeting these criteria, all your profile information will be deleted.

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

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

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> nvram -r secondary
```

The following command clears the memory of the primary controller:

```
admin> nvram -r primary
```

The following command clears nonvolatile RAM for the entire system:

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

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

See Also `load, save, reset`

O

oamloop

Description Sends Asynchronous Transfer Mode (ATM) operations, administration, 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`

Command element	Description
`–e`	(End-to-End). Transmit an end-to-end OAM loop cell, to be looped by the user connection point.
`–s`	(Segment). Transmit a segment OAM loop cell, to be looped by the first network connection point.
`–c count`	Transmit the specified number of cells. If this argument is not specified, the count defaults to 0 (zero), which means that the cells are transmitted continuously until the administrator sends an interrupt by pressing Ctrl+C.
`–i sec`	Transmit the cells at the specified interval, 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 To transmit 10 cells end-to-end:

```
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 carry out commands on that slot card.

Permission level `diagnostic`

Usage `open` *`shelf`* [*`slot`*]

Command element	Description
`shelf`	The shelf number (always 1).
`slot`	The number of the expansion slot you want to diagnose.

Example 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 `system`

Usage `ospf [options]`

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

Command element	Description
`?`	Display help information.
size	Display size of the OSPF routing table.
areas	Display OSPF areas.
stats	Display OSPF statistics.
`intf [ip_addr]`	Display information about one or more OSPF interfaces.
`translators`	Display the router IDs of not-so-stubby area (NSSA) border routers.
`lsa area ls-type ls-id ls-orig`	Display detailed information about OSPF LSAs. ■ *area* is the area ID. ■ *ls-type* is the LSA type. You can specify one of the following options for *ls-type*: – `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 autonomous system boundary routers. ■ *ls-id* is the target address of the router. ■ *ls-orig* is the address of the advertising router.
`lsdb [area]`	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).

Command element	Description
`nbrs [ip_addr]`	Display information about one or more OSPF neighbors.
`routers`	Display OSPF router information.
`ext`	Display OSPF external autonomous system advertisements.
`rtab`	Display OSPF routing table.
`database ext`	Display OSPF database summary.
`internal`	Display OSPF internal routes.

Example *Displaying the size of the OSPF routing table*

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

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

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

The fields in the output contain the following information:

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

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

Example *Displaying OSPF areas*

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

```
admin> ospf areas
Area ID Authentication Area Type #ifcs  #nets  #rtrs  #brdrs  #intnr
0.0.0.0 Simple-passwd  Normal     1      0      2      0       3
```

The fields in the output contain the following information:

Field	Specifies
Area ID	Area number in dotted decimal format.
Authentication	Type of authentication: `Simple-passwd`, `MD5`, or `Null`.
Area Type	Type of OSPF area: `Normal`, `Stub`, or `NSSA`.
#ifcs	Number of 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 ABRs in the area.
#intnr	Number of reachable internal routers in the area.

Example *Displaying general information about OSPF*

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

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

```
Incremental ext.(5) updates:  0   Incremental ext.(7) updates:   0
External (type-5) LSA database -
Current state:                Normal
Number of LSAs:               1
Number of overflows:          0
```

The fields in the output contain the following information:

Field	Specifies
OSPF version	Version of the OSPF protocols running.
OSPF Router ID	IP address assigned to the TAOS unit, which is typically the address specified for the Ethernet interface.
AS boundary capability	Yes if the TAOS unit functions as an autonomous system border router (ASBR) or No if it does not function as an ASBR.
Attached areas	Number of areas to which this 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).

Field	Specifies
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.
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.

Example *Displaying summarized information about OSPF interfaces*

To display summarized information about OSPF interfaces:

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

The fields in the output contain the following information:

Field	Specifies
Ifc Address	Address assigned to the TAOS unit's Ethernet interface. To identify WAN links, use the `Type` and `State` fields.
Phys	Name of the interface or the `connection` profile for WAN links.
Assoc. Area	Area in which the interface resides.
Type	Point-to-point (`P-P`) or broadcast (`Bcast`). WAN links are P-P links.
State	State of the link according to RFC 1583. There are many possible states, and not all states apply to all interfaces.

Field	Specifies
#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.

Example *Displaying information about a specific OSPF interface*

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

```
ospf intf ip_addr
```

For example:

```
admin> ospf intf 200.194.194.2
              Interface address:      200.194.194.2
              Attached area:          0.0.0.0
              Physical interface:     phani (wan1)
              Interface mask:         255.255.255.255
              Interface type:         P-P
              State:                  (0x8) P-P
              Designated Router:      0.0.0.0
              Backup DR:              0.0.0.0
              Remote Address:         200.194.194.3
DR Priority:       5  Hello interval:  30   Rxmt interval:  5
Dead interval:   120  TX delay:         1   Poll interval:  0
Max pkt size:   1500  TOS 0 cost:      10
# Neighbors:       1  # Adjacencies:    1   # Full 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.

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

Example *Displaying OSPF link state advertisements (LSAs)*

To specify an LSA to be expanded, use the following format for the ospf command:

ospf lsa *area ls-type ls-id ls-orig*

The command requires that you include the first four fields of the LSA as listed in the database. You can select the first four fields and paste them in after typing the command.

For example, to show an expanded view of an autonomous system external (ASE) LSA for area 0.0.0.0, where the target address of the router is 10.5.2.160 and the address of the advertising router is 10.5.2.162:

```
admin> ospf lsa 0.0.0.0 ase 10.5.2.160 10.5.2.162
LSA  type: ASE ls id: 10.5.2.160 adv rtr: 110.5.2.162 age: 568
          seq #: 80000037 cksum: 0xfffa
          Net mask: 255.255.255.255 Tos 0 metric: 10 E type: 1
          Forwarding Address: 0.0.0.0 Tag: c0000000
```

The fields in the output contain the following information:

Field	Specifies
LSA type	Type of LSA.
ls id	Target address of the router.
adv rtr	Address of the advertising router.
age	Age of the route in seconds.

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

Example *Displaying an expanded view of a router LSA*

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

```
admin> ospf lsa 0.0.0.0 rtr 202.1.1.1 202.1.1.1
        LS age:      66
        LS options:  (0x2) E
        LS type:     1
        LS ID (destination): 202.1.1.1
        LS originator:       202.1.1.1
        LS sequence no:      0x80000399
        LS checksum:         0xb449
        LS length:           48
        Router type:     (0x2) ASBR
        # router ifcs:   2
                Link ID:          10.105.0.8
                Link Data:        10.105.0.7
                Interface type:   (2) TrnsNetwork
                        No. of metrics: 0
                        TOS 0 metric:   10 (0)
                Link ID:          10.123.0.6
                Link Data:        10.123.0.7
                Interface type:   (2) TrnsNetwork
                        No. of metrics: 0
                        TOS 0 metric:   10 (0)
```

The fields in the output contain the following information:

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

Field	Specifies
LS type	Type of link as defined in RFC 1583: ■ Type 1 (RTR) are router-LSAs that describe the collected states of the router's interfaces. ■ Type 2 (NET) are network-LSAs that describe the set of routers attached to the network. ■ Types 3 and 4 (SUM) describe routes to networks in remote areas, or autonomous system boundary routers. ■ Type 5 (ASE) are autonomous system external (ASE) LSAs that describe routes to destinations external to the autonomous system. A default route for the autonomous system can also be described by an ASE LSA.
LS ID	IP address of the advertisement's destination.
LS originator	IP address of the advertisement's source.
LS sequence no	Number that begins with 80000000 and increments by one for each LSA. It is used for detecting old and duplicate LSAs.
LS checksum	A checksum covering the entire packet, except for the 64-bit authentication field.
LS length	Length of the LSA in bytes.
Router type	Type of router, either ASBR or ABR.
# router ifcs	Number of interfaces on the router.
Link ID	IP address of the associated router interface.
Link Data	Name of the device on the other side of the link.
Interface type	Type of interface: ■ 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 (TOS) for the LSA.
metric	Cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.

Example *Displaying an expanded view of a network LSA*

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

```
admin> ospf lsa 0.0.0.0 net 100.103.100.204 10.103.0.204
        LS age:      814
        LS options:  (0x2) E
        LS type:     2
        LS ID (destination): 100.103.100.204
        LS originator:       10.103.0.204
        LS sequence no:      0x80000027
        LS checksum:         0x8f32
        LS length:           36
        Network mask:        255.255.0.0
                Attached Router: 10.103.0.204     (1)
                Attached Router: 10.103.0.254     (1)
                Attached Router: 10.123.0.254     (1)
```

The fields in the output contain the following information:

Field	Specifies
`LS age`	Age of the LSA in seconds.
`LS options`	Optional functions associated with the LSA. When `E` is specified, entire OSPF areas can be configured as stub areas. When `T` is specified, routes only for TOS 0 are calculated.
`LS type`	Type of link as defined in RFC 1583: ■ Type 1 (`RTR`) are router-LSAs that describe the collected states of the router's interfaces. ■ Type 2 (`NET`) are network-LSAs that describe the set of routers attached to the network. ■ Types 3 and 4 (`SUM`) describe routes to networks in remote areas, or autonomous system boundary routers. ■ Type 5 (`ASE`) are autonomous system external (ASE) LSAs that describe routes to destinations external to the autonomous system. A default route for the autonomous system can also be described by an ASE LSA.
`LS ID`	IP address of the advertisement's destination.
`LS originator`	IP address of the advertisement's source.
`LS sequence no`	Number that begins with 80000000 and increments by one for each LSA. It is used for detecting old and duplicate LSAs.
`LS checksum`	A checksum covering the entire packet, except for the 64-bit authentication field.
`LS length`	Length of the LSA in bytes.
`Network mask`	Subnet mask.
`Attached Router`	Another router running OSPF on the network. The number in parentheses is the cost to that router.

Example *Displaying the OSPF link-state database*

To display the link-state database for the first configured area (or for the only defined area), include the `lsdb` option with the `ospf` command. For example:

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

The fields in the output contain the following information:

Field	Specifies
`Area`	Area ID.
`Type`	Type of link as defined in RFC 1583: ■ Type 1 (`RTR`) are router-LSAs that describe the collected states of the router's interfaces. ■ Type 2 (`NET`) are network-LSAs that describe the set of routers attached to the network. ■ Types 3 and 4 (`SUM`) describe routes to networks in remote areas, or autonomous system boundary routers. ■ Type 7 are ASE-7 link advertisements that are only flooded within an NSSA.
`LS ID`	Specifies the target address of the route.
`LS originator`	Specifies the address of the advertising router.
`Seqno`	Indicates a hexadecimal number that begins with 80000000 and increments by one for each LSA received.
`Age`	Specifies the age of the route in seconds.
`Xsum`	Indicates the checksum of the LSA.
`advertisements`	Specifies the total number of entries in the link-state database.
`Checksum total`	Indicates the checksum of the link-state database.

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

Example *Displaying OSPF neighbor information*

To display information about OSPF neighbors to the 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.
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.

Field	Specifies
Physical interface	The name of the interface on which the unit and the neighbor communicate: ■ ie0 or ie[*shelf*]-[*slot*]-[*item*] is an Ethernet interface. The shelf number is always 1. ■ wanN is a WAN connection, entered as it becomes active.
DR choice	IP address of the neighbor's designated router.
Backup choice	IP address of the neighbor's backup designated router.
DR Priority	Priority of the designated router.
DB summary qlen	Number of LSAs in the database summary list.
LS rxl qlen	Number of LSAs in the retransmission list.
LS req qlen	Number of LSAs in the request list.
Last hello	How long ago (in seconds) a hello packet was received.
# LS rxmits	Number of link-state update retransmissions.
# Direct acks	Number of direct acknowledgments sent.
# Dup LS rcvd	Number of duplicate LSAs received.
# Old LS rcvd	Number of old link-state updates received.
# Dup acks rcv	Number of duplicate acknowledgments received.
# Nbr losses	Number of times the neighbor went offline.
# Adj. resets	Number of times the adjacency has been re-established after a restart.

Example *Displaying OSPF routers*

To display OSPF routers, include the routers option with the ospf command. For example:

```
admin> ospf routers
DType  RType  Destination    Area      Cost    Next hop(s)     #
ASBR   OSPF   200.192.192.3  0.0.0.0   10      200.194.194.3   2
```

The fields in the output contain the following information:

Field	Specifies
DType	Internal route type.
RType	internal router type.
Destination	Router's IP address.
Area	Area in which the router resides.
Cost	Cost of the router.

Field	Specifies
Next hop(s)	Next hop in the route to the destination.
#	Number of the interface used to reach the destination.

Example *Displaying OSPF external autonomous system advertisements*

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

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

The fields in the output contain the following information:

Field	Specifies
Type	ASE5.
LS ID	Target address of the route.
LS originator	Address of the advertising router.
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.
# advertisements	Total number of entries in the ASE5 database.
Checksum total	Checksum of the ASE5 database.

Example *Displaying the OSPF routing table*

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

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

The fields in the output contain the following information:

Field	Specifies
DType	Internal route type. DType displays one of the following values: RTE (generic route), ASBR (autonomous system border route), or BR (area border route).
RType	Internal router type. RType displays one of the following values: FIX (static route), NONE, DEL (deleted), OSPF (OSPF-computed), OSE1 (type 1 external), or OSE2 (type 2 external).
Destination	Destination address and subnet mask of the route.
Area	Area ID of the route.
Cost	Cost of the route.
Flags	Hexadecimal number representing an internal flag.
Next hop(s)	Next hop in the route to the destination.
#	Number of the interface used to reach the destination.

Example *Displaying summarized OSPF database information*

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

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

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

If you specify the *ext* option, the 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: ■ Type 1 (RTR) are router-LSAs that describe the collected states of the router's interfaces. ■ Type 2 (NET) are network-LSAs that describe the set of routers attached to the network. ■ Types 3 and 4 (SUM) describe routes to networks in remote areas, or autonomous system boundary routers. ■ Type 5 (ASE) are autonomous system external (ASE) LSAs that describe routes to destinations external to the autonomous system. A default route for the autonomous system can also be described by an ASE LSA. ■ Type 7 are ASE-7 link advertisements that are only flooded within an NSSA.
LS ID	Target address of the route.
LS originator	Address of the advertising router.
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.
# advertisements	Total number of entries in the database.
Checksum total	Checksum of the database.

Example *Displaying internal OSPF routes*

When the TAOS unit uses the internal routes feature, it exports routes by means of the router LSA (type 1), instead of by means of the usual ASE-5. If the 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:

admin> **ospf internal**

```
               Area: 0.0.0.0
Destination     Mask              Cost
10.5.2.160      255.255.255.255     10
10.5.2.161      255.255.255.255     10
100.5.4.78      255.255.255.0       10
```

The fields in the output contain the following information:

Field	Specifies
`Area`	Name of the area.
`Destination`	Destination of the route.
`Mask`	Subnet mask for the route.
`Cost`	Cost of the route.

P

ping

Description Sends Internet Control Message Protocol (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`*

Command 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 To send ICMP echo request packets to host-231:

```
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, 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
```

To check the power supply on an APX unit:

```
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 slot card, displays general Primary Rate Interface (PRI) messages, shows a timestamp relative to the time the card booted, and identifies PRI messages that have cyclic redundancy check (CRC) errors or that are too long.

You can use `pridisplay` on a T1, E1, or T3 card only. You must first carry out the `open` command to open a session with the card.

Permission level `diagnostic`

Usage `pridisplay` *octets* [*line*]

Command element	Description
octets	The maximum number of octets to display per message. If you specify 0 (zero), the TAOS unit does not display any data.
line	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 `user`

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

Command element	Description
`-s [profile_name]`	If *profile_name* 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.
`-f [-f]`	Flush all cached entries. The second `-f` flag specifies that all cached routes are flushed without waiting for confirmation.
`-t`	Toggle debug output.

Example *Displaying statistics for all cached private-route profiles*

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
```

Following are the fields in the 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.

Example *Displaying statistics for a specified private-route profile*

To display statistics for statistics for the private-route profile named `check`:

```
admin> prtcache -s check
Profile Name     Created    Exp After(min)   Use Count   Refresh Cache
_____________________________________________________________________
check           12:32:53   1                0          Yes
```

Example *Flushing all cached private-route profiles*

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.

Q

quiesce

Description Deactivates individual T1 Primary Rate Interface (PRI) lines or channels connected to the TAOS unit by busying them out or taking them out of service. Deactivating the line does not end calls that are currently active on the line. When an active call disconnects, that channel is taken out of service.

Using the `quiesce` command for a line is equivalent to setting the `maintenance-state` parameter in the `t1` profile to `yes`. Restoring the line sets the parameter to `no`. When the parameter is set to `yes`, individual channels on that line cannot be restored. This setting is preserved across power ups.

Permission level `system`

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

Command element	Description
`-d`	Deactivate a single DS0 channel.
`-e`	Restore a single DS0 channel that has been deactivated.
`-r` *`line`*	Restore the specified T1 PRI line that has been deactivated.
`-q` *`line`*	Deactivate the specified T1 PRI line.
`-t`	Toggle debug display.

Example To deactivate 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
```

Note Restoring a deactivated 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.

Dependencies The specified T1 line must be enabled and configured for T1 PRI. 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 T1 PRI line out of service. The line-status window displays the condition as an `o` in an out of service channel. When all channels on the line are out of service, 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 out of service. There is no sure way for the TAOS unit to tell the switch to take a channel out of service. Because channels cannot be taken out of service, incoming calls are presented to the TAOS unit even if the T1 PRI line is deactivated. 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, active trunk in the hunt group.

quit

Description Terminates the current Telnet session.

Permission level `user`

Usage `quit`

Example To end the current Telnet session:

```
admin> quit
Connection closed by foreign host.
my-station%
```

R

read

Description Reads a copy of the specified profile into the edit buffer, making it the working profile. If the profile is one of a kind, such as the `ip-global` profile, it has no index field. If an index field exists for a profile, it must be specified on the command line.

Only the working profile can be modified. The `set` and `list` commands apply only to the working profile.

Note The working profile remains in the edit buffer until you overwrite the buffer with another `read` command or the `new` command. To save changes made in the buffer, you must use the `write` command.

Permission level `system`

Usage `read` *`profile-type`* [*`profile-index`*][`-f`]

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

By default, 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.

Example *Reading a profile on an APX unit*

To find the right index for an `ip-interface` profile, read that profile, and list its contents:

```
admin> dir ip-interface
66  10/20/2001 14:02:02  { { shelf-1 slot-12 1 } 0 }
66  10/27/2001 16:34:40  { { shelf-1 slot-12 2 } 0 }
66  10/27/2001 16:34:47  { { shelf-1 slot-12 3 } 0 }
66  10/27/2001 16:34:54  { { shelf-1 slot-12 4 } 0 }
66  10/28/2001 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 = 10.10.10.10
proxy-mode = Off
rip-mode = routing-off
route-filter = ""
rip2-use-multicast = yes
ospf = { no 0.0.0.0 normal 10 40 5 simple ascend0 0 1 16777215 +
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
directed-broadcast-allowed = yes
vrouter = ""
management-only-interface = no
```

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 run 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 = 10.10.10.10
proxy-mode = Off
rip-mode = routing-off
route-filter = ""
rip2-use-multicast = yes
ospf = { no 0.0.0.0 normal 10 40 5 simple ascend0 0 1 16777215 +
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
directed-broadcast-allowed = yes
vrouter = ""
management-only-interface = no
```

Example *Reading a profile on a MAX TNT unit*

To find the index for an `ip-interface` profile, read the profile, and list its contents:

```
admin> dir ip-interface
66  12/20/2001 14:02:02  { { shelf-1 slot-12 1 } 0 }
66  12/27/2001 16:34:40  { { shelf-1 slot-12 2 } 0 }
66  12/27/2001 16:34:47  { { shelf-1 slot-12 3 } 0 }
66  12/27/2001 16:34:54  { { shelf-1 slot-12 4 } 0 }
66  12/28/2001 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 = 10.10.10.10
proxy-mode = Off
rip-mode = routing-off
route-filter = ""
rip2-use-multicast = yes
ospf = { no 0.0.0.0 normal 10 40 5 simple ascend0 0 1 16777215 +
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
directed-broadcast-allowed = yes
vrouter = ""
management-only-interface = no
```

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 run 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 = 10.10.10.10
proxy-mode = Off
rip-mode = routing-off
route-filter = ""
rip2-use-multicast = yes
ospf = { no 0.0.0.0 normal 10 40 5 simple ascend0 0 1 16777215 +
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
directed-broadcast-allowed = yes
vrouter = ""
management-only-interface = no
```

See Also `get, list, new, set, write`

readflash

Description Displays the contents of PCMCIA flash memory cards `flash-card-1` and `flash-card-2`.

Permission level `update`

Usage `readflash`

Example To display flash card contents:

```
admin> readflash
Flash1 (task "CLI session input task" at 0x80ba2810, time: 71861.25) 64
octets @ 0x80659308
[0000]: a6 0a 0d 00 d6 ec a6 3d 1f 8b 08 00 00 00 00 00
[0010]: 02 03 ec fd 7f 7c 9c 65 95 3f 0e 9f b9 67 26 99
[0020]: a6 d3 f6 4e 3a 4d a7 a5 94 49 72 67 12 da 04 87
[0030]: 12 24 48 90 21 49 a1 2a 6a 5a 42 ad 82 18 d3 02
Flash2 (task "CLI session input task" at 0x80ba2810, time: 71861.25) 64
octets @ 0x80659308
[0000]: a6 0a 0d 00 d6 ec a6 3d 1f 8b 08 00 00 00 00 00
[0010]: 02 03 ec fd 7f 7c 9c 65 95 3f 0e 9f b9 67 26 99
[0020]: a6 d3 f6 4e 3a 4d a7 a5 94 49 72 67 12 da 04 87
[0030]: 12 24 48 90 21 49 a1 2a 6a 5a 42 ad 82 18 d3 02
```

Dependencies The `readflash` command requires that you enable diagnostic output.

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 occurs 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]`

Command element	Description
`-f`	Force a switchover without prompting for confirmation.

Example To force a switchover without prompting for confirmation:

```
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`

Command element	Description
`-a`	Refresh all types of configuration.
`-n`	Refresh dedicated profile 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.

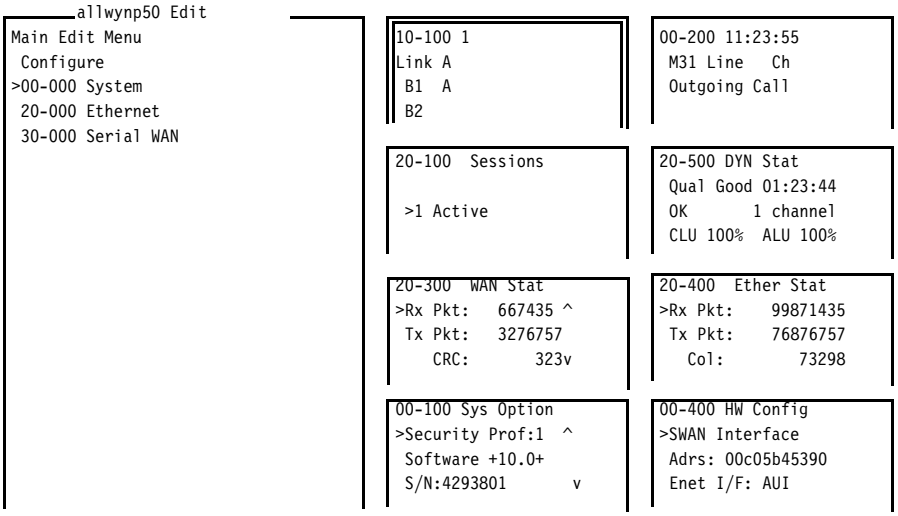
Permission level `diagnostic`

Usage `remote` *`station_name`*

Command element	Description
`station_name`	Specifies the station name of the remote device. The value you enter must match the value of a `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
```



To exit from the remote management session and return to the command-line interface session on the shelf controller, type Ctrl+C three times in quick succession. Either end of the connection can terminate a Multilink Protocol Plus™ (MP+) connection by hanging up all channels of the connection.

The 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:

Error message	Explanation
`not authorized`	Permissions are insufficient for beginning a remote management session. You must authenticate a `user` profile that enables the `system` permission.
`cannot find profile for` *`station`*	No profile was found for the specified station name.
`profile for` *`station`* `does not specify MPP`	A profile was located for the station name, but it did not specify the MP+ encapsulation protocol.
`cannot establish connection for` *`station`*	The MP+ connection to the remote station could not be established.
`station` `did not negotiate MPP`	The remote station did not negotiate an MP+ connection.
`far end does not support remote management`	The remote station is running a version of TAOS that does not support remote management.
`management session failed`	A temporary condition, such as premature termination of the connection, caused the management session to fail.
`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 restart the idle timer. Therefore, the `idle` parameter in the `connection` profile at both the calling and answering ends of the connection must be disabled during a remote management session, and restored just before exiting.
- Remote management works best at higher terminal speeds.

reset

Description Restarts the TAOS unit, one redundant shelf controller, or both redundant shelf controllers. When you restart the unit, all active connections are terminated. All users are logged out and the default security level is reactivated. In addition, a system restart can cause a WAN line to temporarily be shut down because of a momentary loss of signaling or framing information. After a restart, the TAOS unit runs a power-on self test (POST).

Permission level `update`

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

Command element	Description
No options	Restart the unit, one redundant controller, or both redundant controllers. On an APX unit, using the `reset` command with no options restarts 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 restart the primary controller.
`-f`	Force a restart without prompting for confirmation.
`-a`	Restart the shelf controller.
`-r` *`controller`*	Restart one or both redundant controllers. For *`controller`*, you can specify one of the following: ■ `primary`—Restart the primary controller. ■ `secondary`—Restart the secondary controller. ■ `both`—Restart both controllers.

Example To restart a MAX TNT unit:

```
admin> reset
```

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

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

The following command restarts the primary controller:

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

The following command restarts 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`

rm

Description Deletes a file or directory.

Permission level system

Usage rm *socket/path*

Command element	Description
socket	PCMCIA flash memory card number.
path	Subdirectory to be deleted.

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

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

See Also ls, mkdir, mv

routecall

Description Tests call routing by simulating an incoming or outgoing call and verifying to which slot card the call is routed.

Permission level diagnostic

Usage routecall [-c a | d | p | t| v | 1] [-d {{*shelf slot item*} *logical-item*}] [-f {{*shelf slot item*} *logical-item*}] [-n *numChans*] [-p *phoneNumber*] [-r d | h | n][-v 1 | 3 | 8| 9 | f | r | u] [-s {{*shelf slot item*} *logical-item*}]

Command element	Description
-c	Specifies the type of incoming call to simulate. Following are the available options: ■ a—analog call ■ d—digital call ■ p—PHS call ■ t—trunk call ■ v—Voice over IP (VoIP) call ■ 1 (one)—V.110 call
-d {{*shelf slot item*} *logical-item*}	Specifies the destination device. The default is {{0 0 0}0}.
-f {{*shelf slot item*} *logical-item*}	Frees the device allocated for the routecall command.
-n *numChans*	Specifies the number of channels needed for the call. The default is 1.
-p *phoneNumber*	Specifies the telephone number for the incoming call. The default is null.

Command element	Description
`-r`	Specifies the type of slot card to which to route the incoming call. Following are the available options: ■ `d`—dual ■ `h`—host (the default) ■ `n`—network
`-v`	Specifies the codec to use for a VoIP call. Following are the available options: ■ 1 (one)—G.711 ■ 3—G.723 ■ 8—G.728 ■ 9—G.729 ■ `f`—Full rate GSM ■ `r`—RT-24 ■ `u`—Unknown (the default)
`-s {{`*`shelf slot item`*`}` *`logical-item`*`}`	Specifies the source device. The default is `{{0 0 0}0}`.

Example For an incoming digital call from the line card in slot 23:

```
admin> routecall -c d -r h -s {{ 1 23 }}
Call will be route to device(s): 1:27:6/25
```

For an outgoing call from the host card in slot 15:

```
admin> routecall -c t -r n -s {{ 1 15 }}
Call will be route to device(s): 1:23:1/1
```

To free all the allocated resources.

```
admin> routecall -f {{1 27 6 }}
```

S

save

Description Saves all profiles, all profiles of a given type, or a specific profile to a file or PCMCIA flash memory 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 Trivial File Transfer Protocol (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*]

Command 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 *encryption_type password*	Use encryption. The *encryption_type* argument specifies the method to be used for encryption and decryption. You can specify des or md5. The *password* argument specifies the password used to generate the key for encryption and decryption. The -e option supports only a network target.
target	The destination of the file to be saved. Following are valid specifications: ■ network *host filename*— A network hostname or IP address and the name of the file on that host. ■ console— The PC you are using in a terminal session. ■ flash *device/filename*—The PCMCIA flash memory card.
profile-type	The type of profile to be read, or the profile itself if it does not require an index specification.
profile-index	The name or address that distinguishes a profile from others of the same type. To see profile indexes, enter the dir command (dir *profile-type*).
network *host filename*	The hostname or IP address of the source network and the name of the file on that host.
-p *profile1*, *profile2*...	Save the specified list of profiles.
-x *profile1*, *profile2*...	Save all profiles, except those in the specified list.

Example *Saving all profiles of a specified type*

To save 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.

Example *Saving an entire configuration to a hard disk*

To save the entire configuration to a hard disk, start the capture utility and specify the `console` option:

```
admin> save console
; saving all profiles
...
```

All configured profiles and parameters scroll to the capture buffer. When the entire configuration has been displayed, the following output appears:

```
;
;
; all profiles saved
```

To save the file, stop the capture.

Example *Saving a specific profile to a file on a network host*

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
```

Example *Saving a configuration in Data Encryption Standard (DES)-encrypted format*

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:

Error message	Explanation
`-e option:unknown encryption method` *`method`*	You specified an incorrect encryption method when you saved the configuration.
`File is corrupted, Encryption tag not found`	The configuration file is corrupted.
`File is corrupted, Version tag not found`	
`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`

sca

Description Displays or clears Serial Communications Adapter (SCA) statistics. You must first carry out the `open` command to open a session with a T1 or E1 FrameLine slot card.

Permission level `diagnostic`

Usage `sca [-s] [-c] [-p]`

Command element	Description
`-s`	Show statistics
`-c`	Clear statistics
`-p`	Toggle continuous stats display

Example To open a session with a card in slot 2:

```
admin> open 1 2
```

To display SCA statistics:

```
ue1-1/2> sca -s
SCA statistics :
01/00:rx(Bad,Abort,CRC,Ovr,Residu,short)=0, 0, 0, 0, 0, 0
rx(#good,#octets)=60, 895
tx(#good,#octets)=23891, 35842664
buffers in queue(#rx,#tx)=30, 292
01/01:rx(Bad,Abort,CRC,Ovr,Residu,short)=0, 0, 0, 0, 0, 0
```

```
rx(#good,#octets)=21083, 31480862
tx(#good,#octets)=74646, 112039744
buffers in queue(#rx,#tx)=13, 16
01/02:rx(Bad,Abort,CRC,Ovr,Residu,short)=0, 0, 0, 0, 0, 0
rx(#good,#octets)=16, 228
tx(#good,#octets)=15345, 23052042
buffers in queue(#rx,#tx)=14, 17
```

screen

Description Changes window display sizes for the current session only.

Permission level system

Usage screen *screen-length* [*status-length*] [-w *width*]

Command element	Description
screen-length	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
status-length	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 *status-length* value must be less than the *screen-length* by at least six lines.
-w *width*	The width of the screen. You can specify a value for *width* from 80 through 256. The default is 80. The specified screen width is the number of characters that are visible without scrolling, including the system prompt and spaces following it. For example, if the screen width is 80 characters and the prompt is admin> (a 6-character prompt followed by a space), the maximum number of visible characters in a command is 72. The user can scroll to the characters not currently visible by moving the cursor left or right. The control sequence Ctrl+L, Ctrl+R enables you to redraw the current line.

If the status window is open when you run the screen command, the window is resized dynamically. If it is not open, the status window is resized when you next open it.

Example 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*|?

Command element	Description
param-name	Name of the parameter in the current or specified context of the working profile.
param-index	Parameter index, which might be required for some complex or array parameters. (See the physical address example below.)
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 To open the line-interface subprofile and set the telephone 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
isdn-emulation-side = te
robbed-bit-mode = wink-start
default-call-type = digital
switch-type = att-pri
nfas-group-id = 0
nfas-id = 0
incoming-call-handling = internal-processing
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
overlap-receiving = no
pri-prefix-number = ""
trailing-digits = 2
t302-timer = 10000
channel-config = [ { switched-channel 9 "" 1 255 } { switched-channe+
maintenance-state = no
input-sample-count = one-sample
sendDisc-val = 0
hunt-grp-phone-number-1 = ""
hunt-grp-phone-number-2 = ""
hunt-grp-phone-number-3 = ""
collect-incoming-digits = no
t1-inter-digit-timeout = 3000
r1-use-anir = no
r1-first-digit-timer = 340
r1-anir-delay = 350
r1-anir-timer = 200
r1-modified = no
first-ds0 = 0
last-ds0 = 0
nailed-group = 32768
ss7-continuity = { loopback single-tone-2010 }
admin> set channel 1 phone = 5551212
admin> write
T1/{ shelf-1 slot-2 1 } written
```

See Also list, new, read, write

set rule

Description Specifies a Border Gateway Protocol (BGP) policy as an acceptance policy, an injection policy, or an advertisement policy.

Permission level system

Usage Specifying up to 79 characters, you configure an acceptance policy with the following rules:

```
set rule rulenumber permit|deny|include policyname
    [if
        [prefix [exactly] prefix/subnetmask]
        [prefix-longer-than subnetmask]
        [as-path string|empty]
        [community tag]]
    [then
        [input-multi-exit-disc number|strip]
        [degree-of-preference number]]
```

You configure an injection policy with the following rules:

```
set rule rulenumber permit|deny|include policyname
    [if
        [prefix [exactly] prefix/subnetmask]
        [as-path string|empty]
        [community tag]]
```

You configure an advertisement policy with the following rules:

```
set rule rulenumber permit|deny|include policyname
    [if
        [prefix [exactly] prefix/subnetmask]
        [as-path string|empty]
        [community tag]]
    [then
        [local-pref number]
        [output-multi-exit-disc number|strip]
        [next-hop ipaddress]
        [community add|strip tag]
        [ignore-community-restrictions]]
```

Following are the options you can specify:

Command element	Description
rulenumber	Number value from 1 to 20. ■ Use the *rulenumber* of an existing rule to replace that rule. ■ Add this rule to the end of the list of rules by using a *rulenumber* value that is 1 greater than the current largest rule number. ■ A maximum of 20 rules is permitted in a policy. If more rules are needed, they can be added with the `include` *policyname* option.
`permit`	Allows the IP prefix into the BGP routing table if the criteria in the rule are met.
`deny`	Prohibits the IP prefix from the BGP routing table if the criteria in the rule are met.
`include` *policyname*	Inserts an existing policy *policyname* into the current policy. Included policies can themselves include other policies, up to a maximum level of 10 nested included policies.

`if`	Compares the prospective IP prefix against corresponding elements specified after `if` in this rule. Specifying no `if` elements causes all prefixes to match the current rule. ■ If all elements of the IP prefix match these `if` criteria, this rule is applied to the prefix and the prefix is either permitted or denied. ■ If the elements do not match, the list of policy rules is further scanned for a matching rule. ■ If no matches are found, the IP prefix is denied from the BGP database.
`prefix` *prefix*`/`*subnetmask*	IP prefix and subnet mask to compare the prospective IP prefix against. The subnet mask indicates the number of high-order bits in the IP prefix. ■ Specify *prefix* in dotted decimal notation. ■ Specify *subnetmask* as a number from 1 through 32, preceded by a slash (/)—for example, /24. By default, any prefix that matches the subnet mask in the rule prefix in the leftmost—most significant—bits, matches the rule prefix.
`exactly`	Requires the entire prospective IP prefix and subnet mask to exactly match the IP prefix and subnet mask specified in the rule.
`prefix-longer-than` *subnetmask*	When used with the `deny` keyword, prohibits from the BGP routing table any prospective IP address with a prefix containing more high-order bits than are specified by the subnet mask.
`as-path` *string*	Autonomous system path *string* to compare the prospective IP prefix against. *string* is a list of autonomous system numbers, separated by periods (.)—for example, `AS1.AS2.AS3`. or `AS2.AS1`. When *string* is compared to an autonomous system path *sequence*, the order of the sequence must match the order of *string*. When *string* is compared to an autonomous system path *set*, the *set* is put in ascending numerical order, and then matched against *string*. Multiple sequences or sets in a single autonomous system path are concatenated before being compared to *string*. The following special characters have the following meaning in the expression: ■ An asterisk (*) matches one or more entries in the autonomous system sequence. ■ A question mark (?) matches any single item in the autonomous system sequence.

`empty`	Value for *`string`* that matches only paths containing no autonomous system path information. Use `as-path empty` only to permit or deny routes originating from an internal or confederation member peer within the autonomous system of the TAOS unit.
`community`	Identifier *`tag`* that categorizes one or more groups of destinations against which to compare the prospective IP prefix. See RFC 1997 for more information about BGP communities.
`tag`	Thirty-two-bit number that indicates a destination category in one of the following forms: ■ One 32-bit value identifying the autonomous system of the destination ■ Two 16-bit values: one containing the autonomous system number of the destination, and the other containing additional information about the autonomous system. If only the first 16-bit word is considered significant in matching the community *`tag`*, replace the second 16-bit value with the keyword `any`. ■ One of the following reserved community keywords that restrict route advertisement for peers receiving the route information: – `no-export`—Destinations only within a confederation. Advertise the route only to BGP peers within your confederation or autonomous system. – `no-advertise`—No destinations. Do not advertise this route. – `no-export-subconfed`—Internal destinations only. Advertise this route only to internal BGP peers. The restrictions imposed by these reserved community keywords do not apply to the TAOS unit originating this information.
`then`	Assigns the following metric or metrics to any IP prefix selected for acceptance by the rule.
`input-multi-exit-disc` *`number`*`|strip`	Assigns an arbitrary *`number`* for the learned multiexit discriminator, overriding any that is learned from the peer. *`number`* is a 32-bit integer. The `strip` keyword causes any multiexit discriminator information learned from a peer to be ignored. `input-multi-exit-disc` can be abbreviated as `imed` in this command. Lower numbers indicate an increased preference for a specific route. Use this metric to discriminate among multiple exit or entry points between the same pair of neighboring autonomous systems.

`degree-of-preference` *number*	Assigns a degree-of-preference *number* to a route. *number* is a 32-bit integer. `degree-of-preference` can be abbreviated as `dop` in this command Higher numbers indicate an increased preference for a specific route when more than one route exists. Use this metric to screen a particular autonomous system from your map of routes, for example. If you do not assign a degree of preference to the IP prefix, one of the following values is assigned by default: ■ If the route comes from an internal peer, the learned local preference number is assigned. ■ If the route comes from an external peer, *number* is based on the autonomous system path length, with a shorter path being preferred.
`local-pref` *number*	Assigns an arbitrary rating *number* to an external route for advertisement to internal or confederation-member peers only. *number* is a 32-bit integer. `local-pref` can be abbreviated as `lp` in this command. Higher numbers indicate an increased preference for a specific route when more than one route exists. Use this metric to screen a particular autonomous system from your map of routes, for example. If you do not assign a local preference rating to the IP prefix, one of the following values is assigned by default: ■ If the route comes from an internal peer, the learned local preference number is assigned. ■ If the route comes from an external peer, *number* is based on the autonomous system path length, with a shorter path being preferred.
`output-multi-exit-disc` *number*`|strip`	Assigns an arbitrary rating *number* for the multiexit discriminator to an external route for advertisement to external or confederation member peers only. *number* is a 32-bit integer. A multiexit discriminator configured in a policy takes precedence over one configured in a route summarization. `output-multi-exit-disc` can be abbreviated as `omed` in this command. Lower numbers indicate an increased preference for a specific route. Use this metric to discriminate among multiple exit or entry points between the same pair of neighboring autonomous systems.

	If you do not assign a multiexit discriminator, no value is sent unless the TAOS unit is advertising one of its own summarizations that specifies a multiexit discriminator. In this case, the value specified in the `bgp-summarization` profile is used if none is present in the policy. To avoid advertising any multiexit discriminator, use the `strip` keyword.
`next-hop` *`ipaddress`*	Assigns the IP address to advertise as the next hop. If you do not assign a value, a value is computed automatically for the best possible next hop to reach this route. Note that setting this parameter in a policy takes precedence over over setting the `always-next-hop` parameter in the `bgp-peer` profile
`add`	Adds the community categories identified in *`tag`* to the IP prefix to be advertised.
`strip`	Removes existing community categories from the IP prefix to be advertised.
`ignore-community-restrictions`	Instructs the TAOS unit to ignore the restrictive keywords `no-advertise`, `no-export`, and `no-export-subconfed` when advertising this route to a peer. Use this keyword in the rule to override these restrictions received from other peers.

Example This section shows how to create a BGP policy with multiple rules that accepts routing information from just one peer. Before creating the policy, it is helpful to gather some information about the BGP configuration on the TAOS unit. Use the bgp `show peer` command to display BGP peer information. In the following example, the peers has been configured to accept, inject and advertise all routes:

```
admin> bgp show peer
Remote Peer           AS Flg  DM  Up  Accept  Inject  Advertise
-------------------------------------------------------------
apx1  (200.200.200.1) 2--         Up  all     all     all
```

The output shows that just one BGP peer, `apx1`, is configured to accept, inject, and advertise all routes.

Use the `bgp show path` command to display all the paths in the BGP routing table. For example:

```
admin> bgp show path
O:IGP
Sequence: 3
NH:200.200.200.3   LP:     100 MED Learned/Used:          0/
0
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.3
NLRI:+220.220.220.3/32/1/0
O:IGP
NH:200.200.200.1   LP:           8 MED Learned/Used:          8/
8
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+1.1.1.0/24/1/0 +134.112.30.254/32/1/0
```

```
NH:200.200.200.1   LP:          9 MED Learned/Used:          7/
7
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+12.12.12.0/24/1/0 +12.12.12.2/32/1/0
NH:200.200.200.1   LP:         16 MED Learned/Used:          0/
0
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+12.12.12.1/32/1/0 +131.108.0.0/24/1/0
134.112.30.0/24/1/0 +194.194.194.0/24/1/0
200.200.200.0/24/1/0 +202.202.202.0/24/1/0
+220.220.220.1/32/1/0 +221.221.221.1/32/1/0
NH:Self-generated  LP:         16 MED Learned/Used:          0/
0
Metrics to NH:60/2/1/4 Gateway to NH:134.112.30.1
NLRI:+220.220.220.9/32/4000/0 +200.200.200.0/24/4000/0
+199.199.199.0/24/4000/0 +134.112.30.0/24/4000/0
```

The network layer reachability information (NLRI) in the output shows all routes that are accepted from the peer. The following procedure shows how to create a policy (called `two_networks`) to permit two network routes (`194.194.194.0/24` and `1.1.1.0/24`):

1 Create the policy.

```
admin> new bgp-policy two_networks
BGP-POLICY/two_networks read
```

2 List the policy.

```
admin> list
[in BGP-POLICY/two_networks (new)]
name* = two_networks
next-policy = ""
rule = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" +
```

3 List the rule.

```
admin> list rule
[in BGP-POLICY/two_networks:rule (new)]
rule[1] = ""
rule[2] = ""
rule[3] = ""
rule[4] = ""
rule[5] = ""
rule[6] = ""
rule[7] = ""
rule[8] = ""
rule[9] = ""
rule[10] = ""
rule[11] = ""
rule[12] = ""
rule[13] = ""
rule[14] = ""
rule[15] = ""
rule[16] = ""
rule[17] = ""
rule[18] = ""
```

```
rule[19] = ""
rule[20] = ""
```

As the output shows, the policy is created with no rules.

4 Apply rules to the policy to permit routes from two networks and set the input multiexit discriminator and save your changes.

```
admin> set 1 = permit if prefix 194.194.194.0/24 then imed 5
admin> set 2 = permit if prefix 1.1.1.0/24 then imed 5
admin> write
BGP-POLICY/two_networks written
```

5 List the policy.

```
admin> list
[in BGP-POLICY/two_networks:rule]
rule[1] = "permit if prefix 194.194.194.0/24 then imed 5"
rule[2] = "permit if prefix 1.1.1.0/24 then imed 5"
rule[3] = ""
rule[4] = ""
. . .
```

6 Apply the policy as an acceptance policy to peer apx1.

```
apx1-admin> read bgp-peer apx1
BGP-PEER/apx1 read
apx1-admin> list
[in BGP-PEER/apx1]
peer-name* = apx1
enable = yes
peer-ip-address = 200.200.200.1
my-ip-address = 200.200.200.9
autonomous-system = 2
always-next-hop = no
route-reflector-client = no
confederation-member = no
default-gateway-metric = 0
accept-policy = all
inject-policy = all
advertise-policy = all
```

```
admin> set accept-policy = two_networks
admin> write
BGP-PEER/apx1 written
```

7 Use the `bgp show peer` command to display information about the peer.

```
admin> bgp show peer
Remote Peer           AS  Flg  DM  Up  Accept        Inject  Advertise
-------------------------------------------------------------------
apx1 (200.200.200.1)  2       --  Up  two_networks  all     all
```

The `two_networks` policy is listed under the `Accept` field.

8 Use the `bgp show path` command to display all the paths in the BGP routing table.

```
admin> bgp show path
O:IGP
NH:200.200.200.1   LP:          8 MED Learned/Used:          8/      5
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+1.1.1.0/24/1/0
NH:200.200.200.1   LP:         16 MED Learned/Used:          0/      5
Metrics to NH:0/32/0/3 Gateway to NH:200.200.200.1
NLRI:+194.194.194.0/24/1/0
```

Only the `194.194.194.0/24` and `1.1.1.0/24` networks are listed in the NLRI fields in the output to the `show peer` command, and they both use a multiexit discriminator of 5. This information appears because step 4 set the `two_networks` policy to accept routes only from those two networks, and set the multiexit discriminator to 5.

show

Description On an APX unit, displays information about installed slot cards and their status, as well as the communication status of the primary and secondary controllers. 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`*]]

Command element	Description
`shelf-number`	The shelf number (always 1).
`slot-number`	The number of an expansion slot.
`item-number`	The number of a specific item (device or channel) on the slot card.

Example *Displaying information about slot cards on an APX unit*

In the following example, the `show` command is run on the primary controller while the left controller is primary:

```
admin> show
Controller { left-controller } ( PRIMARY ):
                      Reqd   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 run 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 (POSTs).
`BOOT`	The card has been recognized by the shelf controller and has begun to carry out 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 restarted.
`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.

Example *Displaying information about slot cards on a MAX TNT unit*

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 (POSTs).
BOOT	The card has been recognized by the shelf controller and has begun to carry out 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 restarted.
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. The slot card state remains the same through a system restart 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.

Permission level `diagnostic`

Usage `slot [-u|-d|-r|-t|-b|-m|? -all][`*`shelf-number`*`][`*`slot-number`*`]`

Command element	Description
-u	Start up the specified slot card.
-d	Deactivate the specified slot card.
-r	Delete the profiles for a card that has been removed.
-t	Toggle the module debug level.
-b	Force a hardware restart.

Command element	Description
`-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.
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.

Example *Starting up a slot card*

To start 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.

Example *syslog message generated when a card is restarted*

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
```

Example *syslog message generated when a card is deactivated*

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 show record is generated:

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

Example *syslog message generated when a card is started up*

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
```

Example *NVRAM log message generated when a card is restarted*

When you use the slot -b command, the following nonvolatile RAM (NVRAM) record is generated:

```
SLOT CARD BOUNCED: Index: 220 Revision: 9.1 Slot shelf_num/slot_num
Date: 10/22/2001.       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: 9.1 Slot 1/6
Date: 10/22/2001.       Time: 12:35:05
Card bounced by 10.40.40.94, user profile admin.
```

Example *NVRAM log message generated when a card is deactivated*

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: 9.1 Slot 1/6
Date: 10/22/2001.       Time: 12:36:54
Card downed by 10.40.40.94, user profile admin.
```

Dependencies Any time the `-u` (start up), `-d` (deactivate), or `-m` (maintenance) option is entered, a warning message is sent to the console as a reminder that the slot state change is 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 deactivated even after a system restart.

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 NVRAM is cleared.

Caution If any errors occur during loading (for example, missing load images or corrupted images), the loader deactivates the slot card in question. You must manually start 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 user-based security model (USM) user.

Permission level `update`

Usage `snmpauthpass` *`username password`*

Command element	Description
`username`	SNMPv3 USM user for whom an authentication key is generated.
`password`	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 `snmpMgrStats, snmprivpass`

snmpMgrStats

Description Displays the number of invalid requests by SNMP managers.

Permission level system

Usage snmpMgrStats

Example To display the number of invalid requests:

```
admin> snmpmgrstats
SnmpManager       Illegal Access
200.165.64.50     0
200.166.65.51     0
200.167.66.52     0
200.168.67.53     0
200.169.68.54     0
200.170.69.55     6
```

See Also snmpauthpass, snmprivpass

snmprivpass

Description Generates the privacy key of an SNMPv3 USM user.

Permission level update

Usage snmpPrivPass *username password*

Command element	Description
username	SNMPv3 USM user for whom a privacy key is generated.
password	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, snmpMgrStats

sntp

Description Displays messages related to Simple Network Time Protocol (SNTP) functionality.

Permission level `system`

Usage `sntp [-d | -f ]`

Command element	Description
`-d`	Display SNTP information.
`-f`	Force an update of the time and date.

Permission level `To display SNTP information:`

```
admin> sntp -d
Mode: enabled
Max delta: 0, Last Delta: 0
Total SNTP updates: 0
System start time : Thu Mar 7 15:23:10 2002
Original system start time: Thu Mar 7 15:23:10 2002
Next request in 1 sec
admin> sntp -f
SNTP: client request
```

status

Description Displays the status windows. You can configure the content of the windows to show connection, line, or log-message information.

Permission level `system`

Usage `status [on|off]`

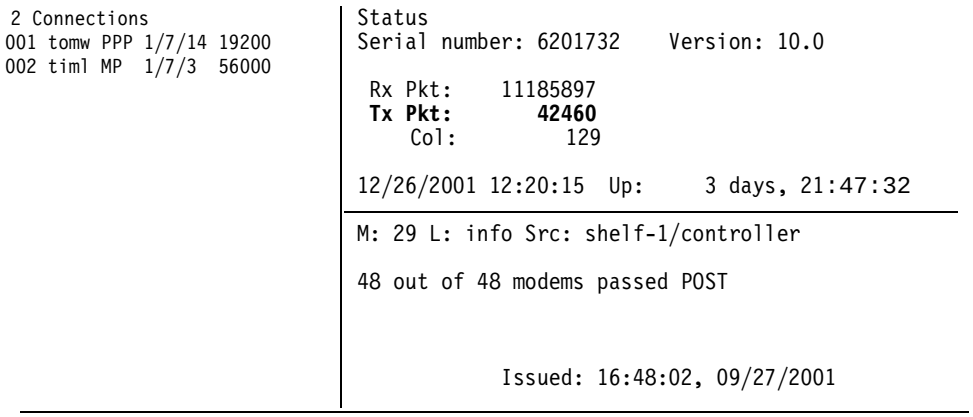
Command element	Description
`on`	Display the status windows.
`off`	Hide the status windows.

Example To display the status windows:

```
admin> status
```

or

```
admin> status on
```



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

Command element	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: ■ `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: ■ `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 `reqd-state` setting: ■ `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: ■ `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.

Dependencies 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.

T

t1channels

Description Displays administrative information about T1 channels.

Permission level `system`

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

Command element	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:

Field	Description
`dvOp`	The current operational state of the channel (also specified by `device-state`): ■ `Down` indicates that the channel is in a nonoperational state. ■ `Up` indicates that the channel is in normal operations mode.
`dvUpSt`	The status of the channel in normal operations mode: ■ `Idle` indicates that no call is on the line. ■ `Busy` indicates that the channel is handling a call.
`dvRq`	The required state of the channel as specified by `reqd-state`: ■ `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`): ■ `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.

Example *Displaying information about all available T1 channels*

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  )
```

Example *Listing disabled channels*

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  )
```

Example *Displaying all possible T1 channels*

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]
```

Example *Displaying the T1 channels in use*

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

```
admin> t1 -i
T1 channels allocated/in-use:
                                (dvOp  dvUpSt  dvRq  sAdm)
Channel { {  1 13  1 } 15 }   (UP    Busy    UP    UP  )
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  )
```

Dependencies 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.

See Also `line, show, slot`

t1-stats

Description Reports DS1-level line errors on a T1 or T3 card. You must first carry out the `open` command to open a session with the card.

Permission level `diagnostic`

Usage `t1-stats [-c] line`

Command element	Description
`-c`	Reset statistics to 0 (zero) after displaying them.
`line`	Line on the card.

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

```
admin> open 1 13
```

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
```

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 zeroes, 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 –c 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*]

Command 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.

Command element	Description
`-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 with `host-231`:

```
admin> telnet host-231
Connecting to host-231 (10.65.12.231)...
Escape character is '^]'
Connected
```

Dependencies 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`

terminal-server

Description Starts terminal-server mode, which has its own command interface.

Permission level `termserv`

Usage `terminal-server`

Example To start terminal-server mode:

```
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, telnet`

thermalstatus

Description Displays a number of temperature-related values to show the overall thermal status of the unit. The values include:

- Ambient temperature at fan tray intake.
- Shelf-controller temperature.
- High, low, and alarm temperature thresholds.
- Slot-card temperature for slot cards that support temperature reporting. Currently, no slot cards support thermal information reporting.
- Power supply thermal status, and whether the power supplies are in an overheated state.
- Fan tray status, including the fan tray operational mode, low-noise speed in revolutions per minute (RPM), current fan mode, and current speed of each fan in RPMs.

Permission level `system`

Usage `thermalstatus`

Example To display the overall thermal status of the unit:

```
admin> thermalstatus
System Thermal status
 Ambient temperature at intake : 27 C (80 F)
 Shelf controller temperature  : 35 C (95 F)
 High temperature threshold  : 36 C (96 F)
 Low temperature threshold   : 32 C (89 F)
 Alarm temperature threshold : 38 C (100 F)
Slot cards:
 (no slot cards contain thermal information)

Power supply thermal status
  Power Supply #       Temp
================================
    A                  OK
    B                  OK
    C                  n/a
    D                  OK


Fantray status
 Fan operational mode:  auto-regulation
 Low-noise RPM:         2000
 Current fan mode:      Full-speed
 Fan #         RPM              Status
=========================================
  1           3289             GOOD
  2           3214             GOOD
  3           3075             GOOD
  4           3143             GOOD
  5           3214             GOOD
  6           3289             GOOD
```

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 or 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 restarts, it loses the token information.

Permission level `system`

Usage tokencount [-a | -c *token* | -d | -e | -i | -u *num*] [*pattern*]

Command element	Description
-a	Set token counters to 0 (zero). If the system restarts, all token counters are set to 0 (zero). If a card restarts, counters on that card are set to 0 (zero).
-c *token*	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 *num*	Define a token-search pattern and assign it the specified number.
pattern	Pattern of the token to search for. 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 message	Explanation
`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 time-to-live (TTL) 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 time-out interval, the command output is an asterisk.

Because the destination host is not supposed to process the UDP probe packets, 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]`

Command element	Description
`-n`	Print hop addresses numerically rather than symbolically and numerically (this eliminates a name server address-to-name lookup for each gateway found on the path).
`-v`	Verbose output. Include received ICMP packets other than `time exceeded` and `port unreachable`.
`-m max_ttl`	Set the maximum TTL (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` (zero). This results in a datagram size of 38 bytes (a UDP packet carrying no data).

Example To trace the route an IP packet follows 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 annotation might indicate that there is a problem with the associated device.
!F	Fragmentation needed. This annotation 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 annotation might indicate that there is a problem with the associated device.
!??	Reply received with inappropriate type. This annotation might indicate that there is a problem with the associated device.

See Also `ping, netstat`

U

udpstat

Description Displays the packets on a UDP port.

Permission level `diagnostic`

Usage `udpstat [VRoutername] [-p portnum] [-t time] [-b bytes]`

Command element	Description
VRoutername	Name of the virtual router (VRouter). If you do not specify a VRouter name, the system assumes the global VRouter.
-p *portnum*	Display the packets received on the port specified by *portnum*.
-t *time*	Display the packets received on the port at the specified time.
-b *bytes*	Display the packets consisting of the specified number of bytes.
-k	Stop the display.

uds3lines

Description Displays information regarding unchannelized DS3 lines.

Permission level system

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

Command element	Description
-a	Show information about all unchannelized DS3 lines.
-d	Show disabled lines.
-f	Show all free lines.
-u	Show lines that are in use.

Example To display information about all unchannelized DS3 lines:

```
admin> uds3lines -a
All UDS3 lines:
                              (dvOp   dvUpSt  dvRq    sAdm    nailg)
Line   {    1  13  1 }       (Up     Idle    UP      UP      00012)
```

The output displays the following information:

Field	Description
dvOp	The current operational state of the line (also specified by device-state): ■ 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: ■ 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: ■ 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): ■ 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.
nailg	The dedicated group to which the line has been assigned.

See Also atmlines

uptime

Description On an APX unit, reports how long the primary controller and individual cards have been operational. 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. The `uptime` command does *not* report the version number of code used by the controllers, but reports the primary or secondary status of each controller. The code version for the controllers is obtained with 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 running and how long individual cards have been operational.

Permission level `diagnostic`

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

Command element	Description
No options	Display the system uptime.
`-a`	For the primary controller on an APX 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.
slot	Display the uptime for the specified slot card.
shelf slot	Display the uptime for the slot card specified by shelf and slot. The shelf number is always 1.

Example *Displaying the uptime for all slot cards on an APX unit*

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     9.1
{ shelf-1 slot-2 }           t3-card    2 days 00:40:31     9.1
{ shelf-1 slot-3 }       ether3-card    2 days 00:40:41     9.1
{ shelf-1 slot-4 }       ether3-card    2 days 00:40:41     9.1
{ shelf-1 slot-5 }         madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-6 }         madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-7 }         madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-8 }         madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-9 }         madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-10 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-11 }          t3-card    2 days 00:40:31     9.1
{ shelf-1 slot-12 }          t3-card    2 days 00:40:31     9.1
{ shelf-1 slot-13 }        csmv-card    2 days 00:39:07     9.1
```

```
{ shelf-1 slot-14 }        csmv-card    2 days 00:39:07     9.1
{ shelf-1 slot-15 }        csmv-card    2 days 00:39:07     9.1
{ shelf-1 slot-16 }        csmv-card    2 days 00:39:07     9.1
{ shelf-1 slot-17 }      ether3-card    2 days 00:40:41     9.1
{ shelf-1 slot-18 }      ether3-card    2 days 00:40:41     9.1
{ shelf-1 slot-19 }        csmv-card    2 days 00:39:07     9.1
{ shelf-1 slot-24 }      ether3-card    2 days 00:40:41     9.1
{ shelf-1 slot-25 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-26 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-27 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-28 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-29 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-30 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-31 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-32 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-33 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-34 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-35 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-36 }        madd-card    2 days 00:39:47     9.1
{ shelf-1 slot-37 }      ether3-card    2 days 00:40:41     9.1
{ shelf-1 slot-38 }      ether3-card    2 days 00:40:41     9.1
{ shelf-1 slot-39 }        csmv-card    2 days 00:39:07     9.1
{ 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 )
```

Example *Displaying the uptime for all slot cards on a MAX TNT unit*

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 9.1
{ shelf-1 slot-2 } 4ether2-card 9 days 01:05:28 9.1
{ shelf-1 slot-3 } hdlc2-card 9 days 01:04:02 9.1
{ shelf-1 slot-4 } csmx-card 9 days 01:03:40 9.1
{ shelf-1 slot-6 } csmx-card 9 days 01:04:30 9.1
{ shelf-1 controller } shelf-controller 9 days 01:06:10 9.1
```

userstat

Description Displays user session status.

Permission level system

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

Command element	Description
-s	Show session information in an 80-character-wide format (the default).
-l	Show 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 *sessionid*	Terminate a user session that uses Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Multilink Protocol Plus™ (MP+), Telnet, Telnet binary, Raw Transmission Control Protocol (TCP), or the terminal server. The -k option does not terminate frame relay or DTPT service types.
-a *ipaddr*	Show session information for a specified IP address.
-u *username*	Show session information for a specified username.
-o [*format*]	Restrict the output to specified fields. Following are the available formats: ■ %i—session ID ■ %l—line or channel ■ %s—location (*slot*:*item*) ■ %r—transmit rate and 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 *Displaying session information*

To display session information:

```
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 (*shelf.slot.line/channel*) of the network port on which the connection was established, such as a T1 line/channel. The shelf number is always 1.
Slot:Item	*Shelf:slot:item/logical-item* 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. 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.
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.

Field	Description
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)
```

Example *Restricting the output to certain fields*

If you use the -o option and indicate the codes for SessionID and Line/Chan 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)
```

Example *Displaying information for a known IP address*

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)
```

Example *Displaying information for a known username*

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)
```

Example *Displaying the caller's telephone number*

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)
```

Example *Terminating a user session*

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
```

V

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 10.0.1
```

view

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

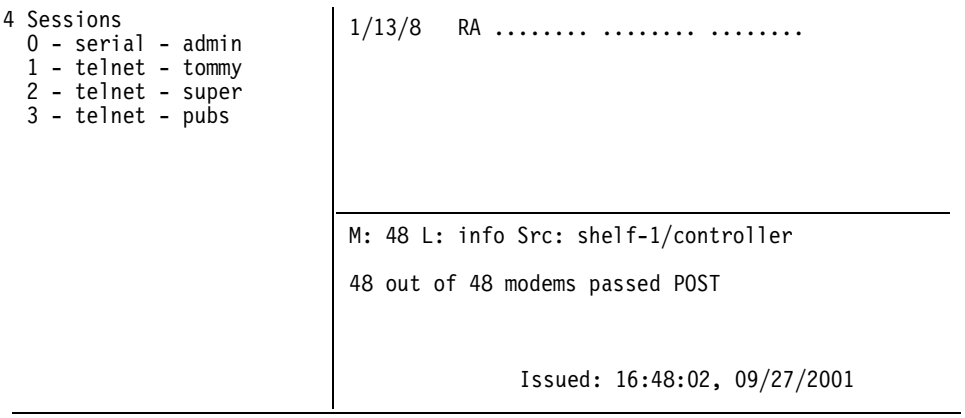
Permission level `system`

Usage `view` *`position status-type`*

Command element	Description
`position`	The window position can be `top`, `bottom`, or `left`, indicating which area of the status window will be affected by the command.
`status-type`	If the specified window position is `top` or `bottom`, the window can display one of the following types of status information: ■ `general` (general status information) ■ `log` (the 32-message log buffer) ■ `line` (T1 line and channel status) If the specified window position is `left`, the window can display one of the following types of status information: ■ `connection` (WAN connection status) ■ `session` (management status)

Example To display session management information:

```
admin> view left session
```



See Also connection, line, log, status

vrouter

Description Displays entries in the virtual router (VRouter) table.

Permission level system

Usage vrouter [dump [full]]

Command element	Description
dump	Displays the entries in the VRouter table.
full	Displays extended information about the entries in the VRouter table.

Example To display the entries in the VRouter table:

```
admin> vrouter dump
Total number of VRouters = 1
Index = 1, Name = cli, ID = 1
```

W

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 the current `user` profile:

```
admin> whoami
tommy
```

See Also `auth`

write

Description Validates the settings of the working profile and then writes it from the edit buffer to nonvolatile RAM (NVRAM).

If the working profile has an index field (a parameter followed by an asterisk), that parameter must have a value or the write operation is not allowed. If you modify a profile and do not use the `write` command before reading another profile, the changes are lost.

Permission level `update`

Usage `write [-f]`

Command element	Description
`-f`	Force the write 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 = ""
sub-address = ""
clid = ""
ip-options = { yes yes 0.0.0.0/0 0.0.0.0/0 1 60 120 no no 0 0.0.0.0 +
ipx-options = { no router-peer both both no 00:00:00:00 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 "" "" no +
ppp-options = { no-ppp-auth none "" "" "" "" stac 1524 no 600 600 no+
```

```
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 }
x75-options = { 7 10 1000 1024 }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
dhcp-options = { no 1 4 }
shared-prof = no
max-shared-users = 0
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 }
sdtn-packets-server = no
AT-string = ""
port-redirect-options = { none 0 0.0.0.0 }
modem-on-hold-timeout = conn-profile-use-global
admin> write
CONNECTION/newyork written
```

See Also list, new, read, set

APX/MAX TNT Profile Reference

2

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

A

access-properties

Description A subprofile that enables you to specify a group name, context prefix, security model, and security level for a view-based access control model (VACM) configuration.

Usage Following is a listing of an `access-properties` subprofile with its default settings:

```
admin> list access-properties
[in VACM-ACCESS/{"" "" v1 none }:access-properties (new)]
group-name = ""
context-prefix = ""
security-model = v1
security-level = none
```

Location `VACM-ACCESS/{"" "" v1 none }`

ADMIN-STATE-PERM-IF

Description A read-only profile that holds information about the TAOS unit's dedicated interfaces. The system creates a profile for an active dedicated interface and assigns it an interface index.

Usage Following is a listing of an `admin-state-perm-if` profile called `homenet`:

```
[in ADMIN-STATE-PERM-IF/homenet]
station* = homenet
snmp-interface = 6
desired-state = admin-state-up
desired-trap-state = trap-state-enabled
inet-profile-type = 1
```

ADMIN-STATE-PHYS-IF

Description A read-only profile that holds information about the system's physical interfaces. The system creates a profile for each of its physical interfaces.

Usage Following is a listing of an `admin-state-phys-if` profile for a device in slot 1:

```
[in ADMIN-STATE-PHYS-IF/{ shelf-1 slot-1 1 }]
device-address* = { shelf-1 slot-1 1 }
slot-type = 8t1-card
snmp-interface = 731
modem-table-index = 0
desired-state = admin-state-down
desired-trap-state = trap-state-enabled
```

aesa-address

Description A subprofile that enables you to configure an ATM end system address (AESA).

Usage Following are listings of `aesa-address` subprofiles with their default settings:

```
[in ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address+
format = undefined
idp-portion = { "" "" }
dsp-portion = { "" "" "" }
[in CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa+]
format = undefined
idp-portion = { "" "" }
dsp-portion = { "" "" "" }
[in CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa+]
format = undefined
idp-portion = { "" "" }
dsp-portion = { "" "" "" }
```

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr`

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 Following is a listing of an `answer-defaults` profile with its default settings:

```
[in ANSWER-DEFAULTS (new)]
use-answer-for-all-defaults = yes
force-56kbps = no
profiles-required = yes
clid-auth-mode = ignore
clid-selection = first
callback-clid-prefix = ""
ppp-answer = { yes no-ppp-auth none "" yes 0 none 1524 no 600 600 no no 1524+
mp-answer = { yes 1 2 no }
mpp-answer = { yes quadratic transmit 1 1 15 5 10 70 }
fr-answer = { yes }
tcp-clear-answer = { yes }
v120-answer = { yes 256 }
ip-answer = { yes yes no 1 no 0 }
ipx-answer = { no router-peer }
session-info = { "" "" no no 120 no-idle 120 0 }
framed-only = no
hdlc-nrm-answer = { no }
visa2-answer = { no }
atm-answer = { no }
priority-answer = { none none 40 0 0 60 }
```

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 Following is a listing of an `atm-address` subprofile with its default settings:

```
[in ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address+
numbering-plan = undefined
e164-native-address = ""
aesa-address = { undefined { "" "" } { "" "" "" } }
```

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options`

atm-answer

Description A subprofile that lets you specify whether the system accepts incoming Asynchronous Transfer Mode (ATM) switched virtual circuit (SVC) calls.

Usage Following is a listing of an `atm-answer` subprofile with its default setting:

```
[in ANSWER-DEFAULTS:atm-answer (new)]
svc-enabled = no
```

Location `ANSWER-DEFAULTS`

ATM-INTERFACE

Description A profile that enables you to configure a logical Asynchronous Transfer Mode (ATM) interface associated with a physical ATM port.

Usage Following is a listing of an `atm-interface` profile with its default settings:

```
[in ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 } (new)]
interface-address* = { { any-shelf any-slot 0 } 0 }
name = ""
svc-options = { no uni-3.1 { undefined "" { undefined { "" "" } { "" "" "" }+
```

atm-options

Description A subprofile containing options for configuring an Asynchronous Transfer Mode (ATM) connection.

Usage Following is a listing of an `atm-options` subprofile with its default settings:

```
[in CONNECTION/"":atm-options (new)]
atm1483type = aal5-llc
vpi = 0
vci = 32
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
```

Location `CONNECTION/""`

ATMP

Description A profile that enables you to configure an Ascend Tunnel Management Protocol (ATMP) tunnel.

Usage Following is a listing of an `atmp` profile with its default settings:

```
[in ATMP (new)]
agent-mode = tunnel-disabled
agent-type = gateway-home-agent
udp-port = 5150
home-agent-password = ""
atmp-sap-reply = no
retry-timeout = 3
retry-limit = 10
idle-timer = 0
mtu-limit = 0
force-fragmentation = no
atmp-snmp-trap = no
```

Dependencies You must restart the TAOS unit in order to begin ATMP operations.

ATMSVC-ROUTE

Description A profile that enables you to configure a static Asynchronous Transfer Mode (ATM) route.

Usage Following is a listing of an `atmsvc-route` profile with its default settings:

```
[in ATMSVC-ROUTE/"" (new)]
name* = ""
active = no
address-prefix = ""
interface-address = { { any-shelf any-slot 0 } 1 }
```

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 Following is a listing of an `auxiliary-syslog [1]` subprofile with its default settings:

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

Location `LOG`

B

BASE

Description A read-only profile that displays the software versions in use, enabled features, network interfaces, and other system information.

Usage Following is a sample listing of a `base` profile:

```
[in BASE]
shelf-number = 1
software-version = 9
software-revision = 0
software-level = b
d-channel-enabled = yes
aim-enabled = no
switched-enabled = yes
multi-rate-enabled = no
frame-relay-enabled = yes
maxlink-client-enabled = disabled
data-call-enabled = yes
r2-signaling-enabled = no
serial-number = 6530207
hardware-level = 0
countries-enabled = 0
modem-dialout-enabled = no
firewalls-enabled = no
network-management-enabled = no
phs-support = no
selectools-enabled = no
tnt-adsl-restricted = no
tnt-sdsl-restricted = no
tnt-idsl-restricted = no
voip-enabled = no
voip-max-capacity-allowed = no
xcom-ss7 = disabled
pptp-enabled = disabled
network-mgmt-voip-enabled = no
fgd-signaling-enabled = no
```

BGP-GLOBAL

Description A profile that enables you to define global parameters for the Border Gateway Protocol (BGP) on this TAOS unit. You can define only one BGP policy per TAOS unit.

Usage Following is a listing of a `bgp-global` profile with its default settings:

```
[in BGP-GLOBAL (new)]
enable = no
autonomous-system = 65534
id = 0.0.0.0
connect-retry-interval = 120
```

```
keepalive-time = 30
hold-time = 90
sub-as = 0
cluster-id = 0.0.0.0
igp-lockstep = no
max-multi-paths = 1
static-route-redist-policy = ""
conn-route-redist-policy = ""
local-pref-default = 100
always-compare-med = no
```

BGP-PEER

Description A profile that enables you to define a Border Gateway Protocol (BGP) peer relationship between this TAOS unit and another BGP peer.

Usage Following is a listing of a `bgp-peer` profile with its default settings:

```
[in BGP-PEER/"" (new)]
peer-name* = ""
enable = no
peer-ip-address = 0.0.0.0
my-ip-address = 0.0.0.0
autonomous-system = 65534
always-next-hop = no
route-reflector-client = no
confederation-member = no
default-gateway-metric = 0
accept-policy = ""
inject-policy = ""
advertise-policy = ""
```

BGP-POLICY

Description A profile that enables you to define acceptance, injection, advertisement, and redistribution policies for a Border Gateway Protocol (BGP) configuration. You can fine-tune the routes accepted, injected, and advertised to and from other peers, and specify which static and connected routes to redistribute into BGP.

Usage Following is a listing of a `bgp-policy` profile with its default settings:

```
[in BGP-POLICY/"" (new)]
name* = ""
next-policy = ""
rule = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ]
```

BGP-SUMMARIZATION

Description A profile that enables you to define Border Gateway Protocol (BGP) route summarizations to advertise to BGP peers.

Usage Following is a listing of a `bgp-summarization` profile with its default settings:

```
[in BGP-SUMMARIZATION/{ 0.0.0.0/0 } (new)]
prefix* = { 0.0.0.0/0 }
enable = no
summarization-policy = all
```

Note The TAOS implementation of BGP does not support BGP route aggregation—the summarization and advertisement of static connected, local, and Interior Gateway Protocol (IGP) routes into BGP.

bootp-relay

Description A subprofile containing options for configuring the BOOTP relay feature.

Usage Following is a listing of a `bootp-relay` subprofile with its default settings:

```
[in IP-GLOBAL:bootp-relay (new)]
active = no
bootp-servers = [ 0.0.0.0 0.0.0.0 ]
```

Location `IP-GLOBAL`

bridging-options

Description *Not supported.*

C

CALL-LOGGING

Description A profile that enables you to configure the TAOS unit to communicate with one or more call-log hosts.

Usage Following is a listing of a `call-logging` profile with its default settings:

```
[in CALL-LOGGING (new)]
call-log-enable = no
call-log-host-1 = 0.0.0.0
call-log-host-2 = 0.0.0.0
call-log-host-3 = 0.0.0.0
call-log-port = 1646
call-log-key = ""
call-log-timeout = 1
call-log-id-base = acct-base-10
call-log-reset-time = 0
call-log-stop-only = yes
call-log-limit-retry = 0
```

```
call-log-server-index = host-1
call-log-radius-compat = 16-bit-vendor-specific
call-log-multi-packet = no
call-log-stream-period = 15
call-log-connection-packets-enable = no
call-log-csm-modem-diag = no
voip-call-logging = yes
```

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

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 Following is a listing of a `call-route` profile with its default settings:

```
[in CALL-ROUTE/{ { { any-shelf any-slot 0 } 0 } 0 } (new)]
index* = { { { any-shelf any-slot 0 } 0 } 0 }
trunk-group = 0
phone-number = ""
preferred-source = { { any-shelf any-slot 0 } 0 }
call-route-type = any-call-type
cost = 0
```

call-route-info

Note The `call-route-info` subprofile has been replaced by the `call-route` profile.

Description A subprofile that specifies a device to which the TAOS unit must route calls received on a particular channel.

Usage Following are listings of `call-route-info` subprofiles with their default settings:

```
[in DS3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
```

```
[in E1/{ any-shelf any-slot 0 }:line-interface:channel-config[1]:call+
shelf = any-shelf
slot = any-slot
item-number = 0
```

```
[in E3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
```

```
[in OC3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
```

```
[in SWAN/{ any-shelf any-slot 0 }:line-config:call-route-info (new)]
shelf = any-shelf
slot = any-slot
item-number = 0

[in T1/{ any-shelf any-slot 0 }:line-interface:channel-config[1]:call+
shelf = any-shelf
slot = any-slot
item-number = 0
```

Dependencies Although use of the `call-route-info` subprofile is not recommended, any nondefault setting you specify for it takes precedence over a `preferred-source` specification in a `call-route` profile.

Location `DS3-ATM/{ any-shelf any-slot 0 }:line-config`
`E1/{ any-shelf any-slot 0 }:line-interface:channel-config`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config`
`SWAN/{ any-shelf any-slot 0 }:line-config`
`T1/{ any-shelf any-slot 0 }:line-interface:channel-config`

CALL-SWITCHING

Description A profile that contains settings for switching a call through another network interface.

Usage Following is a listing of a `call-switching` profile with its default settings:

```
[in CALL-SWITCHING]
enabled = no
comparison-rule = { no }
```

channel-config

Description A subprofile containing configuration options for the channels of an E1 or T1 line. The index for each subprofile is a channel number.

Usage Following is a listing of all the `channel-config` subprofiles for an E1 line, with their default settings:

```
[in E1/{ any-shelf any-slot 0 }:line-interface:channel-config (new)]
channel-config[1] = { switched-channel 9 "" 1 255 }
channel-config[2] = { switched-channel 9 "" 1 255 }
channel-config[3] = { switched-channel 9 "" 1 255 }
channel-config[4] = { switched-channel 9 "" 1 255 }
channel-config[5] = { switched-channel 9 "" 1 255 }
channel-config[6] = { switched-channel 9 "" 1 255 }
channel-config[7] = { switched-channel 9 "" 1 255 }
channel-config[8] = { switched-channel 9 "" 1 255 }
channel-config[9] = { switched-channel 9 "" 1 255 }
channel-config[10] = { switched-channel 9 "" 1 255 }
channel-config[11] = { switched-channel 9 "" 1 255 }
channel-config[12] = { switched-channel 9 "" 1 255 }
channel-config[13] = { switched-channel 9 "" 1 255 }
```

```
channel-config[14] = { switched-channel 9 "" 1 255 }
channel-config[15] = { switched-channel 9 "" 1 255 }
channel-config[16] = { switched-channel 9 "" 1 255 }
channel-config[17] = { switched-channel 9 "" 1 255 }
channel-config[18] = { switched-channel 9 "" 1 255 }
channel-config[19] = { switched-channel 9 "" 1 255 }
channel-config[20] = { switched-channel 9 "" 1 255 }
channel-config[21] = { switched-channel 9 "" 1 255 }
channel-config[22] = { switched-channel 9 "" 1 255 }
channel-config[23] = { switched-channel 9 "" 1 255 }
channel-config[24] = { switched-channel 9 "" 1 255 }
channel-config[25] = { switched-channel 9 "" 1 255 }
channel-config[26] = { switched-channel 9 "" 1 255 }
channel-config[27] = { switched-channel 9 "" 1 255 }
channel-config[28] = { switched-channel 9 "" 1 255 }
channel-config[29] = { switched-channel 9 "" 1 255 }
channel-config[30] = { switched-channel 9 "" 1 255 }
channel-config[31] = { switched-channel 9 "" 1 255 }
channel-config[32] = { switched-channel 9 "" 1 255 }
```

Following is a listing of an individual `channel-config` subprofile for an `E1` line, with its default settings:

```
[in E1/{ any-shelf any-slot 0 }:line-interface:channel-config[1] (new)]
channel-usage = switched-channel
trunk-group = 9
phone-number = ""
nailed-group = 1
idle-pattern = 255
```

Following is a listing of all the `channel-config` subprofiles for a `T1` line, with their default settings:

```
[in T1/{ any-shelf any-slot 0 }:line-interface:channel-config (new)]
channel-config[1] = { switched-channel 9 "" 1 255 }
channel-config[2] = { switched-channel 9 "" 1 255 }
channel-config[3] = { switched-channel 9 "" 1 255 }
channel-config[4] = { switched-channel 9 "" 1 255 }
channel-config[5] = { switched-channel 9 "" 1 255 }
channel-config[6] = { switched-channel 9 "" 1 255 }
channel-config[7] = { switched-channel 9 "" 1 255 }
channel-config[8] = { switched-channel 9 "" 1 255 }
channel-config[9] = { switched-channel 9 "" 1 255 }
channel-config[10] = { switched-channel 9 "" 1 255 }
channel-config[11] = { switched-channel 9 "" 1 255 }
channel-config[12] = { switched-channel 9 "" 1 255 }
channel-config[13] = { switched-channel 9 "" 1 255 }
channel-config[14] = { switched-channel 9 "" 1 255 }
channel-config[15] = { switched-channel 9 "" 1 255 }
channel-config[16] = { switched-channel 9 "" 1 255 }
channel-config[17] = { switched-channel 9 "" 1 255 }
channel-config[18] = { switched-channel 9 "" 1 255 }
channel-config[19] = { switched-channel 9 "" 1 255 }
channel-config[20] = { switched-channel 9 "" 1 255 }
```

```
channel-config[21] = { switched-channel 9 "" 1 255 }
channel-config[22] = { switched-channel 9 "" 1 255 }
channel-config[23] = { switched-channel 9 "" 1 255 }
channel-config[24] = { switched-channel 9 "" 1 255 }
```

Following is a listing of an individual `channel-config` subprofile for a `T1` line, with its default settings:

```
[in T1/{ any-shelf any-slot 0 }:line-interface:channel-config[1] (new)]
channel-usage = switched-channel
trunk-group = 9
phone-number = ""
nailed-group = 1
idle-pattern = 255
```

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

clocking

Description A subprofile containing settings for an internal clock on a Serial WAN (SWAN) line.

Usage Following is a listing of a `clocking` subprofile with its default settings:

```
[in SWAN/{ any-shelf any-slot 0 }:line-config:clocking (new)]
clock-mode = external-clock
divider = 1
exp = 2
line-rate = 2048000
```

Location `SWAN/{ any-shelf any-slot 0 }:line-config`

comparison-rule

Description A subprofile that enables you to specify the type of comparison the system uses to detect a call that requires call switching.

Usage Following is a listing of a `comparison-rule` subprofile with its default setting:

```
[in CALL-SWITCHING:comparison-rule]
call-route-empty-phone-number-acceptable = no
```

Location `CALL-SWITCHING`

congestion-control

Description A subprofile that enables you to configure congestion-control for an SS7 configuration.

Usage Following is a listing of a `congestion-control` subprofile with its default settings:

```
[in SS7-GATEWAY:congestion-control (new)]
congestion-control-type = l3-queue-depth
cl1-level = 60
cl1-action = send-info-to-mgc
cl2-level = 120
cl2-action = reject-new-call
```

Location `SS7-GATEWAY`

CONNECTION

Description A profile containing connection-specific information, including authentication settings, compression values, and filter specifications.

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 Following is a `connection` profile with its default settings:

```
[in CONNECTION/"" (new)]
station* = ""
active = no
encapsulation-protocol = mpp
called-number-type = national
dial-number = ""
subaddress = ""
clid = ""
ip-options = { yes yes 0.0.0.0/0 0.0.0.0/0 1 60 120 no no 0 0.0.0.0 +
ipx-options = { no router-peer both both no 00:00:00:00 00:00:00:00 "" no [+
bridging-options = { 0 no }
session-options = { "" "" no no 120 no-idle 120 "" 0 disabled autobaud +
telco-options = { ans-and-orig no off 1 no no 56k-clear 0 "" "" no no 0 any }
ppp-options = { no-ppp-auth none "" "" "" "" stac 1524 no 600 600 no +
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 }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
dhcp-options = { no 1 4 }
shared-prof = no
max-shared-users = 0
framed-only = no
tunnel-options = { disabled atmp-protocol 0 rip-off "" "" 5150 "" "" "" "" +
vrouter = ""
```

```
atm-options = { aal5-llc 0 32 no "" none 1 { no { undefined "" { undefined {+
hdlc-nrm-options = { 2000 2 60000 5000 2 yes yes 255 }
visa2-options = { 10000 04 06 15 05 03 00:03:00:00 }
sdtn-packets-server = no
AT-string = ""
port-redirect-options = { none 0 0.0.0.0 }
modem-on-hold-timeout = conn-profile-use-global
priority-options = { none none 73 0 0 60 }
tos-copying = no
```

D

date

Description A subprofile that displays the day of the week and the current system date.

Usage Following is a listing of a `date` subprofile:

```
[in TIMEDATE:date]
weekday = Monday
month = May
year = 2002
day = 6
```

Location `TIMEDATE`

default-call-mapping

Description A subprofile that simplifies the configuration of Layer 2 Tunneling Protocol (L2TP) dial-out. The system uses the `default-call-mapping` subprofile to get the call type used in the Integrated Services Digital Network (ISDN) call from the bearer/framing type combination in the outgoing Call Request packet from the L2TP network server (LNS).

Usage Following is a listing of all the `default-call-mapping` subprofiles for a particular tunnel configuration:

```
[in TUNNEL-SERVER/"":dialout-options:default-call-mapping (new)]
default-call-mapping[1] = { no any any 56k-clear }
default-call-mapping[2] = { no any any 56k-clear }
default-call-mapping[3] = { no any any 56k-clear }
default-call-mapping[4] = { no any any 56k-clear }
```

Following is a listing of an individual `default-call-mapping` subprofile with its default settings:

```
[in TUNNEL-SERVER/"":dialout-options:default-call-mapping[1] (new)]
valid-entry = no
bearer-type = any
framing-type = any
data-service = 56k-clear
```

Location `TUNNEL-SERVER/"":dialout-options`

device-address

Description A subprofile that specifies the address of any of the following devices:

- High-Level Data Link Control (HDLC) processor
- Channel on an E1, T1, or T3 slot card
- Modem on a digital modem card
- V.35 interface on a Serial WAN (SWAN) slot card
- Ethernet interface on an Ethernet slot card

Usage Following are listings of `device-address` subprofiles:

```
[in ADMIN-STATE-PERM-IF/{ shelf-1 slot-2 9 }:device-address]
shelf = shelf-1
slot = slot-2
item-number = 9
```

```
[in DEVICE-STATE/{ { shelf-1 slot-14 9 } 2 }:device-address]
physical-address = { shelf-1 slot-14 9 }
logical-item = 2
```

Location `ADMIN-STATE-PERM-IF/{ any-shelf any-slot 0 }`
`DEVICE-STATE/{ { any-shelf any-slot 0} 0}`

DEVICE-STATE

Description A read-only profile that stores the current state of a device. The TAOS unit creates a `device-state` profile when a slot card enters the `Up` state. The unit does not store the `device-state` profile in nonvolatile RAM (NVRAM), so the profile's settings do not persist when the system is restarted or the unit is turned off. The `device-state` setting might differ from the `reqd-state` setting during state changes, such as when a device is being deactivated. State changes are complete when the `device-state` and the `reqd-state` match.

Usage Following is a listing of a `device-state` profile:

```
[in DEVICE-STATE/{ { shelf-1 slot-1 1 } 1 }]
device-address* = { { shelf-1 slot-1 1 } 1 }
device-state = down-dev-state
up-status = idle-up-status
reqd-state = down-reqd-state
```

Dependencies A Simple Network Management Protocol (SNMP) manager can read the `device-state` profile.

DEVICE-SUMMARY

Description A read-only profile that supplies information about different classes of host devices available in the system.

Usage Following is a listing of a `device-summary` profile:

```
[in DEVICE-SUMMARY/modem]
device-class* = modem
total-count = 192
operational-count = 192
disabled-count = 0
```

Dependencies The `device-summary` profile is available in RAM only. it is not stored in nonvolatile RAM (NVRAM) or by the `save` command.

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 Following is a listing of a `dhcp-options` subprofile with its default settings:

```
[in CONNECTION/"":dhcp-options (new)]
reply-enabled = no
pool-number = 1
maximum-leases = 4
```

Location `CONNECTION/""`

dhcp-server

Description A subprofile that enables you to configure the TAOS unit as a Dynamic Host Configuration Protocol (DHCP) server.

Usage Following is a listing of a `dhcp-server` subprofile with its default settings:

```
[in IP-GLOBAL:dhcp-server (new)]
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 00:00:00:00:00+
```

Location `IP-GLOBAL`

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 Following is a listing of a `dialout-configuration` subprofile with its default settings:

```
[in TERMINAL-SERVER:dialout-configuration (new)]
enable = no
direct-access = no
port-for-direct-access = 5000
password-for-direct-access = ""
security-for-direct-access = none
```

Location `TERMINAL-SERVER`

dialout-options

Description A subprofile that enables you to configure Layer 2 Tunneling Protocol (L2TP) dial-out using only Remote Authentication Dial-In User Service (RADIUS) profiles.

Usage Following is a listing of a `dialout-options` subprofile with its default settings:

```
[in TUNNEL-SERVER/"":dialout-options (new)]
enabled = no
dial-number-lookup = no
lookup-prefix = ""
dial-number-prefix = ""
default-call-mapping = [ { no any any 56k-clear } { no any any +
```

Location `TUNNEL-SERVER`

DNIS

Description A profile that enables you to configure Dialed Number Information Service (DNIS) parameters.

Usage Following is a listing of a `dnis` profile with its default settings:

```
[in DNIS/"" (new)]
dialed-number* = ""
call-type = digital
```

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.

Usage Following is a listing of a `dns-local-table` subprofile with its default settings:

```
[in IP-GLOBAL:dns-local-table (new)]
enabled = no
auto-update = no
table-config = [ { "" 0.0.0.0 } { "" 0.0.0.0 } { "" 0.0.0.0 } { "" 0.0.0.0 }+
```

Dependencies Consider the following

- 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.
- 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 the value of `dns-list-size`).

Location `IP-GLOBAL`

DS1-CLOCK-ERROR

Description A profile that enables you to configure thresholds for switching to a new clock source. When line errors for the highest-priority clock exceed specified limits, the clock is switched to the source with the next highest priority.

Usage Following is a listing of a `ds1-clock-error` profile for an E1 system with its default settings:

```
[in DS1-CLOCK-ERROR (new)]
enabled = no
crc-threshold = 0
frame-slips-threshold = 0
fer-threshold = 0
febe-threshold = 0
lcv-threshold = 0
```

Following is a listing of a `ds1-clock-error` profile for a T1 system with its default settings:

```
[in DS1-CLOCK-ERROR (new)]
enabled = no
crc-threshold = 0
frame-slips-threshold = 0
fer-threshold = 0
oof-threshold = 0
lcv-threshold = 0
```

DS3-ATM

Description A profile containing configuration settings for a DS3-ATM slot card.

Usage Following is a listing of a `ds3-atm` profile with its default settings:

```
[in DS3-ATM/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
line-config = { 9 1 static no-loopback no no C-BIT-PLCP 0-15/32-4095 [ { no +
```

DS3-ATM-STAT

Description A read-only profile that indicates the status of a DS3-ATM line.

Usage Following is a sample listing of a `ds3-atm-stat` profile:

```
[in DS3-ATM-STAT/{ shelf-1 slot-1 1 }]
physical-address* = { shelf-1 slot-1 1 }
line-state = active
vpi-vci-range = vpi-0-255-vci-32-8191
f-bit-error-count = 232
p-bit-error-count = 14
cp-bit-error-count = 10
feb-error-count = 22
bpv-error-count = 4065
loss-of-signal = False
loss-of-frame = False
yellow-receive = False
ais-receive = False
```

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 Following are listings of `dsp-portion` subprofiles with their default settings:

```
[in ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }: svc-options: atm-address:+
ho-dsp = ""
esi = ""
sel = ""
```

```
[in CONNECTION/"": atm-options: svc-options: incoming-caller-addr: aesa+
ho-dsp = ""
esi = ""
sel = ""
```

```
[in CONNECTION/"": atm-options: svc-options: outgoing-called-addr: aesa+
ho-dsp = ""
esi = ""
sel = ""
```

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address:aesa-address`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa-address`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa-address`

E

E1

Description A profile that contains configuration settings for an E1 line and its channels.

Usage Following is a listing of an `e1` profile with its default settings:

```
[in E1/{ any-shelf any-slot 0 }]
name = ""
physical-address* = { any-shelf any-slot 0 }
line-interface = { yes none g703 eligible middle-priority isdn te digital+
back-to-back = false
```

E3-ATM

Description A profile containing configuration settings for an E3-ATM slot card.

Usage Following is a listing of an `e3-atm` profile and its default settings:

```
[in E3-ATM/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
line-config = { 9 1 no-loopback no no g832-adm 0-15/32-4095 [ { no 1000 1000+
```

E3-ATM-STAT

Description A read-only profile that indicates the status of an E3-ATM line.

Usage Following is a sample listing of an `e3-atm-stat` profile:

```
[E3-ATM-STAT/{ shelf-1 slot-7 1 }
physical-address ( shelf-1 slot-7 1 }
link-state = active
f-bit-error-count = 0
p-bit-error-count = 0
cp-bit-error-count = 0
feb-error-count = 0
bpv-error-count = 0
loss-of-signal = False
loss-of-frame = False
yellow-receive = False
ais-receive = False
```

ETHER-INFO

Description A read-only profile that specifies the media access control (MAC) address and link state of an Ethernet interface. The `ether-info` profile is created when the Ethernet interface on the shelf controller or installed Ethernet slot card enters an active state, and deleted when the slot is deactivated. The contents of the profile are not written to nonvolatile RAM (NVRAM).

Usage Following is a listing of an `ether-info` profile with its default settings:

```
[in ETHER-INFO/{ shelf-1 controller 1 }]
interface-address* = { shelf-1 controller 1 }
mac-address = 00:c0:7b:63:b0:57
link-state = unknown
```

ETHERNET

Description A profile that defines the physical components of a system Ethernet interface.

Usage Following is a listing of an `ethernet` profile with its default settings:

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

EXTERNAL-AUTH

Description A profile containing configuration options for controlling and tracking user access by means of Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control (TACACS), and Terminal Access Controller Access Control Plus (TACACS+).

Usage Following is a listing of an `external-auth` profile with its default settings:

```
[in EXTERNAL-AUTH (new)]
auth-type = None
acct-type = none
rad-serv-enable = no
rad-auth-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" no 1 no no no 0 yes yes +
rad-acct-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" 1 0 acct-base-10 0 0 +
rad-auth-server = { 0 no rad-serv-attr-any [ 0.0.0.0 0.0.0.0 0.0.0.0 +
tac-auth-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" 0 }
tacplus-auth-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" 0 0 }
tacplus-acct-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" }
password-profile = { Ascend-CLID Ascend-DNIS ascend ascend ascend ascend+
local-profiles-first = lpf-yes
noattr6-use-termsrv = yes
cli-user-auth = local-then-external
```

F

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 Following is a listing of a `filter` profile with its default settings:

```
[in FILTER/"" (new)]
filter-name* = ""
input-filters = [ { no no generic-filter { 0 0 no no 00:00:00:00: +
output-filters = [ { no no generic-filter { 0 0 no no 00:00:00:00:+
```

FIREWALL

Description *Not supported*.

FRAME-RELAY

Description A profile that specifies the data link to a frame relay switch or customer premises equipment (CPE).

Usage Following is a listing of a `frame-relay` profile with its default settings:

```
[in FRAME-RELAY/"" (new)]
fr-name* = ""
active = no
nailed-up-group = 1
nailed-mode = ft1
called-number-type = 2
switched-call-type = 56k-clear
phone-number = ""
billing-number = ""
transit-number = ""
call-by-call-id = 0
link-mgmt = none
link-type = dte
n391-val = 6
n392-val = 3
n393-val = 4
t391-val = 10
t392-val = 15
mru = 1532
dceN392-val = 3
dceN393-val = 4
link-mgmt-dlci = dlci0
mfr-bundle-name = ""
svc-options = { no "" }
fast-path-enabled = no
```

fr-answer

Description A subprofile that enable the TAOS unit to answer incoming connections that use frame relay encapsulation.

Usage Following is a listing of an `fr-answer` subprofile with its default setting:

```
[in ANSWER-DEFAULTS:fr-answer (new)]
enabled = yes
```

Location `ANSWER-DEFAULTS`

fr-options

Description A subprofile containing settings for frame relay connections.

Usage Following is a listing of an fr-options subprofile with its default settings:

```
[in CONNECTION/"":fr-options (new)]
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 = ""
```

Dependencies For the settings in the fr-options subprofile to have any effect, frame relay calls must be enabled in the answer-defaults profile.

Location CONNECTION/""

G

gen-filter

Description A subprofile containing a generic filter specification.

Usage Following is a listing of a gen-filter subprofile for an input filter, with its default settings:

```
[in FILTER/"":input-filters[1]:gen-filter (new)]
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
```

Following is a listing of a gen-filter subprofile for an output filter, with its default settings:

```
[in FILTER/"":output-filters[1]:gen-filter (new)]
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
```

Location FILTER/"":input-filters
FILTER/"":output-filters

H

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 Following is a listing of an `hdlc-nrm-answer` subprofile with its default setting:

```
[in ANSWER-DEFAULTS:hdlc-nrm-answer (new)]
enabled = no
```

Location `ANSWER-DEFAULTS`

hdlc-nrm-options

Description A subprofile containing settings for High-Level Data Link Control-Normal Response Mode (HDLC-NRM) connections.

Usage Following is a listing of an `hdlc-nrm-options` subprofile with its default settings:

```
[in CONNECTION/"":hdlc-nrm-options (new)]
snrm-response-timeout = 2000
snrm-retry-counter = 2
poll-timeout = 60000
poll-rate = 5000
poll-retry-count = 2
primary = yes
async-drop = yes
station-poll-address = 255
```

Location `CONNECTION/""`

I

idp-portion

Description A subprofile containing settings for the initial domain part (IDP) portion of an ATM end system address (AESA).

Usage Following are listings of `dsp-portion` subprofiles with their default settings:

```
[in ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }: svc-options: atm-address:+
afi = ""
idi = ""

[in CONNECTION/"": atm-options: svc-options: incoming-caller-addr: aesa+
afi = ""
idi = ""

[in CONNECTION/"": atm-options: svc-options: outgoing-called-addr: aesa+
afi = ""
idi = ""
```

Location ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address:aesa-address
CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa-address
CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa-address

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 Following is a listing of an immediate-mode-options subprofile with its default settings:

```
[in TERMINAL-SERVER:immediate-mode-options (new)]
service = none
telnet-host-auth = no
host = ""
port = 0
```

Location TERMINAL-SERVER

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 Following is a listing of an incoming-caller-addr subprofile with its default settings:

```
[in CONNECTION/"":atm-options:svc-options:incoming-caller-addr (new)]
numbering-plan = undefined
e164-native-address = ""
aesa-address = { undefined { "" "" } { "" "" "" } }
```

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/"":atm-options:svc-options

input-filters

Description A subprofile containing input-filter specifications. The index for each subprofile is a filter number from 1 through 30.

Usage Following is a listing of the input-filters subprofiles for a particular interface:

```
[in FILTER/"":input-filters (new)]
input-filters[1] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[2] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[3] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
```

```
input-filters[4] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[5] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[6] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[7] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[8] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[9] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[10] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[11] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
input-filters[12] = { no no generic-filter { 0 0 no no 00:00:00:00:00+
...
```

Following is a listing of an individual `input-filters` subprofile with its default settings:

```
[in FILTER/"":input-filters[1] (new)]
valid-entry = no
forward = no
type = generic-filter
gen-filter = { 0 0 no no 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:+
ip-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 no }
route-filter = { 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0 none }
ipx-filter = { 00:00:00:00 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 0 000 normal+
```

Location `FILTER/""`

input-ipx-sap-filters

Description A subprofile containing Service Advertising Protocol (SAP) input-filter specifications. The index for each subprofile is a filter number from 1 through 8.

Usage Following is a listing of all the `input-ipx-sap-filters` subprofiles for a particular SAP filter:

```
[in IPX-SAP-FILTER/"":input-ipx-sap-filters (new)]
input-ipx-sap-filters[1] = { no exclude 00:00 "" }
input-ipx-sap-filters[2] = { no exclude 00:00 "" }
input-ipx-sap-filters[3] = { no exclude 00:00 "" }
input-ipx-sap-filters[4] = { no exclude 00:00 "" }
input-ipx-sap-filters[5] = { no exclude 00:00 "" }
input-ipx-sap-filters[6] = { no exclude 00:00 "" }
input-ipx-sap-filters[7] = { no exclude 00:00 "" }
input-ipx-sap-filters[8] = { no exclude 00:00 "" }
```

Following is a listing of an individual `input-ipx-sap-filters` subprofile with its default settings:

```
[in IPX-SAP-FILTER/"":input-ipx-sap-filters[1] (new)]
valid-filter = no
type-filter = exclude
server-type = 00:00
server-name = ""
```

Location `IPX-SAP-FILTER/""`

interval-performance-monitoring

Description A subprofile that contains interval performance statistics for Synchronous Transport Module (STM) lines and paths.

Usage Following is a listing of all the `interval-performance-monitoring` subprofiles in the `stm-stat` profile:

```
[in STM-STAT/{ shelf-1 slot-2 2 }:interval-performance-monitoring]
interval-performance-monitoring[1] = { 0 0 0 0 0 0 0 0 0 0 0 0 }
interval-performance-monitoring[2] = { 0 0 0 0 0 0 0 0 0 0 0 0 }
interval-performance-monitoring[3] = { 0 0 0 0 0 0 0 0 0 0 0 0 }
interval-performance-monitoring[4] = { 0 0 0 0 0 0 0 0 0 0 0 0 }
```

Following is a listing of an individual `interval-performance-monitoring` subprofile in the `stm-path` profile:

```
[in STM-STAT/{ shelf-1 slot-2 1 }:interval-performance-monitoring[1]]
sonet-section-errored-seconds = 0
sonet-section-severely-errored-seconds = 0
sonet-section-severely-errored-framing-seconds = 0
sonet-section-coding-violations = 0
sonet-line-errored-seconds = 0
sonet-line-severely-errored-seconds = 0
sonet-line-coding-violations = 0
sonet-line-unavailable-seconds = 0
sonet-far-end-line-errored-seconds = 0
sonet-far-end-line-severely-errored-seconds = 0
sonet-far-end-line-coding-violations = 0
sonet-far-end-line-unavailable-seconds = 0
```

Following is a listing of all the `interval-performance-monitoring` subprofiles in the `stm-path-stat` profile:

```
[in STM-PATH-STAT/{ shelf-1 slot-2 4 }:interval-performance-monitoring]
interval-performance-monitoring[1] = { 0 0 0 0 0 0 0 0 }
interval-performance-monitoring[2] = { 0 0 0 0 0 0 0 0 }
interval-performance-monitoring[3] = { 0 0 0 0 0 0 0 0 }
interval-performance-monitoring[4] = { 0 0 0 0 0 0 0 0 }
```

Following is a listing of an individual `interval-performance-monitoring` subprofile in the `stm-path-stat` profile:

```
[in STM-PATH-STAT/{ shelf-1 slot-2 1 }:interval-performance-monitoring[1]]
sonet-path-errored-seconds = 0
sonet-path-severely-errored-seconds = 0
sonet-path-coding-violations = 0
sonet-path-unavailable-seconds = 0
sonet-far-end-path-errored-seconds = 0
sonet-far-end-path-severely-errored-seconds = 0
sonet-far-end-path-coding-violations = 0
sonet-far-end-path-unavailable-seconds = 0
```

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }`
`STM-STAT/{ any-shelf any-slot 0 }`

ip-answer

Description A subprofile containing default settings for Internet Protocol (IP) calls, regardless of their encapsulation protocol.

Usage Following is a listing of an `ip-answer` subprofile with its default settings:

```
[in ANSWER-DEFAULTS:ip-answer (new)]
enabled = yes
vj-header-prediction = yes
assign-address = no
routing-metric = 1
private-route-profile-required = no
pool-for-async-framed-user = 0
```

Location `ANSWER-DEFAULTS`

ip-filter

Description A subprofile containing an Internet Protocol (IP) filter specification.

Usage Following is a listing of an `ip-filter` subprofile for an input filter, with its default settings:

```
[in FILTER/"":input-filters[1]:ip-filter (new)]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
src-port-cmp = none
source-port = 0
dst-port-cmp = none
dest-port = 0
tcp-estab = no
```

Following is a listing of an `ip-filter` subprofile for an output filter, with its default settings:

```
[in FILTER/"":output-filters[1]:ip-filter (new)]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
src-port-cmp = none
source-port = 0
dst-port-cmp = none
dest-port = 0
tcp-estab = no
```

Location `FILTER/"":input-filters`
`FILTER/"":output-filters`

IP-GLOBAL

Description A profile that contains global settings for Transmission Control Protocol/Internet Protocol (TCP/IP).

Usage Following is a listing of an `ip-global` profile with its default settings:

```
[in IP-GLOBAL (new)]
domain-name = ""
dns-primary-server = 0.0.0.0
dhcp-server = { no 0 0 0 0 "" "" 0.0.0.0 [ { 0.0.0.0 00:00:00:00:00:00 } +
dns-secondary-server = 0.0.0.0
dns-server-query-type = udp
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-chaining = no
pool-ospf-adv-type = type-1
pool-base-address = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0+
assign-count = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0+
pool-name = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ""+
rip-policy = Poison-Rvrs
summarize-rip-routes = no
rip-trigger = yes
bootp-enabled = no
bootp-relay = { no [ 0.0.0.0 0.0.0.0 ] }
drop-source-routed-ip-packets = no
ignore-def-route = yes
rarp-enabled = no
udp-cksum = yes
tcp-timeout = 0
dialout-poison = no
telnet-password = ""
user-profile = ""
shared-prof = no
dns-list-attempt = no
static-pref = 100
rip-pref = 100
rip-queue-depth = 50
ospf-pref = 10
ospf-ase-pref = 150
ospf-global = { yes yes 0 }
rip-tag = c8:00:00:00
rip-ase-type = 1
iproute-cache-enable = yes
iproute-cache-size = 0
ipport-cache-enable = yes
suppress-host-routes = no
sntp-info = { sntp-disabled utc+0000 [ 0.0.0.0 0.0.0.0 0.0.0.0 ] 10 }
dns-list-size = 6
client-primary-dns-server = 0.0.0.0
```

```
client-secondary-dns-server = 0.0.0.0
allow-as-client-dns-info = True
dns-local-table = { no no [ { "" 0.0.0.0 } { "" 0.0.0.0 } { "" 0.0.0.0 } +
multicast-forwarding = no
mbone-profile = ""
mbone-lan-interface = { { any-shelf any-slot 0 } 0 }
multicast-hbeat-addr = 0.0.0.0
multicast-hbeat-port = 0
multicast-hbeat-slot-time = 0
multicast-hbeat-number-slot = 0
multicast-hbeat-alarm-threshold = 0
multicast-hbeat-src-addr = 0.0.0.0
multicast-hbeat-src-addr-mask = 0.0.0.0
sec-domain-name = ""
multicast-member-timeout = 360
finger = no
ignore-icmp-redirects = no
icmp-reply-directed-bcast = yes
send-icmp-dest-unreachable = yes
global-vrouter = main
router-id = 0.0.0.0
default-filter-cache-time = 1440
tcp-syn-flood-protect = no
throttle-no-port-match-udp-traffic-on-slot = no
dns-cache-enable = yes
dns-auto-update-interval = 300
mbone-backup = [ { no "" { { any-shelf any-slot 0 } 0 } 0 } { no "" { { +
mbone-timeout = 0
```

IP-INTERFACE

Description A profile containing configuration options for an Internet Protocol (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 slot 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 slot card or a shelf-controller's Ethernet port. For example, for the first Ethernet port on a slot 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.

Following is a listing of an `ip-interface` profile with its default settings:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } (new)]
interface-address* = { { any-shelf any-slot 0 } 0 }
ip-address = 0.0.0.0/0
proxy-mode = Off
rip-mode = routing-off
route-filter = ""
rip2-use-multicast = yes
ospf = { no 0.0.0.0 normal 10 40 5 simple ascend0 0 1 16777215 type-1+
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
directed-broadcast-allowed = yes
vrouter = ""
management-only-interface = no
```

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 can function. Do not delete the default profile if you want your other configurations to work.
- If `proxy-mode` is enabled in any `ip-interface` profile for a given Ethernet port, it is enabled for all ARP requests coming into the physical port.

ip-options

Description A subprofile containing settings for Internet Protocol (IP) routing.

Usage Following is a listing of an `ip-options` subprofile with its default settings:

```
[in CONNECTION/"":ip-options (new)]
ip-routing-enabled = yes
vj-header-prediction = yes
remote-address = 0.0.0.0/0
local-address = 0.0.0.0/0
routing-metric = 1
preference = 60
```

```
down-preference = 120
private-route = no
multicast-allowed = no
address-pool = 0
ip-direct = 0.0.0.0
rip = routing-off
route-filter = ""
source-ip-check = no
ospf-options = { no 0.0.0.0 normal 30 120 5 simple ascend0 0 10 1000 type-1 +
multicast-rate-limit = 100
multicast-group-leave-delay = 0
client-dns-primary-addr = 0.0.0.0
client-dns-secondary-addr = 0.0.0.0
client-dns-addr-assign = yes
client-default-gateway = 0.0.0.0
tos-options = { no 000 normal incoming precedence-tos 00 }
tos-filter = ""
client-wins-primary-addr = 0.0.0.0
client-wins-secondary-addr = 0.0.0.0
client-wins-addr-assign = yes
private-route-table = ""
private-route-profile-required = no
```

Dependencies For settings in an `ip-options` subprofile to have any effect, IP routing calls must be enabled in the `answer-defaults` profile.

Location `CONNECTION/""`

IP-ROUTE

Description A profile containing the information required by the Internet Protocol (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 Following is a listing of an `ip-route` profile with its default settings:

```
[in IP-ROUTE/"" (new)]
name* = ""
dest-address = 0.0.0.0/0
gateway-address = 0.0.0.0
metric = 8
cost = 1
preference = 60
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
private-route = no
active-route = yes
ase7-adv = N/A
vrouter = ""
inter-vrouter = ""
```

ipx-answer

Description A subprofile containing default settings for Internetwork Packet Exchange (IPX) calls.

Usage Following is a listing of an `ipx-answer` subprofile with its default settings:

```
[in ANSWER-DEFAULTS:ipx-answer (new)]
enabled = no
peer-mode = router-peer
```

Location `ANSWER-DEFAULTS`

ipx-filter

Description A subprofile containing an Internetwork Packet Exchange (IPX) filter specification.

Usage Following is a listing of an `ipx-filter` subprofile for an input filter, with its default settings:

```
[in FILTER/"":input-filters[1]:ipx-filter (new)]
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
```

Following is a listing of an `ipx-filter` subprofile for an output filter, with its default settings:

```
[in FILTER/"":output-filters[1]:ipx-filter (new)]
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
```

Location `FILTER/"":input-filters`
`FILTER/"":output-filters`

IPX-GLOBAL

Description A profile that contains global settings for Internetwork Packet Exchange (IPX).

Usage Following is a listing of an `ipx-global` profile with its default settings:

```
[in IPX-GLOBAL (new)]
interface-address = { { any-shelf any-slot 0 } 0 }
ipx-routing-enabled = no
ipx-dialin-pool = 00:00:00:00
global-vrouter = main
```

IPX-INTERFACE

Description A profile that contains configuration options for an Internetwork Packet Exchange (IPX) interface.

Usage Following is a listing of an `ipx-interface` profile with its default settings:

```
[in IPX-INTERFACE/{ { any-shelf any-slot 0 } 0 } (new)]
interface-address* = { { any-shelf any-slot 0 } 0 }
ipx-routing-enabled = no
ipx-frame = None
ipx-net-number = 00:00:00:00
ipx-type-20 = no
ipx-sap-filter-name = ""
vrouter = ""
```

ipx-options

Description A subprofile containing settings for Internetwork Packet Exchange (IPX) routing.

Usage Following is a listing of an `ipx-options` subprofile with its default settings:

```
[in CONNECTION/"":ipx-options (new)]
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 = [ 0 0 0 0 0 0 ]
ipx-header-compression = no
```

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/""`

IPX-ROUTE

Description A profile containing the information required by the Internetwork Packet Exchange (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 Following is a listing of an `ipx-route` profile with its default settings:

```
[in IPX-ROUTE/"" (new)]
name* = ""
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
```

IPX-SAP-FILTER

Description A profile containing Service Advertising Protocol (SAP) filter specifications for including or excluding services from the TAOS unit's SAP table.

Usage Following is a listing of an `ipx-sap-filter` profile with its default settings:

```
[in IPX-SAP-FILTER/"" (new)]
ipx-sap-filter-name* = ""
input-ipx-sap-filters = [ { no exclude 00:00 "" } { no exclude 00:00 "" } { +
output-ipx-sap-filters = [ { no exclude 00:00 "" } { no exclude 00:00 "" } {+
```

L

l2tp-config

Description A subprofile that enables you to configure Layer 2 Tunneling Protocol (L2TP) values when the TAOS unit acts as an L2TP access concentrator (LAC).

Usage Following is a listing of an `l2tp-config` subprofile with its default settings:

```
[in L2-TUNNEL-GLOBAL:l2tp-config (new)]
retry-timer-mode = linear
first-retry-timer = 1000
max-retry-timer = 8000
retry-count = 6
hello-timer = 60
control-connect-establish-timer = 60
lac-incoming-call-timer = 60
base-udp-port = 0
data-pkt-udp-cksum = yes
dialout-auth-lns = no
dialout-send-profile-name = no
```

```
verify-remote-host-name = no
acct-tunnel-connection-encoding = normal
default-tunnel-server = ""
tunnel-server-pre-sccrq-lookup = no
suppress-endpoint-discriminator = no
max-calls-per-tunnel = 0
```

Location L2-TUNNEL-GLOBAL

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 Following is a listing of an `l2-tunnel-global` profile with its default settings:

```
[in L2-TUNNEL-GLOBAL (new)]
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 no no normal no }
l2f-mode = disabled
l2f-system-name = ""
l2f-retry-count = 4
l2f-retry-interval = 0
l2f-tunnel-secret = shared-tunnel-secret
l2f-ignore-mid-sequence = yes
```

LAN-MODEM

Description A profile created by the system for each installed digital modem card.

Usage Following is a listing of a `lan-modem` profile:

```
[in LAN-MODEM/{ shelf-1 slot-2 0 }]
physical-address* = { shelf-1 slot-2 0 }
modem-disable-mode = [ enable enable enable enable enable enable +
```

Dependencies The `lan-modem` profile exists until a different slot card is detected in the slot. Removing or deactivating a slot card does not delete the profile or change its contents.

line-config

Description A subprofile containing line configuration options for a DS3-ATM, E3-ATM, OC3-ATM, or Serial WAN (SWAN) slot card.

Usage Following is a listing of a `line-config` profile for a DS3-ATM slot card, with its default settings:

```
[in DS3-ATM/{ any-shelf any-slot 0 }:line-config (new)]
trunk-group = 9
nailed-group = 1
activation = static
loopback = no-loopback
high-tx-output = no
receive-equalization = no
framer-mode = C-BIT-PLCP
vpi-vci-range = 0-15/32-4095
traffic-shapers = [ { no 1000 1000 2 no 0 } { no 1000 1000 2 no 1 } { no +
cell-payload-scramble = yes
status-change-trap-enable = no
```

Following is a listing of a `line-config` profile for an E3-ATM slot card, with its default settings:

```
[in E3-ATM/{ any-shelf any-slot 0 }:line-config (new)]
trunk-group = 9
nailed-group = 1
loopback = no-loopback
high-tx-output = no
receive-equalization = no
framer-mode = g832-adm
vpi-vci-range = 0-15/32-4095
traffic-shapers = [ { no 1000 1000 2 no 0 } { no 1000 1000 2 no 1 } { no +
cell-payload-scramble = yes
```

Following is a listing of a `line-config` profile for an OC3-ATM slot card, with its default settings:

```
[in OC3-ATM/{ any-shelf any-slot 0 }:line-config (new)]
trunk-group = 0
nailed-group = 1
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 = no
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 no 1 } { no +
```

Following is a listing of a `line-config` profile for a SWAN slot card, with its default settings:

```
[in SWAN/{ any-shelf any-slot 0 }:line-config (new)]
trunk-group = 0
nailed-group = 1
activation = static
clocking = { external-clock 1 2 2048000 }
```

Following is a listing of a line-config profile for an unchannelized DS3 slot card, with its default settings:

```
[in UDS3/{ any-shelf any-slot 0 }:line-config (new)]
trunk-group = 0
nailed-group = 1
activation = static
line-type = c-bit-parity
line-coding = b3zs
loopback = no-loopback
status-change-trap-enable = no
```

Location `DS3-ATM/{ any-shelf any-slot 0 }`
`E3-ATM/{ any-shelf any-slot 0 }`
`OC3-ATM/{ any-shelf any-slot 0 }`
`SWAN/{ any-shelf any-slot 0 }`
`UDS3/{ any-shelf any-slot 0 }`

line-interface

Description A subprofile containing T1 Primary Rate Interface (PRI) or E1 PRI line configuration options.

Usage Following is a listing of a `line-interface` subprofile for an E1 line, with its default settings:

```
[in E1/{ any-shelf any-slot 0 }:line-interface (new)]
enabled = yes
t-online-type = nt
frame-type = 2ds
clock-source = not-eligible
clock-priority = high-priority
signaling-mode = isdn
isdn-emulation-side = te
default-call-type = digital
switch-type = net5-pri
nfas-id = 0
incoming-call-handling = internal-processing
front-end-type = short-haul
overlap-receiving = no
pri-prefix-number = ""
trailing-digits = 2
t302-timer = 10000
channel-config = [ { switched-channel 9 "" 1 } { switched-channel 9 "" 1 }+
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-b-no_match-signal = signal-b-7
group-b-collect-signal = signal-b-7
group-ii-signal = signal-ii-2
input-sample-count = one-sample
answer-delay = 200
caller-id = no-caller-id
timer1-collect-call = 0
timer2-collect-call = 0
hunt-grp-phone-number-1 = ""
hunt-grp-phone-number-2 = ""
hunt-grp-phone-number-3 = ""
collect-incoming-digits = no
t1-inter-digit-timeout = 3000
r1-use-anir = no
r1-first-digit-timer = 340
r1-anir-delay = 350
r1-anir-timer = 200
r1-modified = no
ss7-continuity = { loopback single-tone-2000 }
status-change-trap-enable = no
```

Following is a listing of a `line-interface` subprofile for a T1 line, with its default settings:

```
[in T1/{ any-shelf any-slot 0 }:line-interface (new)]
enabled = no
frame-type = d4
encoding = ami
clock-source = eligible
clock-priority = middle-priority
signaling-mode = inband
isdn-emulation-side = te
robbed-bit-mode = wink-start
default-call-type = digital
switch-type = att-pri
nfas-group-id = 0
nfas-id = 0
incoming-call-handling = internal-processing
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
overlap-receiving = no
pri-prefix-number = ""
trailing-digits = 2
t302-timer = 10000
```

```
channel-config = [ { switched-channel 9 "" 1 255 } { switched-channel 9 "" 1+
maintenance-state = no
input-sample-count = one-sample
senddisc-val = 0
hunt-grp-phone-number-1 = ""
hunt-grp-phone-number-2 = ""
hunt-grp-phone-number-3 = ""
collect-incoming-digits = no
t1-inter-digit-timeout = 3000
r1-use-anir = no
r1-first-digit-timer = 340
r1-anir-delay = 350
r1-anir-timer = 200
r1-modified = no
ss7-continuity = { loopback single-tone-2010 }
down-trans-delay = 25
up-trans-delay = 100
status-change-trap-enable = no
```

Location `E1/{ any-shelf any-slot 0 }`
`T1/{ any-shelf any-slot 0 }`

LOAD-SELECT

Description A read-only profile that specifies which slot-card images to load to PCMCIA flash memory when you use a `load tar` command. Following a system restart, the TAOS unit creates the `load-select` profile if one is not present. The profile lists the entire set of supported slot-card images and an intended load action for each slot-card type when the image is present in a `tar` file. It also contains an `unknown-cards` setting, which represents new slot 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, the system then deletes code images that were present on the PCMCIA flash memory card but were not updated.

Usage Following is a listing of a `load-select` profile with its default settings:

```
[in LOAD-SELECT (new)]
unknown-cards = auto
8t1 = auto
8e1 = auto
t3 = auto
pctfit = auto
pctfie = auto
ut1 = auto
ue1 = auto
uds3 = auto
ds3-atm = auto
enet2 = auto
amdm = auto
hdlc2 = auto
```

```
swan = auto
idsl = auto
capadsl = auto
dmtadsl = auto
sdsl = auto
sdsl70d = auto
sdsl70v = auto
```

Dependencies An explicit `load` command for a particular slot-card type overrides the settings in the `load-select` profile.

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 Following is a listing of a `log` profile with its default settings:

```
[in LOG (new)]
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-call-progress = no
log-software-version = no
syslog-level = info
auxiliary-syslog = [ { no info 0.0.0.0 514 local0 } { no info 0.0.0.0 514 +
```

M

mbone-backup

Description A subprofile that enables you to configure backup multicast backbones (MBONEs).

Usage Following is a listing of all the `mbone-backup` subprofiles with their default settings:

```
[in IP-GLOBAL:mbone-backup]
mbone-backup[1] = { no "" { { any-shelf any-slot 0 } 0 } 0 }
mbone-backup[2] = { no "" { { any-shelf any-slot 0 } 0 } 0 }
mbone-backup[3] = { no "" { { any-shelf any-slot 0 } 0 } 0 }
```

Following is a listing of an individual mbone-backup subprofile with its default settings:

```
[in IP-GLOBAL:mbone-backup[1]]
enabled = no
mbone-profile = ""
mbone-lan-interface = { { any-shelf any-slot 0 } 0 }
mbone-timeout = 0
```

Location IP-GLOBAL

menu-mode-options

Description A subprofile containing terminal-server configuration options for menu mode.

Usage Following is a listing of a menu-mode-options subprofile with its default settings:

```
[in TERMINAL-SERVER:menu-mode-options (new)]
start-with-menus = no
toggle-screen = no
remote-configuration = no
text-1 = ""
host-1 = ""
service-1 = telnet
port-1 = 0
user-1 = ""
text-2 = ""
host-2 = ""
service-2 = telnet
port-2 = 0
user-2 = ""
text-3 = ""
host-3 = ""
service-3 = telnet
port-3 = 0
user-3 = ""
text-4 = ""
host-4 = ""
service-4 = telnet
port-4 = 0
user-4 = ""
menu-selection-string = ""
```

Location TERMINAL-SERVER

modem-configuration

Description A subprofile containing options for configuring the unit's digital modems.

Usage Following is a listing of a `modem-configuration` subprofile with its default settings:

```
[in TERMINAL-SERVER:modem-configuration (new)]
v42/mnp = will-v42
max-baud-rate = 33600-max-baud
modem-transmit-level = -13-db-mdm-trn-level
cell-mode-first = no
cell-level = -18-db-cell-level
7-even = no
modem-mod = v90-modulation
AT-answer-string = ""
modem-on-hold-timeout = moh-disabled
quick-connect-enabled = no
max-v92-receive-baud-rate = 48000-max-v92-baud
v44-enabled = no
```

Location `TERMINAL-SERVER`

mp-answer

Description A subprofile that enable the TAOS unit to answer incoming connections that use Multilink PPP (MP) encapsulation.

Usage Following is a listing of an `mp-answer` subprofile with its default setting:

```
[in ANSWER-DEFAULTS:mp-answer (new)]
enabled = yes
minimum-channels = 1
maximum-channels = 2
bacp-enable = no
```

Location `ANSWER-DEFAULTS`

mp-options

Description A subprofile containing settings for Multilink PPP (MP) connections.

Usage Following is a listing of an `mp-options` subprofile with its default settings:

```
[in CONNECTION/"":mp-options (new)]
enabled = yes
base-channel-count = 1
minimum-channels = 1
maximum-channels = 2
bacp-enable = no
callbackrequest-enable = no
```

Dependencies For the settings in the `mp-options` subprofile to have any effect, MP calls must be enabled in the `answer-defaults` profile.

Location `CONNECTION/""`

mpp-answer

Description A subprofile that enable the TAOS unit to answer incoming connections that use Multilink Protocol Plus™ (MP+) encapsulation.

Usage Following is a listing of an `mpp-answer` subprofile with its default setting:

```
[in ANSWER-DEFAULTS:mpp-answer (new)]
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`

mpp-options

Description A subprofile containing settings for Multilink Protocol Plus™ (MP+) connections.

Usage Following is a listing of an `mpp-options` subprofile with its default settings:

```
[in CONNECTION/"":mpp-options (new)]
enabled = yes
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
x25chan-target-utilization = 70
```

Dependencies For the settings in the `mpp-options` subprofile to have any effect, MP+ calls must be enabled in the `answer-defaults` profile.

Location `CONNECTION/""`

MULTI-LINK-FR

Description A profile that enables you to configure multilink frame relay (MFR).

Usage Following is a listing of a `multi-link-fr` profile with its default settings:

```
[in MULTI-LINK-FR/"" (new)]
mfr-bundle-name* = ""
active = no
mfr-bundle-type = mfr-dte
max-bundle-members = 1
min-bandwidth = 0
```

O

OC3-ATM

Description A profile containing configuration settings for an OC3-ATM slot card.

Usage Following is a listing of an `oc3-atm` profile with its default settings:

```
[in OC3-ATM/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
line-config = { 0 1 no-loopback sdh STS-3c no no no no no 0-15/32-4095+
```

OC3-ATM-STAT

Description A read-only profile that indicates the status of an OC3-ATM line.

Usage Following is a sample listing of an `oc3-atm-stat` profile:

```
[in OC3-ATM-STAT/{ shelf-1 slot-2 1 }]
physical-address* = { shelf-1 slot-2 1 }
line-state = active
vpi-vci-range = vpi-0-255-vci-32-8191
loss-of-signal = False
loss-of-frame = False
ais-receive = True
yellow-receive = False
```

ospf

Description A subprofile that enables you to configure Open Shortest Path First (OSPF) routing on an Ethernet interface.

Usage Following is a listing of an `ospf` subprofile with its default settings:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf (new)]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 10
dead-interval = 40
priority = 5
authen-type = simple
auth-key = ascend0
key-id = 0
cost = 1
down-cost = 16777215
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no
```

```
network-type = Broadcast
poll-interval = 10
md5-auth-key = ascend0
```

Location IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }

ospf-global

Description A subprofile that enables you to define global Open Shortest Path First (OSPF) behavior.

Usage Following is a listing of an `ospf-global` subprofile with its default settings:

```
[in IP-GLOBAL:ospf-global (new)]
enable = yes
as-boundary-router = yes
ospf-max-lsa = 0
```

Location IP-GLOBAL

OSPF-NBMA-NEIGHBOR

Description A profile that enables you to configure an Open Shortest Path First (OSPF) router for operation on a nonbroadcast multiaccess (NBMA) network.

Usage Following is a listing of an `ospf-nbma-neighbor` profile with its default settings:

```
[in OSPF-NBMA-NEIGHBOR/"" (new)]
name* = ""
host-name = ""
ip-address = 0.0.0.0
dr-capable = no
```

ospf-options

Description A subprofile that contains settings for Open Shortest Path First (OSPF) routing.

Usage Following is a listing of an `ospf-options` subprofile with its default settings:

```
[in CONNECTION/"":ip-options:ospf-options (new)]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 30
dead-interval = 120
priority = 5
authen-type = simple
auth-key = ascend0
key-id = 0
cost = 10
down-cost = 1000
ase-type = type-1
```

```
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no
network-type = Point-to-Point
poll-interval = 10
md5-auth-key = ascend0
```

Location CONNECTION/"":ip-options

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 Following is a listing of an outgoing-called-addr subprofile with its default settings:

```
[in CONNECTION/"":atm-options:svc-options:outgoing-called-addr (new)]
numbering-plan = undefined
e164-native-address = ""
aesa-address = { undefined { "" "" } { "" "" "" } }
```

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/"":atm-options:svc-options

output-filters

Description A subprofile containing output-filter specifications. The index for each subprofile is a filter number from 1 through 30.

Usage Following is a listing of the output-filters subprofiles for a particular interface:

```
[in FILTER/"":output-filters (new)]
output-filters[1] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[2] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[3] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[4] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[5] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[6] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[7] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[8] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[9] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00:00+
output-filters[10] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00+
output-filters[11] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00+
output-filters[12] = { no no generic-filter { 0 0 no no 00:00:00:00:00:00+
...
```

Following is a listing of an individual `output-filters` subprofile with its default settings:

```
[in FILTER/"":output-filters[1] (new)]
valid-entry = no
forward = no
type = generic-filter
gen-filter = { 0 0 no no 00:00:00:00:00:00:00:00:00:00:00:00 00:00:00:00+
ip-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 no }
route-filter = { 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0 none }
ipx-filter = { 00:00:00:00 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 0 000 normal +
```

Location `FILTER/""`

output-ipx-sap-filters

Description A subprofile containing Service Advertising Protocol (SAP) output-filter specifications. The index for each subprofile is a filter number from 1 through 8.

Usage Following is a listing of all the `output-ipx-sap-filters` subprofiles for a particular SAP filter:

```
[in IPX-SAP-FILTER/"":output-ipx-sap-filters (new)]
output-ipx-sap-filters[1] = { no exclude 00:00 "" }
output-ipx-sap-filters[2] = { no exclude 00:00 "" }
output-ipx-sap-filters[3] = { no exclude 00:00 "" }
output-ipx-sap-filters[4] = { no exclude 00:00 "" }
output-ipx-sap-filters[5] = { no exclude 00:00 "" }
output-ipx-sap-filters[6] = { no exclude 00:00 "" }
output-ipx-sap-filters[7] = { no exclude 00:00 "" }
output-ipx-sap-filters[8] = { no exclude 00:00 "" }
```

Following is a listing of an individual `output-ipx-sap-filters` subprofile with its default settings:

```
[in IPX-SAP-FILTER/"":output-ipx-sap-filters[1] (new)]
valid-filter = no
type-filter = exclude
server-type = 00:00
server-name = ""
```

Location `IPX-SAP-FILTER/""`

P

password-profile

Description A subprofile containing settings for calling line ID (CLID) and Dialed Number Information Service (DNIS) passwords set in a Remote Authentication Dial-In User Service (RADIUS) profile.

Usage Following is a listing of a `password-profile` subprofile with its default settings:

```
[in EXTERNAL-AUTH:password-profile (new)]
clid = Ascend-CLID
dnis = Ascend-DNIS
banner = ascend
```

Location `EXTERNAL-AUTH`

PCTFI

Description A profile that enables you to configure a Peripheral Control Timing Facilities Interface (PCTFI) slot card.

Usage Following is a listing of a `pctfi` profile with its default settings:

```
[in PCTFI/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
interface-version = pelts
trace-id-0 = 0
trace-id-1 = 1
mode = t1
```

PCTFI-STAT

Description A read-only profile that displays information about the state of a Peripheral Control Timing Facilities Interface (PCTFI) slot card.

Usage Following is a sample listing of a `pctfi-stat` profile:

```
[in PCTFI-STAT/{ shelf-1 slot-5 0 }]
physical-address* = { shelf-1 slot-5 0 }
link-0-status = available
link-1-status = available
side-select = side-1
virtual-ds1-line-status = [ { operational non-cas } { unused non-cas } { +
```

performance-monitoring

Description A subprofile that contains performance monitoring statistics for Synchronous Transport Module (STM) lines and paths.

Usage Following is a sample listing of the `performance-monitoring` subprofile in the `stm-stat` profile:

```
[in STM-STAT/{ shelf-1 slot-2 2 }:performance-monitoring]
sonet-section-errored-seconds = 0
sonet-section-severely-errored-seconds = 0
sonet-section-severely-errored-framing-seconds = 0
sonet-section-coding-violations = 0
sonet-line-errored-seconds = 0
sonet-line-severely-errored-seconds = 0
sonet-line-coding-violations = 0
sonet-line-unavailable-seconds = 0
sonet-far-end-line-errored-seconds = 0
sonet-far-end-line-severely-errored-seconds = 0
sonet-far-end-line-coding-violations = 0
sonet-far-end-line-unavailable-seconds = 0
```

Following is a sample listing of the `performance-monitoring` subprofile in the `stm-path-stat` profile:

```
[in STM-PATH-STAT/{ shelf-1 slot-2 4 }:performance-monitoring]
sonet-path-errored-seconds = 0
sonet-path-severely-errored-seconds = 0
sonet-path-coding-violations = 0
sonet-path-unavailable-seconds = 0
sonet-far-end-path-errored-seconds = 0
sonet-far-end-path-severely-errored-seconds = 0
sonet-far-end-path-coding-violations = 0
sonet-far-end-path-unavailable-seconds = 0
```

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }`
`STM-STAT/{ any-shelf any-slot 0 }`

physical-address

Description A subprofile that identifies a physical address.

Usage Following are listings of `physical-address` subprofiles with their default settings:

```
[in DS3-ATM/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
```

```
[in DS3-ATM-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
```

```
[in E1/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in E3-ATM/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in E3-ATM-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in LAN-MODEM/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in OC3-ATM/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in OC3-ATM-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in PCTFI/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in PCTFI-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in SERIAL/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in STM/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in STM-PATH/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
[in STM-PATH-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
```

```
[in STM-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0

[in SWAN/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0

[in T1/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0

[in T1-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0

[in T3/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0

[in T3-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0

[in UDS3/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0

[in UDS3-STAT/{ any-shelf any-slot 0 }:physical-address (new)]
shelf = any-shelf
slot = any-slot
item-number = 0
```

Location DS3-ATM/{ any-shelf any-slot 0 }
DS3-ATM-STAT/{ any-shelf any-slot 0 }
E1/{ any-shelf any-slot 0 }
E3-ATM/{ any-shelf any-slot 0 }
E3-ATM-STAT/{ any-shelf any-slot 0 }
LAN-MODEM {shelf-*N* slot-*N* *N*}
OC3-ATM/{ any-shelf any-slot 0 }
OC3-ATM-STAT/{ any-shelf any-slot 0 }
PCTFI/{ any-shelf any-slot 0 }
PCTFI-STAT/{ any-shelf any-slot 0 }
SERIAL/{ any-shelf any-slot 0 }
STM/{ any-shelf any-slot 0 }
STM-PATH/{ any-shelf any-slot 0 }
STM-PATH-STAT/{ any-shelf any-slot 0 }
STM-STAT/{ any-shelf any-slot 0 }
SWAN/{ any-shelf any-slot 0 }
T1/{ any-shelf any-slot 0 }

```
T1-STAT/{ any-shelf any-slot 0 }
T3/{ any-shelf any-slot 0 }
T3-STAT/{ any-shelf any-slot 0 }
UDS3/{ any-shelf any-slot 0 }
UDS3-STAT/{ any-shelf any-slot 0 }
```

port-redirect-options

Description A subprofile that enables you to redirect certain packet types to a specified server.

Usage Following is a listing of a `port-redirect-options` subprofile with its default settings:

```
[in CONNECTION/"":port-redirect-options (new)]
protocol = none
port-number = 0
redirect-address = 0.0.0.0
```

Location `CONNECTION/""`

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 PPP (MP) and Multilink Protocol Plus™ (MP+).

Usage Following is a listing of a `ppp-answer` subprofile with its default settings:

```
[in ANSWER-DEFAULTS:ppp-answer (new)]
enabled = yes
receive-auth-mode = no-ppp-auth
bi-directional-auth = none
substitute-send-name = ""
disconnect-on-auth-timeout = yes
bridging-group = 0
link-compression = none
mru = 1524
lqm = no
lqm-minimum-period = 600
lqm-maximum-period = 600
cbcp-enabled = no
ipx-header-compression = no
mtu = 1524
auth-for-async-framed-users = required
max-pap-auth-retry = 0
```

Location `ANSWER-DEFAULTS`

ppp-mode-configuration

Description A subprofile containing terminal-server options for Point-to-Point Protocol (PPP) sessions.

Usage Following is a listing of a `ppp-mode-configuration` subprofile with its default settings:

```
[in TERMINAL-SERVER:ppp-mode-configuration (new)]
ppp = no
delay = 5
direct = no
info = session-ppp
```

Location `TERMINAL-SERVER`

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 PPP (MP) and Multilink Protocol Plus™ (MP+).

Usage Following is a listing of a `ppp-options` subprofile with its default settings:

```
[in CONNECTION/"":ppp-options (new)]
send-auth-mode = no-ppp-auth
bi-directional-auth = none
send-password = ""
substitute-send-name = ""
recv-password = ""
substitute-recv-name = ""
link-compression = stac
mru = 1524
lqm = no
lqm-minimum-period = 600
lqm-maximum-period = 600
cbcp-enabled = no
mode-callback-control = cbcp-no-callback
trunk-group-callback-control = 4
split-code-dot-user-enabled = no
mtu = 1524
```

Dependencies PPP calls must be enabled in the `answer-defaults` profile.

Location `CONNECTION/""`

priority-answer

Description A subprofile containing default settings for reduced latency of Real-Time Transport Protocol (RTP) packets.

Usage Following is a listing of a `priority-answer` subprofile with its default settings:

```
[in ANSWER-DEFAULTS:priority-answer]
enabled = no
packet-classification = qos-tag
max-rtp-packet-delay = 40
minimum-rtp-port = 0
maximum-rtp-port = 0
no-high-prio-pkt-duration=60
```

Location `ANSWER-DEFAULTS`

priority-options

Description A subprofile that enables you to configure the TAOS unit for reduced latency of Real-Time Transport Protocol (RTP) packets.

Usage Following is a listing of a `priority-options` subprofile with its default settings.

```
[in CONNECTION/"":priority-options (new)]
enabled= no
packet-classification = qos-tag
max-rtp-packet-delay = 73
minimum-rtp-port = 0
maximum-rtp-port = 0
no-high-prio-pkt-duration=60
```

Location `CONNECTION`

PRIVATE-ROUTE-TABLE

Description A profile that enables you to define a private routing table.

Usage Following is a listing of a `private-route-table` profile with its default settings:

```
[in PRIVATE-ROUTE-TABLE/"" (new)]
name* = ""
route-description-list = [ { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 } { no 0.0.0.0+
```

pstn-attribute

Description A subprofile that specifies public switched telephone network (PSTN) settings for a Voice over IP (VoIP) call.

Usage Following is a listing of a `pstn-attribute` subprofile with its default settings:

```
[in VOIP/{ "" "" }:pstn-attribute (new)]
cause-code-transparency = no
alert-progress-indicator = no-progress-indicator
proceed-progress-indicator = no-progress-indicator
bearer-capability = speech
```

Location `VOIP/{ "" "" }`

Q

q93b-options

Description A subprofile that enables you to configure Q.93B-layer settings.

Usage Following is a listing of a `q93b-options` subprofile with its default settings:

```
[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
```

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options`

QOS

Description A profile that enables you to configure quality-of-service (QOS) settings.

Usage Following is a listing of a `qos` profile with its default settings:

```
[in QOS (new)]
enabled = no
allow-client-dscp = no
tag-map = [ { no 00 0 } { no 00 0 } { no 00 0 } { no 00 0 } { no 00 0 } { no +
```

qsaal-options

Description A subprofile that enables you to configure Q.SAAL layer settings.

Usage Following is a listing of a `qsaal-options` subprofile with its default settings:

```
[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
```

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options`

R

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 Following is a listing of a `rad-acct-client` subprofile with its default settings:

```
[in EXTERNAL-AUTH:rad-acct-client (new)]
acct-host-1 = ""
acct-host-2 = ""
acct-host-3 = ""
acct-port = 0
acct-src-port = 0
acct-key = ""
acct-timeout = 1
acct-sess-interval = 0
acct-id-base = acct-base-10
acct-reset-time = 0
acct-checkpoint = 0
acct-checkpoint-timer = all-sessions
acct-stop-only = yes
acct-limit-retry = 0
acct-drop-stop-on-auth-fail = no
acct-radius-compat = old-ascend
tunnel-accounting = no
voip-accounting = yes
```

Location `EXTERNAL-AUTH`

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 Following is a listing of a `rad-auth-client` subprofile with its default settings:

```
[in EXTERNAL-AUTH:rad-auth-client (new)]
auth-host-1 = ""
auth-host-2 = ""
auth-host-3 = ""
auth-port = 0
auth-src-port = 0
auth-key = ""
auth-pool = no
auth-timeout = 1
auth-rsp-required = no
auth-id-fail-return-busy = no
auth-id-timeout-return-busy = 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-reset-time = 0
auth-id-max-retry-time = 0
auth-radius-compat = old-ascend
auth-keep-user-name = change-name
auth-realm-delimiters = /\@%
id-auth-prefix = ""
allow-auth-config-rqsts = yes
auth-req-delim-count = 0
auth-req-strip-side = none
auth-network-route-server = yes
id-auth-prefix-x25 = ""
allow-unencrypted-tunnel-password = no
auth-cli-user-dnis = ""
allow-nas-port-type-in-cli-user-auth = yes
```

Location `EXTERNAL-AUTH`

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 Following is a listing of a `rad-auth-server` subprofile with its default settings:

```
[in EXTERNAL-AUTH:rad-auth-server (new)]
auth-port = 0
auth-session-key = no
auth-attribute-type = rad-serv-attr-any
auth-client = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 +
auth-netmask = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 +
auth-key = [ "" "" "" "" "" "" "" "" "" ]
auth-radius-compat = old-ascend
```

Location `EXTERNAL-AUTH`

resilience-options

Description A subprofile that enables you to set the type of behavior that the TAOS unit follows when a T1 or E1 line is lost, and to specify the length of time that connections are maintained.

Usage Following is a listing of a `resilience-options` subprofile with its default settings:

```
[in SS7-GATEWAY:resilience-options (new)]
type = release-all
duration = 0
```

Location `SS7-GATEWAY`

rlogin-options

Description A subprofile containing options for configuring `rlogin` connections.

Usage Following is a listing of an `rlogin-options` subprofile with its default settings:

```
[in TERMINAL-SERVER:terminal-mode-configuration:rlogin-options (new)]
rlogin = no
max-source-port = 1023
min-source-port = 128
```

Location `TERMINAL-SERVER:terminal-mode-configuration`

route-description-list

Description A subprofile containing private routing table specifications. The index for each subprofile is a filter number from 1 through 24.

Usage Following is a listing of all the `route-description-list` subprofiles for a particular private route table:

```
[in PRIVATE-ROUTE-TABLE/"":route-description-list (new)]
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[4] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[5] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[6] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[7] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[8] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[9] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[10] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[11] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[12] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[13] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[14] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[15] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[16] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[17] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[18] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[19] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[20] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[21] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[22] = { no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 }
route-description-list[23] = { 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 }
```

Following is a listing of an individual `route-description-list` subprofile with its default settings:

```
[in PRIVATE-ROUTE-TABLE/"":route-description-list[1] (new)]
enabled = no
dest-address = 0.0.0.0/0
netmask = 0.0.0.0
gateway-address = 0.0.0.0
metric = 0
```

Location `PRIVATE-ROUTE-TABLE/""`

route-filter

Description A subprofile containing a route-filter specification.

Usage Following is a listing of a `route-filter` subprofile for an input filter, with its default settings:

```
[in FILTER/"":input-filters[1]:route-filter (new)]
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
route-mask = 0.0.0.0
route-address = 0.0.0.0
add-metric = 0
action = none
```

Following is a listing of a `route-filter` subprofile for an output filter, with its default settings:

```
[in FILTER/"":output-filters[1]:route-filter (new)]
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
route-mask = 0.0.0.0
route-address = 0.0.0.0
add-metric = 0
action = none
```

Location `FILTER/"":input-filters`
`FILTER/"":output-filters`

rt-fax-options

Description A subprofile that enables you to fine-tune the performance of real-time fax processing.

Usage Following is a listing of an `rt-fax-options` subprofile with its default settings:

```
[in VOIP/{ "" "" }:rt-fax-options (new)]
rt-fax-enable = no
ecm-enable = yes
low-latency-mode = yes
command-spoof = yes
local-retransmit-lsf = yes
packet-redundancy = 0
fixed-packets = no
```

Location `VOIP/{ "" "" }`

S

security-properties

Description A subprofile that enables you to specify a security name and security model for a view-based access control model (VACM) configuration.

Usage Following is a listing of a `security-properties` subprofile with its default settings:

```
[in VACM-SECURITY-GROUP/{ v1 "" }:security-properties (new)]
security-model = v1
security-name = ""
```

Location `VACM-SECURITY-GROUP/{ v1 "" }`

SERIAL

Description A profile that specifies physical interface settings for a system serial interface.

Usage Following is a listing of a `serial` profile with its default settings:

```
[in SERIAL/{ any-shelf any-slot 0 } (new)]
physical-address* = { any-shelf any-slot 0 }
term-rate = 9600-bps
flow-control = none
user-profile = admin
auto-logout = no
```

session-info

Description A subprofile containing default settings for incoming connections. None of these settings are specific to any encapsulation method or network protocol.

Usage Following is a listing of a `session-info` subprofile with its default settings:

```
[in ANSWER-DEFAULTS:session-info (new)]
call-filter = ""
data-filter = ""
filter-persistence = no
filter-required = no
idle-timer = 120
ts-idle-mode = no-idle
ts-idle-timer = 120
max-call-duration = 0
```

Location `ANSWER-DEFAULTS`

session-options

Description A subprofile that specifies session settings not specific to any encapsulation method or network protocol.

Usage Following is a listing of a `session-options` subprofile with its default settings:

```
[in CONNECTION/"":session-options (new)]
call-filter = ""
data-filter = ""
filter-persistence = no
filter-required = no
idle-timer = 120
ts-idle-mode = no-idle
ts-idle-timer = 120
backup = ""
max-call-duration = 0
ses-adsl-cap-up-rate = 1088000
ses-adsl-cap-down-rate = 2560000
ses-sdsl-rate = 784000
ses-adsl-dmt-up-rate = 896000
ses-adsl-dmt-down-rate = 8000000
rx-data-rate-limit = 0
tx-data-rate-limit = 0
cir-timer = 5000
traffic-shaper = 16
```

Location `CONNECTION/""`

signaling-heartbeat

Description A subprofile that enables you to configure signaling heartbeat messages for an Signaling System 7 (SS7) configuration.

Usage Following is a listing of a `signaling-heartbeat` subprofile with its default settings:

```
[in SS7-GATEWAY:signaling-heartbeat (new)]
enabled = no
interval = 3
```

Location `SS7-GATEWAY`

signaling-tos

Description A subprofile that enables you to configure differentiated services code point (DSCP) marking of Voice over IP (VoIP) signaling traffic.

Usage Following is a listing of a `signaling-tos` subprofile with its default settings:

```
[in VOIP/{ "" "" }:signaling-tos (new)]
active = no
precedence = 100
type-of-service = normal
apply-to = both
marking-type = dscp
dscp = 00
```

Location `VOIP/{ "" "" }`

slip-mode-configuration

Description A subprofile with terminal-server configuration options for asynchronous Serial Line Internet Protocol (SLIP) users.

Usage Following is a listing of a `slip-mode-configuration` subprofile with its default settings:

```
[in TERMINAL-SERVER:slip-mode-configuration (new)]
slip = no
slip-bootp = no
info = basic-slip
```

Location `TERMINAL-SERVER`

SLOT-ADMIN

Description A read-only profile that provides information about a specified slot card.

Usage Following is a sample listing of a `slot-admin` profile:

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

SLOT-INFO

Description A profile that displays the software version, serial number, and other system information about the TAOS unit.

Usage Following is a listing of a `slot-info` profile:

```
[in SLOT-INFO/{ shelf-1 slot-1 0 }]
slot-address* = { shelf-1 slot-1 0 }
serial-number = 0
software-version = 9.1
software-revision = 0
software-level = ""
hardware-level = 0
software-release = c7
```

SLOT-STATE

Description A read-only profile that stores the current state of a slot card.

Usage Following is a listing of a `slot-state` profile:

```
[in SLOT-STATE/{ shelf-1 slot-1 0 }]
slot-address* = { shelf-1 slot-1 0 }
current-state = oper-state-up
```

Dependencies Consider the following:

- The `slot-state` profile does not reside in nonvolatile RAM (NVRAM), so it does not persist across system resets or power cycles.
- Simple Network Management Protocol (SNMP) managers can read the `slot-state` profile.

SLOT-TYPE

Description A read-only profile that stores the type of slot card installed in each slot location on a TAOS unit.

Usage Following is a listing of a `slot-type` profile:

```
[in SLOT-TYPE/{ shelf-1 slot-1 0 }]
slot-address* = { shelf-1 slot-1 0 }
slot-type = 8t1-card
```

Dependencies Consider the following:

- The shelf number is always 1.
- The `slot-type` profile resides in nonvolatile RAM (NVRAM) and persists over system resets.

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 Following is a listing of an `snmp` profile with its default settings:

```
[in SNMP (new)]
enabled = no
read-community = public
read-write-enabled = no
read-write-community = write
enforce-address-security = no
contact = ""
location = ""
queue-depth = 0
csm-modem-diag = no
snmp-message-type = v1-and-v3
security-level = none
enable-vacm = no
early-queue-discard = no
notification-log-age-out = 0
```

SNMP-MANAGER

Description A profile that enables you to specify read/write access and the Simple Network Management Protocol (SNMP) version is use.

Usage Following is a listing of an `snmp-manager` profile with its default settings:

```
[in SNMP-MANAGER/"" (new)]
name* = ""
active = no
write-access = no
snmp-message-type = v1-and-v3
```

SNMPV3-NOTIFICATION

Description A profile that enables you to configure Simple Network Management Protocol Version 3 (SNMPv3) notifications support.

Usage Following is a listing of an `snmpv3-notification` profile with its default settings:

```
[in SNMPV3-NOTIFICATION/"" (new)]
name* = ""
active-enabled = no
tag = ""
type = trap
```

SNMPV3-TARGET-PARAM

Description A profile that enables you to set up security and message-processing features for Simple Network Management Protocol Version 3 (SNMPv3) notifications support.

Usage Following is a listing of an `snmpv3-target-param` profile with its default settings:

```
[in SNMPV3-TARGET-PARAM/"" (new)]
name* = ""
active-enabled = no
msg-proc-model = v1
security-model = v1
security-name = ""
security-level = none
```

SNMPV3-USM-USER

Description A profile that enables you to configure security features based on the Simple Network Management Protocol Version 3 (SNMPv3) user-based security model (USM) for the specified user.

Usage Following is a listing of an `snmpv3-usm-user` profile with its default settings:

```
[in SNMPV3-USM-USER/"" (new)]
name* = ""
active-enabled = no
read-write-access = no
auth-protocol = md5-auth
priv-protocol = no-priv
auth-key = ""
priv-key = ""
```

sntp-info

Description A subprofile containing settings required to maintain the system time from a Simple Network Time Protocol (SNTP) server.

Usage Following is a listing of an `sntp-info` profile with its default settings:

```
[in IP-GLOBAL:sntp-info (new)]
enabled = sntp-disabled
gmt-offset = utc+0000
host = [ 0.0.0.0 0.0.0.0 0.0.0.0 ]
update-threshold = 10
update-interval = 600
```

Location `IP-GLOBAL`

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 T1 or E1 line. Both ends of the connection must agree on the continuity check to be used for the line.

Usage Following is a listing of an `ss7-continuity` subprofile for an E1 line, with its default settings:

```
[in E1/{ any-shelf any-slot 0 }:line-interface:ss7-continuity (new)]
incoming-procedure = loopback
outgoing-procedure = single-tone-2000
```

Following is a listing of an `ss7-continuity` subprofile for a T1 line, with its default settings:

```
[in T1/{ any-shelf any-slot 0 }:line-interface:ss7-continuity (new)]
incoming-procedure = loopback
outgoing-procedure = single-tone-2010
```

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

SS7-GATEWAY

Description A profile that contains settings for configuring the Internet call diversion (ICD) for Softswitch signaling gateway.

Usage Following is a listing of an `ss7-gateway` profile with its default settings:

```
[in SS7-GATEWAY (new)]
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 = { ascend 0 1000 3000 30000 7 6 no }
use-system-ip-address-as-source = yes
ipdc-source-address = 0.0.0.0
vrouter = ""
congestion-control = { l3-queue-depth 60 send-info-to-mgc 120 +
signaling-heartbeat = { no 3 }
resilience-options = { release-all 0 }
```

STACKING

Description A profile that contains settings for a unit participating in a group (stack) of TAOS units that manage Multilink PPP (MP) or Multilink Protocol Plus™ (MP+) bundles jointly.

Usage Following is a listing of a `stacking` profile:

```
[in STACKING (new)]
enabled = no
name = ""
udp-port = 5151
multicast-address = 100.90.80.70
multicast-interface-ip-address = 0.0.0.0
data-ip-address = 0.0.0.0
```

static-address

Description A subprofile that enables you to configure up to 100 pairs of Internet Protocol (IP) and media access control (MAC) addresses for a TAOS unit functioning as a Dynamic Host Configuration Protocol (DHCP) server.

Usage Following is a listing of the `static-address` subprofiles:

```
[in IP-GLOBAL:dhcp-server:static-address (new)]
static-address[1] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[2] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[3] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[4] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[5] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[6] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[7] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[8] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[9] = { 0.0.0.0 00:00:00:00:00:00 }
static-address[10] = { 0.0.0.0 00:00:00:00:00:00 }
...
static-address[100] = { 0.0.0.0 00:00:00:00:00:00 }
```

Following is a listing of an individual `static-address` subprofile with its default settings:

```
[in IP-GLOBAL:dhcp-server:static-address[1] (new)]
ip-address = 0.0.0.0
ethernet-address = 00:00:00:00:00:00
```

Location `IP-GLOBAL:dhcp-server`

STM

Description A profile that contains configuration settings for an STM-0 slot card.

Usage Following is a listing of an `stm` profile with its default settings:

```
[in STM/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
loop-timing = yes
```

STM-PATH

Description A profile that contains configuration settings for a Synchronous Transport Module (STM) path.

Usage Following is a listing of an `stm-path` profile with its default settings:

```
[in STM-PATH/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
tributary-mapping = vc-11-async-mapping
```

STM-PATH-STAT

Description A profile that contains Synchronous Transport Module (STM) path statistics.

Usage Following is a sample listing of an `stm-path-stat` profile:

```
[in STM-PATH-STAT/{ shelf-1 slot-2 1 }]
physical-address* = { shelf-1 slot-2 1 }
path-state = available
ais-receive = False
loss-of-pointer = False
signal-degrade = False
signal-fail = False
trace-id-mismatch = False
performance-monitoring = { 0 0 0 0 0 0 0 0 }
interval-performance-monitoring = [ { 0 0 0 0 0 0 0 0 } {0 0 0 0 0 0 0 0 +
```

STM-STAT

Description A profile that contains Synchronous Transport Module (STM) line statistics.

Usage Following is a sample listing of an `stm-stat` profile:

```
[in STM-STAT/{ shelf-1 slot-2 1 }]
physical-address* = { shelf-1 slot-2 1 }
line-state = available
loss-of-signal = False
loss-of-frame = False
ais-receive = False
rdi-receive = False
signal-degrade = True
signal-fail = True
trace-id-mismatch = False
performance-monitoring = { 0 0 0 0 0 0 0 0 0 0 0 0 }
interval-performance-monitoring = [ { 0 0 0 0 0 0 0 0 0 0 0 0 } { 0 0 0 0 0+
```

svc-options

Description A subprofile that enables you to set values for switched virtual circuits (SVCs).

Usage Following are listings of `svc-options` subprofiles with their default settings:

```
[in ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options (new)]
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 }
```

```
[in CONNECTION/"":atm-options:svc-options (new)]
enabled = no
incoming-caller-addr = { undefined "" { undefined { "" "" } { "" "" "" } } }
outgoing-called-addr = { undefined "" { undefined { "" "" } { "" "" "" } } }
```

```
[in FRAME-RELAY/"":svc-options (new)]
enabled = no
fr-address = ""
```

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }`
`CONNECTION/"":atm-options`
`FRAME-RELAY/""`

SWAN

Description A profile that contains line-configuration settings for a Serial WAN (SWAN) slot card.

Usage Following is a listing of a `swan` profile with its default settings:

```
[in SWAN/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
line-config = { 0 1 static { external-clock 1 2 2048000 } }
```

SYSTEM

Description A profile that contains system-wide settings for call management.

Usage Following is a listing of a `system` profile with its default settings:

```
[in SYSTEM (new)]
name = ""
system-rmt-mgmt = yes
v110-subaddress = 0
use-trunk-groups = no
num-digits-trunk-groups = 1
idle-logout = 0
max-dialout-time = 20
parallel-dialing = 12
single-file-incoming = yes
analog-encoding = u-law
sessionid-base = 0
t-online = no
t-online-most-avail-chan = no
call-routing-sort-method = item-first
digital-call-routing-sort-method = slot-first
new-nas-port-id-format = yes
perm-conn-upd-mode = all
userstat-format = "%i %l %s %r %d %a %u %c %t %n"
boot-sr-version = 9.1.0c7
country = us
nas-port-format = not-applicable
```

T

T1

Description A profile that contains configuration settings for a T1 line and its channels.

Usage Following is a listing of a `t1` profile with its default settings:

```
[in T1/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
line-interface = { no d4 ami eligible middle-priority inband te wink-start +
```

T1-STAT

Description A read-only profile that displays information about the state of a T1 line and its channels.

Usage Following is a listing of a `t1-stat` profile:

```
[in T1-STAT/{ shelf-1 slot-1 1 }]
physical-address* = { shelf-1 slot-1 1 }
line-state = disabled
channel-state = [ disabled disabled disabled disabled disabled disabled +
error-count = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 ]
loss-of-carrier = False
loss-of-sync = False
ais-receive = False
yellow-receive = False
ber-receive = False
carrier-established = False
network-loopback = False
```

T3

Description A profile that contains configuration settings for a DS3 line.

Usage Following is a listing of a `t3` profile with its default settings:

```
[in T3/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
frame-type = m13
line-length = 0-225
loopback = no-loopback
```

T3-STAT

Description A read-only profile that displays information about the state of a DS3 line and its individual multiplexed DS2 lines.

Usage Following is a sample listing of a `t3-stat` profile:

```
[in T3-STAT/{ shelf-1 slot-1 0 }]
physical-address* = { shelf-1 slot-1 0 }
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
```

table-config

Description A subprofile that contains eight subprofiles for configuring a local Domain Name System (DNS) table.

Usage Following is a listing of all the `table-config` subprofiles for a DNS table:

```
[in IP-GLOBAL:dns-local-table:table-config (new)]
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 }
```

Following is a listing of an individual `table-config` subprofile with its default settings:

```
[in IP-GLOBAL:dns-local-table:table-config[1] (new)]
host-name = ""
ip-address = 0.0.0.0
```

Location `IP-GLOBAL:dns-local-table`

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 Following is a listing of a `tac-auth-client` subprofile with its default settings:

```
[in EXTERNAL-AUTH:tac-auth-client (new)]
auth-server-1 = 0.0.0.0
auth-server-2 = 0.0.0.0
auth-server-3 = 0.0.0.0
auth-port = 0
auth-src-port = 0
auth-key = ""
auth-timeout = 0
```

Location `EXTERNAL-AUTH`

tacplus-acct-client

Description A subprofile that defines how the TAOS unit interacts as a client of Terminal Access Controller Access Control Plus (TACACS+) accounting servers.

Usage Following is a listing of a `tacplus-acct-client` subprofile with its default settings:

```
[in EXTERNAL-AUTH:tacplus-acct-client (new)]
acct-server-1 = 0.0.0.0
acct-server-2 = 0.0.0.0
acct-server-3 = 0.0.0.0
acct-port = 0
acct-src-port = 0
acct-key = ""
```

Location EXTERNAL-AUTH

tacplus-auth-client

Description A subprofile that defines how the TAOS unit interacts as a client of Terminal Access Controller Access Control Plus (TACACS+) authentication servers.

Usage Following is a listing of a `tacplus-auth-client` subprofile with its default settings:

```
[in EXTERNAL-AUTH:tacplus-auth-client (new)]
auth-server-1 = 0.0.0.0
auth-server-2 = 0.0.0.0
auth-server-3 = 0.0.0.0
auth-port = 0
auth-src-port = 0
auth-key = ""
auth-timeout-time = 0
auth-retries = 0
```

Location EXTERNAL-AUTH

tag-map

Description A subprofile that enables you to assign a specific priority to a packet on the basis of the value of the packet's Internet Protocol (IP) type of service (TOS) byte. Up to 64 different values of the IP TOS byte can be mapped to an individual priority level.

Usage Following is a listing of the `tag-map` subprofiles:

```
[in QOS:tag-map]
tag-map[1] = { no 00 0 }
tag-map[2] = { no 00 0 }
tag-map[3] = { no 00 0 }
...
tag-map[64] = { no 00 0 }
```

Following is a listing of an individual `tag-map` subprofile with its default settings:

```
[in QOS:tag-map[1]]
active = no
dscp = 00
qos-tag = 0
```

Location QOS

tcp-clear-answer

Description A subprofile containing default settings for TCP-Clear connections.

Usage Following is a listing of a `tcp-clear-answer` subprofile with its default settings:

```
[in ANSWER-DEFAULTS:tcp-clear-answer (new)]
enabled = yes
```

Location `ANSWER-DEFAULTS`

tcp-clear-options

Description A subprofile with default settings for TCP-Clear connections.

Usage Following is a listing of a `tcp-clear-options` subprofile with its default settings:

```
[in CONNECTION/"":tcp-clear-options (new)]
host = ""
port = 0
host2 = ""
port2 = 0
host3 = ""
port3 = 0
host4 = ""
port4 = 0
detect-end-of-packet = no
end-of-packet-pattern = ""
flush-length = 256
flush-time = 20
```

Dependencies Consider the following:

- For the settings in the `tcp-clear-options` subprofile to apply, you must set `enabled` to `yes` in the `tcp-clear-answer` subprofile.
- TCP-Clear connections are managed by virtual router (VRouter). 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/""`

telco-options

Description A subprofile that enables you to set telephone-company options for a connection.

Usage Following is a listing of a `telco-options` subprofile with its default settings:

```
[in CONNECTION/"":telco-options (new)]
answer-originate = ans-and-orig
callback = no
call-type = off
nailed-groups = 1
ft1-caller = no
force-56kbps = no
data-service = 56k-clear
call-by-call = 0
billing-number = ""
transit-number = ""
expect-callback = no
dialout-allowed = no
delay-callback = 0
nas-port-type = any
```

Location `CONNECTION/""`

telnet-options

Description A subprofile that contains `telnet` options for interactive users.

Usage Following is a listing of a `telnet-options` subprofile with its default settings:

```
[in TERMINAL-SERVER:terminal-mode-configuration:telnet-options (new)]
telnet = no
telnet-mode = ascii
auto-telnet = no
local-echo = no
```

Location `TERMINAL-SERVER:terminal-mode-configuration`

terminal-mode-configuration

Description A subprofile containing terminal-server configuration options for interactive users.

Usage Following is a listing of a `terminal-mode-configuration` subprofile with its default settings:

```
[in TERMINAL-SERVER:terminal-mode-configuration (new)]
silent-mode = no
clear-screen = yes
system-password = ""
banner = "** Ascend TNT Terminal Server **"
login-prompt = "Login: "
password-prompt = "Password: "
third-login-prompt = ""
```

```
third-prompt-sequence = last
prompt = "ascend% "
terminal-type = vt100
clear-call = no
buffer-chars = yes
ping = no
traceroute = no
tcp = no
rlogin-options = { no 1023 128 }
telnet-options = { no ascii no no }
ip-add-msg = "IP address is "
prompt-format = no
login-timeout = 300
```

Location TERMINAL-SERVER

TERMINAL-SERVER

Description A profile that enables you to configure terminal-server features.

Usage Following is a listing of the `terminal-server` profile with its default settings:

```
[in TERMINAL-SERVER (new)]
enabled = no
security-mode = none
modem-configuration = { will-v42 33600-max-baud -13-db-mdm-trn-level no +
terminal-mode-configuration = { no yes "" "** Ascend TNT Terminal Server +
immediate-mode-options = { none no "" 0 }
menu-mode-options = { no no no "" "" telnet 0 "" "" "" telnet 0 "" "" "" +
ppp-mode-configuration = { no 5 no session-ppp }
slip-mode-configuration = { no no basic-slip no }
dialout-configuration = { no no 5000 "" none }
```

THERMAL

Description A profile that enables you to control fan tray operations.

Usage Following is a listing of the `thermal` profile with its default settings:

```
[in THERMAL]
fantray-lownoise-rpm = 2500
operation-mode = full-speed-only
low-temperature-threshold = 34
high-temperature-threshold = 40
alarm-temperature-trigger = 55
```

Dependencies Because the fan speed is automatically controlled, only the `alarm-temperature-trigger` parameter is supported on an APX 1000 unit.

time

Description A subprofile that specifies the current hour, minute, and second.

Usage Following is a listing of a `time` subprofile:

```
[in TIMEDATE:time]
hour = 8
minute = 21
second = 3
```

Dependencies You can also use the `date` command to set the current hour, minute, and second.

Location `TIMEDATE`

TIMEDATE

Description A profile that shows the current system time and date.

Usage Following is a listing of a `timedate` profile:

```
[in TIMEDATE]
time = { 8 21 3 }
date = { Monday October 2001 15 }
```

tos

Description A subprofile that enables you to configure differentiated services code point (DSCP) marking for Signaling System 7 (SS7) signaling traffic.

Usage Following is a listing of a `tos` subprofile with its default settings:

```
[in SS7-GATEWAY:transport-options:tos (new)]
active = no
precedence = 000
type-of-service = normal
apply-to= both
marking-type = dscp
dscp = 00
```

Location `SS7-GATEWAY:transport-options`

tos-filter

Description A subprofile containing a type of service (TOS) filter specification.

Usage Following is a listing of a `tos-filter` subprofile for an input filter, with its default settings:

```
[in FILTER/"":input-filters[1]:tos-filter (new)]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
```

```
dest-address = 0.0.0.0
src-port-cmp = none
source-port = 0
dst-port-cmp = none
dest-port = 0
precedence = 000
type-of-service = normal
marking-type = precedence-tos
dscp = 00
```

Following is a listing of a `tos-filter` subprofile for an output filter, with its default settings:

```
[in FILTER/"":output-filters[1]:tos-filter (new)]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
src-port-cmp = none
source-port = 0
dst-port-cmp = none
dest-port = 0
precedence = 000
type-of-service = normal
marking-type = precedence-tos
dscp = 00
```

Location `FILTER/"":input-filters`
`FILTER/"":output-filters`

tos-options

Description A subprofile that enables you to set type of service (TOS) values.

Usage Following are listings of `tos-options` subprofiles with their default settings:

```
[in CONNECTION/"":ip-options:tos-options (new)]
active = no
precedence = 000
type-of-service = normal
apply-to = incoming
marking-type = precedence-tos
dscp = 00
```

```
[in VOIP/{ "" "" }:tos-options (new)]
active = no
precedence = 101
type-of-service = latency
apply-to = both
marking-type = precedence-tos
dscp = 00
```

Location `CONNECTION/"":ip-options`
`VOIP/{ "" "" }`

traffic-shapers

Description A subprofile containing traffic-shaper specifications for Asynchronous Transfer Mode (ATM) traffic. Each specification enables you to define the characteristics for different types of data traffic. The index for each subprofile is a traffic-shaper number from 1 through 15.

Usage Following is a listing of all the `traffic-shapers` subprofiles for a DS3-ATM slot card:

```
[in DS3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers (new)]
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 }
```

Following is a listing of an individual `traffic-shapers` subprofile for a DS3-ATM slot card, with its default settings:

```
[in DS3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[1] (new)]
enabled = no
bit-rate = 1000
peak-rate = 1000
max-burst-size= 2
aggregate = no
priority = 0
```

Following is a listing of all the `traffic-shapers` subprofiles for an E3-ATM slot card:

```
[in E3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers (new)]
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 }
```

Following is a listing of an individual `traffic-shapers` subprofile for an E3-ATM slot card, with its default settings:

```
[in E3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[1] (new)]
enabled = no
bit-rate = 1000
peak-rate = 1000
max-burst-size= 2
aggregate = no
priority = 0
```

Following is a listing of all the `traffic-shapers` subprofiles for an OC3-ATM slot card:

```
[in OC3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers (new)]
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 }
```

Following is a listing of an individual `traffic-shapers` subprofile for an OC3-ATM slot card, with its default settings:

```
[in OC3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[1] (new)]
enabled = no
bit-rate = 1000
peak-rate = 1000
max-burst-size= 2
aggregate = no
priority = 0
```

Location `DS3-ATM/{ any-shelf any-slot 0 }:line-config`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config`

TRANSACTION-SERVER

Description A profile that enables you to specify values for the metrics used in the server selection table.

Usage Following is a listing of a `transaction-server` profile with its default settings:

```
[in TRANSACTION-SERVER (new)]
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
```

transport-options

Description A subprofile that contains settings for changing the operation of Signaling System 7 (SS7) data delivery layer (DDL) timers.

At times, you might need to change the duration of various SS7 DDL timers to fine-tune a signaling link. For example, you might want to change time-outs 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 Following is a listing of a `transport-options` subprofile with its default settings:

```
[in SS7-GATEWAY:transport-options (new)]
type = ascend
device-id = 0
t1-duration = 1000
t2-duration = 3000
t3-duration = 30000
window-size = 7
ack-threshold = 6
heart-beat = no
```

Location `SS7-GATEWAY`

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 trap to the SNMP manager.

Usage Following is a listing of a `trap` profile with its default settings:

```
[in TRAP/"" (new)]
host-name* = ""
active-enabled = yes
community-name = ""
host-address = 0.0.0.0
host-port = 162
notify-tag-list = default
target-params-name = default
alarm-enabled = yes
security-enabled = no
port-enabled = no
slot-enabled = no
coldstart-enabled = yes
warmstart-enabled = yes
linkdown-enabled = yes
linkup-enabled = yes
ascend-enabled = yes
console-enabled = yes
use-exceeded-enabled = yes
password-enabled = yes
fr-linkup-enabled = yes
fr-linkdown-enabled = yes
event-overwrite-enabled = yes
radius-change-enabled = yes
mcast-monitor-enabled = yes
lan-modem-enabled = yes
dirdo-enabled = yes
slot-profile-change-enabled = yes
power-supply-enabled = yes
authentication-enabled = yes
config-change-enabled = yes
suspect-access-resource-enabled = yes
ospf-enabled = no
ospf-if-config-error-enabled = no
ospf-if-auth-failure-enabled = no
ospf-if-state-change-enabled = no
ospf-if-rx-bad-packet = no
ospf-tx-retransmit-enabled = no
ospf-nbr-state-change-enabled = no
ospf-virt-if-config-error-enabled = no
ospf-virt-if-auth-failure-enabled = no
ospf-virt-if-state-change-enabled = no
ospf-virt-if-rx-bad-packet = no
ospf-virt-if-tx-retransmit-enabled = no
```

```
ospf-virt-nbr-state-change-enabled = no
ospf-originatelsa-enabled = no
ospf-maxagelsa-enabled = no
ospf-lsdb-overflow-enabled = no
ospf-approaching-overflow-enabled = no
call-log-serv-change-enabled = yes
voip-gk-change-enabled = yes
wan-line-state-change-enabled = yes
call-log-dropped-pkt-enabled = yes
megaco-link-status-enabled = no
secondary-controller-state-change-enabled = no
ascend-link-down-trap-enabled = no
ascend-link-up-trap-enabled = no
l2tp-tunnel-trap-enabled = yes
notification-log-enable = no
```

tree-properties

Description A subprofile that enables you to define a view name and an object identifier (OID) for a view-based access control model (VACM) configuration.

Usage Following is a listing of the `tree-properties` subprofile with its default settings:

```
[in VACM-VIEW-TREE/{ "" "" }:tree-properties (new)]
view-name = ""
view-tree-oid = ""
```

Location `VACM-VIEW-TREE`

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 Following is a listing of a `tunnel-options` subprofile with its default settings:

```
[in CONNECTION/"":tunnel-options (new)]
profile-type = disabled
tunneling-protocol = atmp-protocol
max-tunnels = 0
atmp-ha-rip = rip-off
primary-tunnel-server = ""
secondary-tunnel-server = ""
udp-port = 5150
password = ""
home-network-name = ""
client-auth-id = ""
server-auth-id = ""
vrouter = ""
assignment-id = ""
```

Location `CONNECTION/""`

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 Following is a listing of a `tunnel-server` profile with its default settings:

```
[in TUNNEL-SERVER/"" (new)]
server-endpoint* = ""
enabled = yes
shared-secret = ""
client-auth-id = ""
server-auth-id = ""
dialout-options = { no "" "" "" "" no no }
```

U

UDS3

Description A profile that enables you to configure an unchannelized DS3 line.

Usage Following is a listing of a `uds3` profile with its default settings:

```
[in UDS3/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
line-config = { 0 1 static c-bit-parity b3zs no-loopback no }
```

UDS3-STAT

Description A read-only profile that indicates the status of an unchannelized DS3 line.

Usage Following is a sample listing of a `uds3-stat` profile:

```
[in UDS3-STAT/{ shelf-1 slot-10 1 }]
physical-address* = { shelf-1 slot-10 1 }
line-state = loss-of-signal
f-bit-error-count = 0
p-bit-error-count = 0
cp-bit-error-count = 2
feb-error-count = 17
bpv-error-count = 6724
loss-of-signal = True
loss-of-frame = False
yellow-receive = False
ais-receive = False
```

USER

Description A profile that defines a name, a password, privileges, and default displays for user login accounts.

Usage Following is a listing of a `user` profile with its default settings:

```
[in USER/"" (new)]
name* = ""
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 = *
default-status = no
top-status = general-info
bottom-status = log-window
left-status = connection-list
screen-width = 80
screen-length = 24
status-length = 18
use-scroll-regions = no
log-display-level = none
```

usrRad-options

Description A subprofile that defines connection-specific Remote Authentication Dial-In User Service (RADIUS) accounting options.

Usage Following is a listing of a `usrRad-options` subprofile with its default settings:

```
[in CONNECTION/"":usrRad-options (new)]
acct-type = global
acct-host = 0.0.0.0
acct-port = 1646
acct-key = ""
acct-timeout = 1
acct-id-base = acct-base-10
```

Dependencies RADIUS accounting must be configured in the `rad-acct-client` subprofile of the `external-auth` profile.

Location `CONNECTION/""`

V

v120-answer

Description A subprofile containing default settings for V.120 calls.

Usage Following is a listing of a v120-answer subprofile with its default settings:

```
[in ANSWER-DEFAULTS:v120-answer (new)]
enabled = yes
frame-length = 256
```

Location ANSWER-DEFAULTS

VACM-ACCESS

Description A profile that enables you to map a group name, context prefix, context name, security model, and security level to a view name in a view-based access control model (VACM) configuration.

Usage Following is a listing of a vacm-access profile with its default settings:

```
[in VACM-ACCESS/{ "" "" v1 no+ } (new)]
access-properties* = { "" "" v1 no+ }
active = no
match-method = exact-match
read-view-name = ""
write-view-name = ""
notify-view-name = ""
```

VACM-SECURITY-GROUP

Description A profile that enables you to map a security name and security model to a security group for view-based access control model (VACM) configurations.

Usage Following is a listing of a vacm-security-group profile with its default settings:

```
[in VACM-SECURITY-GROUP/{ v1 "" } (new)]
security-properties* = { v1 "" }
active = no
group-name = ""
```

VACM-VIEW-TREE

Description A profile that enables you to define a view in a view-based access control model (VACM) configuration.

Usage Following is a listing of a vacm-view-tree profile with its default settings:

```
[in VACM-VIEW-TREE/{ "" "" } (new)]
tree-properties* = { "" "" }
active = no
tree-type = included
```

virtual-ds1-line-status

Description A subprofile that indicates the status of up to 28 DS1 virtual tributaries on a Peripheral Control Timing Facilities Interface (PCTFI) slot card.

Usage Following is a listing of all the `virtual-dsl-line-status` subprofiles for a particular PCTFI slot card:

```
[in PCTFI-STAT/{ shelf-1 slot-5 0 }:virtual-ds1-line-status]
virtual-ds1-line-status[1] = { operational non-cas }
virtual-ds1-line-status[2] = { operational non-cas }
virtual-ds1-line-status[3] = { operational non-cas }
virtual-ds1-line-status[4] = { operational non-cas }
virtual-ds1-line-status[5] = { operational non-cas }
virtual-ds1-line-status[6] = { operational non-cas }
virtual-ds1-line-status[7] = { operational non-cas }
virtual-ds1-line-status[8] = { operational non-cas }
virtual-ds1-line-status[9] = { operational non-cas }
virtual-ds1-line-status[10] = { operational non-cas }
virtual-ds1-line-status[11] = { operational non-cas }
virtual-ds1-line-status[12] = { operational non-cas }
virtual-ds1-line-status[13] = { operational non-cas }
virtual-ds1-line-status[14] = { operational non-cas }
virtual-ds1-line-status[15] = { operational non-cas }
virtual-ds1-line-status[16] = { operational non-cas }
virtual-ds1-line-status[17] = { operational non-cas }
virtual-ds1-line-status[18] = { operational non-cas }
virtual-ds1-line-status[19] = { operational non-cas }
virtual-ds1-line-status[20] = { operational non-cas }
virtual-ds1-line-status[21] = { operational non-cas }
virtual-ds1-line-status[22] = { operational non-cas }
virtual-ds1-line-status[23] = { operational non-cas }
virtual-ds1-line-status[24] = { operational non-cas }
virtual-ds1-line-status[25] = { operational non-cas }
virtual-ds1-line-status[26] = { operational non-cas }
virtual-ds1-line-status[27] = { operational non-cas }
virtual-ds1-line-status[28] = { operational non-cas }
```

Following is a listing of an individual `virtual-dsl-line-status` subprofile:

```
[in PCTFI-STAT/{ shelf-1 slot-5 0 }:virtual-ds1-line-status[1]]
f1-bit-state = 0
trunk-state = operational
f4-bit-state = non-cas
```

Location `PCTFI-STAT`

visa2-answer

Description A subprofile that lets you specify whether the system rejects incoming Visa terminal calls.

Usage Following is a listing of a `visa2-answer` subprofile with its default setting:

```
[in ANSWER-DEFAULTS:visa2-answer (new)]
enabled = no
```

Location `ANSWER-DEFAULTS`

visa2-options

Description A subprofile that contains settings for Visa terminal calls.

Usage Following is a listing of a `visa2-options` subprofile with its default settings:

```
[in CONNECTION/"":visa2-options (new)]
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
```

Location `CONNECTION/""`

VOIP

Description A profile that enables you to configure Voice over IP (VoIP).

Usage Following is a listing of a `voip` profile with its default settings:

```
[in VOIP/{ "" "" } (new)]
voip-index* = { "" "" }
gatekeeper-ip = 0.0.0.0
gk-mlg-control = no
vpn-mode = no
single-dial-enable = no
packet-audio-mode = g711-ulaw
frames-per-packet = 2
tos-options = { no 101 latency both precedence-tos 00 }
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 = 672
cut-thru-enable-nearend = yes
```

```
h323-voice-ann-enabled = no
voice-ann-dir = /current
voice-ann-enc = g711-ulaw
call-inter-digit-timeout = 6000
silence-threshold = 0
dtmf-tone-passing = dtmf-tone-passed-inband
rt-fax-options = { no yes yes yes yes 0 no 14400 }
call-hairpin = no
call-keep-alive-timeout = 300
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
pstn-attribute = { no no-progress-indicator no-progress-indicator speech }
sequential-call-enable = yes
ss7voip-call-persistence = no
next-call = **9
rtpqos-polling-enable = no
faststart-enable = yes
signaling-tos = { no 000 normal both dscp 00 }
```

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 Following is a listing of a `voip-index` subprofile with its default settings:

```
[in VOIP/{ "" "" }:voip-index (new)]
gateway-access-number = ""
far-end-number = ""
```

Location `VOIP/{ "" "" }`

VROUTER

Description A profile that enables you to configure settings for a virtual router (VRouter).

Usage Following is a listing of a `vrouter` profile with its default settings:

```
[in VROUTER/"" (new)]
name* = ""
active = yes
vrouter-ip-addr = 0.0.0.0
pool-base-address = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 +
assign-count = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
pool-name = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" +
```

```
pool-summary = no
share-global-pool = yes
rip-policy = Poison-Rvrs
summarize-rip-routes = no
rip-trigger = yes
domain-name = ""
sec-domain-name = ""
dns-primary-server = 0.0.0.0
dns-secondary-server = 0.0.0.0
client-primary-dns-server = 0.0.0.0
client-secondary-dns-server = 0.0.0.0
allow-as-client-dns-info = True
ipx-routing-enabled = yes
ipx-dialin-pool = 00:00:00:00
```

Dependencies Deleting a `vrouter` profile deletes the VRouter. If you delete a VRouter with active connections, a restart is recommended. If you cannot restart the system, you must manually close 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.

W

WATCHDOG-CONFIG

Description A system-created profile that enables you to configure a *watchdog* name and enable warning traps. A watchdog is a software routine that monitors the status of a particular aspect of a TAOS unit.

Usage Following is a listing of a `watchdog-config` profile with its default settings:

```
[in WATCHDOG-CONFIG/{  none 0 } (new)]
watchdog-index* = {  none 0 }
watchdog-trap-enable = yes
watchdog-name = ""
```

APX/MAX TNT Parameter Reference

3

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

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/"":visa2-options

2-char-sequence

Description Specifies a sequence of two character values 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/"":visa2-options

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 one of the following settings:

- yes enables the use of 7-bit even parity for data sent to dial-in terminal-server users.
- no (the default) specifies 8-bit communication, in which no parity bit applies. Accept the default value for most applications.

Example `set 7-even = no`

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

Location TERMINAL-SERVER:modem-configuration

8e1

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

Usage The 8e1 value is read-only and can have one of the following settings:

- auto (the default) indicates that the system loads images for slot cards that are installed in the TAOS unit, and skips images for slot cards that are not installed.
- load indicates that the system loads the image, even if no slot card of that type is installed.
- skip indicates that the system skips the image, even if a slot card of that type is installed.

Example `8e1 = skip`

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

8t1

Description Indicates the action to take when the code image for a T1 slot card is present in a `tar` file.

Usage The `8t1` value is read-only and can have one of the following settings:

- `auto` (the default) indicates that the system loads images for slot cards that are installed in the TAOS unit, and skips images for slot cards that are not installed.
- `load` indicates that the system loads the image, even if no slot card of that type is installed.
- `skip` indicates that the system skips the image, even if a slot card of that type is installed.

Example `8t1 = skip`

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

A

accept-policy

Description Specifies the `bgp-policy` profile that defines an acceptance policy.

Usage Specify a string of up to 15 characters. The default is null.

Example `set accept-policy = two_networks`

Location `BGP-PEER/""`

acct-checkpoint

Description Specifies the interval (in minutes) at which to send checkpoint packets to the Remote Authentication Dial-In User Service (RADIUS) server.

Usage Specify an integer from 0 through 1440. The default is 0 (zero).

Example `set acct-checkpoint = 5`

Dependencies For `acct-checkpoint` to apply, you must set `acct-type` to `radius`.

Location `EXTERNAL-AUTH:rad-acct-client`

acct-checkpoint-timer

Description Specifies whether to send Remote Authentication Dial-In User Service (RADIUS) checkpoint accounting packets on a per-session basis.

Usage Specify one of the following settings:

- `per-session` specifies that checkpoint packets are sent on a per-session basis at the interval specified by the `acct-checkpoint` parameter.
- `all-sessions` (the default) specifies that checkpoint packets are all sent at the same time.

Example `set acct-checkpoint-timer = per-session`

Dependencies For `acct-checkpoint-timer` to apply, you must set `acct-type` to `radius`.

Location `EXTERNAL-AUTH:rad-acct-client`

acct-drop-stop-on-auth-fail

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

Usage Specify one of the following settings:

- `yes` specifies that RADIUS accounting Stop packets are dropped for connections that fail authentication.
- `no` (the default) specifies that RADIUS accounting Stop packets are sent for connections that fail authentication.

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

Dependencies For `acct-drop-stop-on-auth-fail` to apply, you must set `acct-type` to `radius`.

Location `EXTERNAL-AUTH:rad-acct-client`

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`

Dependencies For `acct-host` to apply, you must set `acct-type` to `radius`.

Location `CONNECTION/"":usrRad-options`

acct-host-1
acct-host-2
acct-host-3

Description Specifies the Domain Name System (DNS) hostnames or IP addresses of up to three Remote Authentication Dial-In User Service (RADIUS) accounting servers. 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 to connect to host #3.

Usage Specify a DNS hostname or an IP address in dotted decimal notation. The default is null, which indicates that no RADIUS accounting server exists.

Example `set acct-host-1 = alameda`

Dependencies Consider the following:

- If `acct-type` does not specify RADIUS, `acct-host-1`, `acct-host-2`, and `acct-host-3` do not apply.
- If the TAOS unit connects to a server other than host #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.
- You cannot configure an `acct-host-`*`n`* parameter and an `acct-server-`*`n`* parameter with the same index. For example, you cannot configure `acct-host-1` and `acct-server-1`. However, you can configure an `acct-host-`*`n`* parameter and an `acct-server-`*`n`* parameter with different indexes, such as `acct-host-1` and `acct-server-2`.

Location `EXTERNAL-AUTH:rad-acct-client`

acct-id-base

Description Specifies the numeric base of the Remote Authentication Dial-In User Service (RADIUS) `Acct-Session-ID` attribute.

Usage Specify one of the following settings:

- `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-16`

Dependencies Consider the following:

- For `acct-id-base` to apply, you must set `acct-type` to `radius`.
- Changing the value of `acct-id-base` while accounting sessions are active results in inconsistent reporting between Start and Stop records.
- You can set `acct-id-base` globally and for each connection.
- The `Acct-Session-ID` attribute is defined in section 5.5 of the RADIUS accounting specification.

Location `CONNECTION/"":usrRad-options`
`EXTERNAL-AUTH:rad-acct-client`

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 For `acct-key` to apply, you must set `acct-type` to `radius` or `tacacsplus`.

Location `CONNECTION/"":usrRad-options`
`EXTERNAL-AUTH:rad-acct-client`
`EXTERNAL-AUTH:tacplus-auth-client`

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.

Example `set acct-limit-retry = 10`

Dependencies Consider the following:

- For `acct-limit-retry` to apply, you must set `acct-type` to `radius`.
- 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.

Location `EXTERNAL-AUTH:rad-acct-client`

acct-port

Description Specifies the User Datagram Protocol (UDP) destination port to use for external accounting requests.

Usage Specify a UDP port number from `1` through `32767`. The value must match the port number the accounting daemon uses. When you use Remote Authentication Dial-In User Service (RADIUS) accounting, 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+) accounting, the default is `49`.

Example `set acct-port = 1500`

Dependencies Consider the following:

- For `acct-port` to apply, you must set `acct-type` to `radius` or `tacacsplus`.
- When using RADIUS accounting, you can set `acct-port` globally and for each connection.

Location `CONNECTION/"":usrRad-options`
`EXTERNAL-AUTH:rad-acct-client`
`EXTERNAL-AUTH:tacplus-auth-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 VSAs to the RADIUS server and does not recognize VSAs if the server sends them. 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.

Example `set acct-radius-compat = vendor-specific`

Dependencies Consider the following

- For `acct-radius-compat` to apply, you must set `acct-type` to `radius`.
- At this time, only NavisRadius™ supports 16-bit VSAs.

Location `EXTERNAL-AUTH:rad-acct-client`

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 an integer. 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-host` and you must set `acct-type` to `radius`.

Location `EXTERNAL-AUTH:rad-acct-client`

acct-server-1
acct-server-2
acct-server-3

Note These parameters have been replaced by the `acct-host-1`, `acct-host-2`, and `acct-host-3` parameters. The `acct-server-1`, `acct-server-2`, and `acct-server-3` parameters have been retained for compatibility with earlier TAOS versions.

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:

- For `acct-server` to apply, you must set `acct-type` to `radius` or `tacacsplus`.
- 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-auth-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` through `65535`. The default is `0` (zero), which disables regular RADIUS open-session reports.

Example `set acct-sess-interval = 15`

Dependencies For `acct-sess-interval` to apply, you must set `acct-type` to `radius`.

Location `EXTERNAL-AUTH:rad-acct-client`

acct-src-port

Description Specifies the User Datagram Protocol (UDP) source port to use for Remote Authentication Dial-In User Service (RADIUS) accounting.

Usage Specify a value from 0 through 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 Consider the following:

- For `acct-src-port` to apply, you must set `acct-type` to `radius` or `tacacsplus`.
- 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-auth-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 one of the following settings:

- `yes` (the default) 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`

Dependencies For `acct-stop-only` to apply, you must set `acct-type` to `radius`.

Location `EXTERNAL-AUTH:rad-acct-client`

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.

Usage Specify an integer from 1 through 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 Consider the following:

- For acct-timeout to apply, you must set acct-type to radius. You can use acct-timeout only for RADIUS accounting. Because Terminal Access Controller Access Control Plus (TACACS+) uses Transmission Control Protocol (TCP), it has its own time-out method.
- 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-host. If all RADIUS accounting servers are busy, the TAOS unit stores the accounting request and tries again at a later time. The unit can queue up to 154 requests.

Location CONNECTION/"":usrRad-options
EXTERNAL-AUTH:rad-acct-client

acct-tunnel-connection-encoding

Description Specifies the encoding method used for the Remote Authentication Dial-In User Service (RADIUS) Acct-Tunnel-Connection attribute.

Usage Specify one of the following settings:

- normal (the default) specifies that the value indicated by the Acct-Tunnel-Connection attribute consists of the source and destination IP addresses, tunnel IDs, and connection IDs. This value is for use with NavisRadius™.
- decimal-call-serial-number specifies that the value indicated by the Acct-Tunnel-Connection attribute represents the 32-bit Layer 2 Tunneling Protocol (L2TP) call serial number (CSN) as present in the Incoming Call Request (ICRQ) or Outgoing Call Request (OCRQ) L2TP message, encoded as a decimal string. For the tunnel itself, no CSN exists, and the 32-bit value that is encoded represents the initiator Tunnel ID in the low 16 bits and the server Tunnel ID in the high 16 bits.
- hexadecimal-call-serial-number specifies that the value indicated by the Acct-Tunnel-Connection attribute represents the L2TP CSN as present in the ICRQ or OCRQ L2TP message, encoded as a hexadecimal string.

Example `set acct-tunnel-connection-encoding = decimal-call-serial-number`

Dependencies Consider the following:

- For `acct-tunnel-connection-encoding` to apply, you must set `acct-type` to `radius`.
- There is no guarantee that the CSN is unique at all times. Even in a single tunnel, identical CSN values can occur if tunnel links are initiated from both the L2TP access concentrator (LAC) and the L2TP network server (LNS) side. Therefore, use caution when specifying the CSN with the `Acct-Tunnel-Connection` attribute.

Location `L2-TUNNEL-GLOBAL:l2tp-config`

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.

Usage To enable or disable accounting globally in the `external-auth` profile, specify one of the following settings:

- `none` (the default) disables accounting.
- `radius` enables RADIUS accounting.
- `tacacsplus` enables TACACS+ accounting.

To set the accounting policy for a particular connection, specify one of the following settings in a `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-host` to specify at least one accounting server, and that server must be running a version of the daemon that specifically supports accounting.

Location `CONNECTION/"":usrRad-options`
`EXTERNAL-AUTH`

ack-threshold

Description Specifies the threshold for triggering an acknowledgment while receiving data packets.

Usage Specify an integer from 1 through 63. The default is 6.

Example `set ack-threshold = 10`

Dependencies Consider the following:

- As soon as the specified number of packets is received, the TAOS unit sends an acknowledgment back (regardless of the value of `t1-duration`).
- The value you specify for `ack-threshold` cannot be greater than the value of `window-size`.

Location `SS7-GATEWAY:transport-options`

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 settings:

- `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[`*n*`]:route-filter`
`FILTER/"":output-filters[`*n*`]:route-filter`

activation

Description Selects the signals that indicate that the data circuit-terminating equipment (DCE) is ready to connect.

Usage Specify one of the following settings:

- `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 `DS3-ATM/{ any-shelf any-slot 0 }:line-config`
`SWAN/{ any-shelf any-slot 0 }:line-config`
`UDS3/{ any-shelf any-slot 0 }:line-config`

active

Description Activates an interface, profile, route, or feature.

Usage Specify one of the following settings:

- yes activates the interface, profile, route, or feature.
- no (the default) makes the interface, profile, route, or feature unavailable for use.

Example `set active = yes`

Dependencies 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.

Location
```
ATMSVC-ROUTE/""
CONNECTION/""
CONNECTION/"":ip-options:ospf-options
CONNECTION/"":ip-options:tos-options
FRAME-RELAY/""
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf
IP-GLOBAL:bootp-relay
IP-GLOBAL:dhcp-server
MULTI-LINK-FR/""
QOS:tag-map
SNMP-MANAGER/""
SS7-GATEWAY:transport-options:tos
VOIP/{ "" "" }:signaling-tos
VOIP/{ "" "" }:tos-options
VACM-ACCESS/{ "" "" v1 no+ }
VACM-SECURITY-GROUP/{ v1 "" }
VACM-VIEW-TREE/{ "" "" }
VROUTER/""
```

active-enabled

Description The active-enabled parameter has different uses, depending on the profile in which it is set:

- In an snmpv3-notification or snmpv3-target-param profile, active-enabled specifies whether the profile is used to generate notifications.
- In a trap profile, active-enabled specifies whether traps are sent to the host specified by the profile.
- In an snmpv3-usm-user or user profile, active-enabled 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 one of the following settings:

- 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/""
SNMPV3-TARGET-PARAM/"
SNMPV3-USM-USER/""
TRAP/""
USER/""

active-route

Description Specifies whether the TAOS unit adds a static route to the routing table.

Usage Specify one of the following settings:

- `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.

The default is `yes`, except for the `ip-route` profile called `default`. For the `default ip-route` profile, the default is `no`.

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/""
IPX-ROUTE/""

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 If `action` is set to `add`, `add-metric` does not apply.

Location FILTER/"":input-filters[*n*]:route-filter
FILTER/"":output-filters[*n*]:route-filter

add-persistence

Description Specifies the number of seconds that average line utilization (ALU) must persist beyond the `target-utilization` threshold before the TAOS unit adds bandwidth from available channels.

Usage Specify an integer from 1 through 300. The default is 5.

Example `set add-persistence = 15`

Dependencies Consider the following:

- When adding bandwidth, the unit adds the number of channels specified by `increment-channel-count`.
- When the `seconds-history` value is high, `add-persistence` has little effect.

Location `ANSWER-DEFAULTS:mpp-answer`
`CONNECTION/"":mpp-options`

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), 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/""`

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 through 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 obtains IP addresses from the first defined address pool.

Location `CONNECTION/"":ip-options`

advanced-agent-enabled

Description Indicates whether the Advanced management information base (MIB) is in use.

Usage The `advanced-agent-enabled` value is read-only and can have one of the following settings:

- `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`

advertise-policy

Description Specifies the `bgp-policy` profile that defines an advertisement policy.

Usage Specify a string of up to 15 characters. The default is null.

Example `set advertise-policy = one_network`

Location `BGP-PEER/""`

afi

Description Specifies the hexadecimal code that identifies the type of Asynchronous Transfer Mode (ATM) end system address (AESA) and the syntax of the rest of the address.

Usage The value 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/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address:aesa-address:idp-portion`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa-address:idp-portion`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa-address:idp-portion`

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 settings:

- `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 value, the new setting does not take effect until you restart the system.

Location `ATMP`

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 settings:

- `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 dedicated connection.
- `router-home-agent` specifies that the Home Agent routes tunneled data to the home network.

Example `set agent-type = router-home-agent`

Dependencies For `agent-type` to apply, you must set `agent-mode` to `home-agent`.

Location `ATMP`

aggregate

Description Enables or disables aggregation of the `bit-rate` values of multiple virtual circuits using this shaper.

Usage Specify one of the following settings:

- `yes` specifies that if *n* virtual circuits are using this shaper, the throughput of each virtual circuit is `bit-rate`/*n*.
- `no` (the default) specifies that aggregation is not used.

Example `set aggregate = yes`

Location DS3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[*n*]
OC3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[*n*]

aim-enabled

Description Indicates whether the unit enables Ascend Inverse Multiplexing (AIM).

Usage The aim-enabled value is read-only and can have one of the following settings:

- yes indicates that AIM is enabled.
- no indicates that AIM is not enabled.

Example aim-enabled = yes

Location BASE

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 value is read-only and can have one of the following settings:

- 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

DS3-ATM-STAT/{ any-shelf any-slot 0 }
E3-ATM-STAT/{ any-shelf any-slot 0 }
STM-PATH-STAT/{ any-shelf any-slot 0 }
STM-STAT/{ any-shelf any-slot 0 }
T1-STAT/{ any-shelf any-slot 0 }
T3-STAT/{ any-shelf any-slot 0 }
UDS3-STAT/{ any-shelf any-slot 0 }

alarm-enabled

Description Specifies whether the TAOS unit traps alarm events and sends a trap 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 one of the following settings:

- yes (the default) 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/""

alarm-temperature-trigger

Description Specifies a temperature threshold setting.

Usage Specify a number from 0 through 60 degrees 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 fan tray is lit.

Location THERMAL

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.

Usage Specify one of the following settings:

- `no-progress-indicator` (the default) disables alert reporting of call-routing events on the outbound switched telephone network.
- `none-end2end-isdn` specifies that the outbound MultiVoice® gateway reports when calls are connected to an outbound switched telephone network that does not use Integrated Services Digital Network (ISDN) signaling. The outbound switched telephone network can support robbed-bit or detectable dual-tone multifrequency (DTMF).
- `dest-non-isdn` specifies that the outbound MultiVoice® gateway reports when calls are connected to an outbound 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 incoming 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 outbound 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 outbound MultiVoice® gateway reports whether internetworking 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 outbound 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/{ "" "" }:pstn-attribute`

allow-as-client-dns-info

Description Specifies whether local Domain Name System (DNS) servers should be made accessible to Point-to-Point Protocol (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 one of the following settings:

- `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` (the default) 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/""`

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 one of the following settings:

- `yes` (the default) 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`

allow-client-dscp

Description Specifies whether clients are permitted to set their own values in the type of service (TOS) byte of the IP header.

Usage Specify one of the following settings:

- `no` (the default) specifies that clients are not permitted to set their own values in the TOS byte of the IP header. Any client-set TOS value is cleared to 0 (zero) and assigned a priority as defined in the quality of service (QOS) tag mappings for the differentiated services code point (DSCP) value of 0. By accepting the default value of `no`, you enable a security feature to prevent theft of service.
- `yes` specifies that values in the TOS byte of the IP header set by the client are honored by the system. Packets are assigned a priority as defined in the QOS tag map for the particular DSCP value.

Warning Be aware of the possible security consequences when turning this option on.

Example `set allow-client-dscp = yes`

Location `QOS`

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 PCMCIA flash memory card for use)
- `fsck` (to check the file system on a PCMCIA flash memory card)

Usage Specify one of the following settings:

- `yes` grants permission to upload code to the TAOS unit.
- `no` (the default) denies permission to upload code to the TAOS unit.

Example `set allow-code = yes`

Location `USER/""`

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 one of the following settings:

- `yes` (the default) 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/{ "" "" }`

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 slot card.
e1-stats	Report DS1-level line errors on E1 slot cards.
ether-display	Display the contents of received Ethernet packets.
fe-loop	Perform a line loopback for a T1 or E1 slot card.
idslcmd	Perform loopback and error tests on an IDSL slot card.
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 Primary Rate Interface (PRI) messages.
rlogin	Open an rlogin session.
slot	Administer a slot card.
t1-stats	Report DS1-level line errors on T1 and T3 slot cards.
telnet	Open a Telnet session.
traceroute	Display route statistics.
uptime	Report how long the system has been up and how long individual slot cards have been up.
xdslcmd	Activate a loopback test.

Usage Specify one of the following settings:

- yes grants permission to use diagnostic commands.
- no (the default) denies permission to use diagnostic commands.

Example `set allow-diagnostic = yes`

Location USER/""

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 one of the following settings:

- yes (the default) 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:

- For allow-g711-fallback to apply, you must set allow-coder-fallback to yes.
- 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/{ "" "" }

allow-nas-port-type-in-cli-user-auth

Description Specifies whether the NAS-Port-Type attribute is sent in Remote Authentication Dial-In User Service (RADIUS) Access Request packets for Telnet users.

Usage Specify one of the following values:

- yes (the default) specifies that the NAS-Port-Type attribute is sent in RADIUS Access Request packets for Telnet users.
- no stops the NAS-Port-Type attribute from being sent.

Example `set allow-nas-port-type-in-cli-user-auth = no`

Dependencies The allow-nas-port-type-in-cli-user-auth value applies only when the cli-user-auth parameter is not set to local-only.

Location EXTERNAL-AUTH:rad-auth-client

allow-password

Description Enables or disables permission to view passwords.

Usage Specify one of the following settings:

- yes grants permission to view passwords.
- no (the default) denies permission to view passwords.

Example `set allow-password = yes`

Location USER/""

allow-system

Description Enables or disables permission to use the following system commands:

Command	Description
arptable	Display or modify the TAOS unit's Address Resolution Protocol (ARP) table.
clr-hHistory	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 Internet Group Management Protocol (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.

Command	Description
version	Display software-version information.
view	Change the contents of a status window.

Usage Specify one of the following settings:

- yes grants permission to use system commands.
- no (the default) denies permission to use system commands.

Example `set allow-system = yes`

Location USER/""

allow-termserv

Description Enables or disables permission to use the terminal server and its commands.

Usage Specify one of the following settings:

- yes grants permission to use the terminal server and its commands.
- no (the default) denies permission to use the terminal server and its commands.

Example `set allow-termserv = yes`

Location USER/""

allow-unencrypted-tunnel-password

Description Specifies whether the unit accepts unencrypted tunnel passwords from Remote Authentication Dial-In User Service (RADIUS).

Usage Specify one of the following settings:

- yes specifies that the unit accepts unencrypted tunnel passwords from RAIUDS.
- no (the default) specifies that the unit does not accept unencrypted tunnel passwords from RADIUS.

Example `set allow-unencrypted-tunnel-password = yes`

Location EXTERNAL-AUTH:rad-auth-client

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 one of the following settings:

- yes grants permission to use update commands.
- no (the default) denies permission to use update commands.

Example `set allow-update = yes`

Location USER/""

always-compare-med

Description Specifies whether the unit compares the multiexit discriminators of routes received from different autonomous systems.

Usage Specify one of the following vales:

- yes specifies that the unit compares the multiexit discriminators of routes received from different autonomous systems.
- no (the default) specifies that the unit does not compare the multiexit discriminators of routes received from different autonomous systems.

Example `set always-compare-med = yes`

Location BGP-GLOBAL

always-next-hop

Description Specifies whether the unit uses the local IP address as the next hop in update packets.

Usage Specify one of the following settings:

- yes specifies that the unit uses the local IP address as the next hop in update packets.
- no (the default) specifies that the unit does not use the local IP address as the next hop in update packets.

Example `set always-next-hop = yes`

Location BGP-PEER/""

amdm

Description Indicates the action to take when the code image for an Analog Modem slot card is present in a `tar` file.

Usage The `amdm` value is read-only and can have one of the following settings:

- `auto` (the default) indicates that the system loads images for slot cards that are installed in the TAOS unit, and skips images for slot cards that are not installed.
- `load` indicates that the system loads the image, even if no slot card of that type is installed.
- `skip` indicates that the system skips the image, even if a slot card of that type is installed.

Dependencies A slot 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 slot 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 nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards that are no longer installed in the system.

Location `LOAD-SELECT`

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 settings:

- `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`

answer-delay

Description Specifies the number of milliseconds the TAOS unit waits before answering an incoming R2 call.

Usage Specify a number from 100 through 3000. The default is 200. Change the value if the TAOS unit answers calls too quickly.

Example `set answer-delay = 500`

Location `E1/{ any-shelf any-slot 0 }:line-interface`

answer-originate

Description Specifies whether the `connection` profile enables incoming calls, outgoing calls, or both.

Usage Specify one of the following settings:

- `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 dedicated call types.

Location `CONNECTION/"":telco-options`

apply-to

Description The `apply-to` parameter has different uses, depending on the subprofile in which it is set:

- In a `signaling-tos` subprofile, the `apply-to` parameter specifies how the type of service (TOS) value is applied to the signaling traffic flow and signaling packets over the IP network between the MultiVoice® Gateways.
- In a `tos` subprofile, the `apply-to` parameter specifies how the TOS value is applied to Signaling System 7 (SS7) signaling traffic.
- In a `tos-options` subprofile, the `apply-to` parameter specifies the direction in which TOS is enabled.

Usage Specify one of the following settings:

- `input` (the default) specifies that TOS bits are set in packets received on the interface.
- `output` specifies that TOS bits are set in outgoing packets only.
- `both` specifies that both incoming and outgoing packets are tagged.

Example `set apply-to = both`

Dependencies For the `apply-to` setting to apply, you must set `active` to `yes`.

Location `CONNECTION/"":ip-options:tos-options`
`SS7-GATEWAY:transport-options:tos`
`VOIP/{ "" "" }:signaling-tos`
`VOIP/{ "" "" }:tos-options`

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/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

area-type

Description Specifies the type of Open Shortest Path First (OSPF) area the connection or interface belongs to.

Usage Specify one of the following settings:

- `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 not-so-stubby area (NSSA).

Example `set area-type = normal`

Dependencies You must set `area-type` consistently on all OSPF routers within the area.

Location `CONNECTION/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

as-boundary-router

Description Specifies whether the TAOS unit performs autonomous system boundary router (ASBR) calculations.

Usage Specify one of the following settings:

- `yes` (the default) 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`

Dependencies 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.

Location `IP-GLOBAL: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 by means of this trap.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

ascend-link-down-trap-enabled

Description Specifies whether the TAOS unit generates an `ascendLinkDown` trap when a failure occurs in a communication link between the unit and the Simple Network Management Protocol (SNMP) manager.

Usage Specify one of the following settings:

- `yes` (the default) specifies that the TAOS unit generates an `ascendLinkDown` trap when a failure occurs in a communication link between the unit and the SNMP manager.
- `no` specifies that the TAOS unit does not generate an `ascendLinkDown` trap when a failure occurs in a communication link between the unit and the SNMP manager.

Example `set ascend-link-down-trap-enabled = no`

Dependencies You can set `ascend-link-down-trap-enabled` to `yes` only if `linkdown-enabled` is set to `yes`.

Location `TRAP/""`

ascend-link-up-trap-enabled

Description Specifies whether the TAOS unit generates an `ascendLinkUp` trap when the communication link between the unit and the Simple Network Management Protocol (SNMP) manager is reestablished.

Usage Specify one of the following settings:

- `yes` (the default) specifies that the TAOS unit generates an `ascendLinkUp` trap when the communication link between the unit and the SNMP manager is reestablished.
- `no` specifies that the TAOS unit does not generate an `ascendLinkUp` trap when the communication link between the unit and the SNMP manager is reestablished.

Example `set ascend-link-up-trap-enabled = no`

Dependencies You can set `ascend-link-up-trap-enabled` to `yes` only if `linkup-enabled` is set to `yes`.

Location `TRAP/""`

ase7-adv

Description *Not supported.*

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 (ABRs) can use it to filter a record.

Location `CONNECTION/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`
`IP-ROUTE/""`

ase-type

Description Specifies the Open Shortest Path First (OSPF) autonomous system external (ASE) type of the link state advertisement (LSA).

Usage Specify one of the following settings:

- Type-1 (the default) specifies a type 1 external metric. This metric is expressed in the same units as the link-state metric.
- Type-2 specifies a type 2 external metric. This metric is considered larger than any link-state path. Using a type 2 external metric assumes that routing between autonomous systems is the major cost of routing a packet. A type 2 metric eliminates the need for conversion of external costs to internal link-state metrics.

Example `set ase-type = type-1`

Location `CONNECTION/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`
`IP-ROUTE/""`

assign-address

Description Enables or disables dynamic IP address assignment for incoming calls.

Usage Specify one of the following settings:

- `yes` enables the TAOS unit to assign dynamic IP addresses to incoming calls.
- `no` (the default) 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`

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 Point-to-Point Protocol (PPP) software during negotiation of a connection.

Usage For each pool, specify a number from `0` through `65535`. The default is `0` (zero).

Example `set 3 = 254`

Dependencies Consider the following:

- 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/""`

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/"":tunnel-options`

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 one of the following settings:

- `yes` (the default) 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/"":hdlc-nrm-options`

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 = 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`

atm1483type

Description Specifies the type of (ATM) adaptation layer 5 (AAL 5) multiplexing for the connection.

Usage Specify one of the following settings:

- `aal5-llc` (the default) specifies AAL5 using Logical Link Control (LLC) encapsulation for routed protocols.
- `aal5-vc` specifies AAL 5 using multiplexing for virtual circuits.

Location `CONNECTION/"":atm-options`

atm-direct-enabled

Description Specifies whether Asynchronous Transfer Mode (ATM) direct is enabled.

Usage Specify one of the following settings:

- `yes` specifies that ATM direct is enabled.
- `no` (the default) specifies that ATM direct is disabled.

Example `set atm-direct-enabled = yes`

Location `CONNECTION/"":atm-options`

atm-direct-profile

Description Specifies the name of the `connection` profile to which Asynchronous Transfer Mode (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/"":atm-options`

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 settings:

- `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/"":tunnel-options`

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/{ { any-shelf any-slot 0 } 0 }:svc-options`

atmp-sap-reply

Description Enables or disables a Home Agent's ability to reply to the Mobile Client's Internetwork Packet Exchange (IPX) Nearest Server query if the Home Agent knows about a server on the home network.

Usage Specify one of the following settings:

- `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` (the default) means the TAOS unit does not respond to these queries from a Mobile Client.

Example `set atmp-sap-reply = yes`

Dependencies `atmp-sap-reply` is used only when the TAOS unit acts as a Home Agent.

Location `ATMP`

atmp-snmp-trap

Description Enables or disables the following Simple Network Management Protocol (SNMP) traps for Ascend Tunnel Management Protocol (ATMP):

- `atmpMaxTunnelExceeded` (27)—Generated when the number of tunnels to a home network exceeds the maximum value.
- `atmpAgentErrorSen` (28)—Generated when errors have occurred at the agent level or with tunnel creation and are sent to the peer agent.
- `atmpAgentErrorRecvTrap` (29)—Generated when errors are received from the peer agent.

Usage Specify one of the following settings:

- `yes` enables ATMP SNMP traps.
- `no` (the default) does not enable ATMP SNMP traps.

Example `set atmp-snmp-trap = yes`

Location `ATMP`

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/""`

auth-attribute-type

Description Specifies the attribute(s) used for session matching.

Usage Specify one of the following settings:

- `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 For `auth-attribute-type` to apply, you must set `rad-serv-enable` to `yes` and `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-server`

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`

Dependencies For `auth-boot-host` to apply, you must set `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

auth-boot-host-2

Note This setting is for a customer-specific application outside of the United States. It is not intended for general use.

Description Specifies the IP address of the secondary 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`

Dependencies For `auth-boot-host-2` to apply, you must set `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

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`

Dependencies For `auth-boot-port` to apply, you must set `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

auth-client

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. 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 Consider the following:

- For `auth-client` to apply, you must set `rad-serv-enable` to `yes` and `auth-type` to `radius`.
- If you do not use `auth-netmask` to supply a subnet mask, the system supplies a default subnet mask based on the address class.

Location `EXTERNAL-AUTH:rad-auth-server`

auth-cli-user-dnis

Description Specifies a pseudo-DNIS number for Telnet command-line interface users that need to be authenticated by the Remote Authentication Dial-In User Service (RADIUS) server.

Usage Specify an integer of up to 40 characters. If the value is not null, the number is sent to RADIUS in Access Request packets as the DNIS attribute `Called-Station-Id`. If the value of `auth-cli-user-dnis` is null, `Called-Station-Id` is not sent. Specifying a value for this parameter enables a unit to use the DNIS number as a proxy to send access requests to a RADIUS server that holds the Telnet user accounts.

Example `set auth-cli-user-dnis = 5051`

Dependencies The `auth-cli-user-dnis` value applies only when the `cli-user-auth` parameter is not set to `local-only`.

Location `EXTERNAL-AUTH:rad-auth-client`

authentication-enabled

Description Specifies whether the system generates a trap when an authentication failure occurs.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

authen-type

Description Specifies the type of authentication to use for validating Open Shortest Path First (OSPF) packet exchanges.

Usage Specify one of the following settings:

- `none` specifies that routing exchanges are not authenticated. The 64-bit authentication field in the OSPF header can contain data, but it is not examined on packet reception. When you use this setting, the 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.
- `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/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

auth-for-async-framed-users

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-users = not-required`

Dependencies Consider the following:

- If `auth-for-async-framed-users` 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-users` 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/"":ppp-options`

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 one of the following settings:

- `yes` enables the TAOS unit to send a second RADIUS accounting Start record when the RADIUS `Framed-Address` value is assigned.
- `no` (the default) prevents the TAOS unit from sending a second RADIUS accounting Start record when the RADIUS `Framed-Address` value is assigned.

Example `set auth-frm-adr-start = yes`

Dependencies For `auth-frm-adr-start` to apply, you must set `acct-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

auth-host-1
auth-host-2
auth-host-3

Description Specifies Domain Name System (DNS) hostnames or IP addresses of up to three Remote Authentication Dial-In User Service (RADIUS) authentication servers. 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 to connect to host #3.

Usage Specify a DNS hostname or an IP address in dotted decimal notation. The hostnames or addresses must all point to servers of the same type, as specified by the `auth-type` setting. The default is null, which indicates that no authentication server exists.

Example `set auth-host-1 = alameda`

Dependencies Consider the following:

- If `auth-type` does not specify RADIUS, `auth-host-1`, `auth-host-2`, and `auth-host-3` do not apply.
- You cannot configure an `auth-host-`*n* parameter and an `auth-server-`*n* parameter with the same index. For example, you cannot configure `auth-host-1` and `auth-server-1`. However, you can configure an `auth-host-`*n* parameter and an `auth-server-`*n* parameter with different indexes, such as `auth-host-1` and `auth-server-2`.

Location `EXTERNAL-AUTH: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 Integrated Services Digital Network (ISDN) Disconnect packets when calling line ID (CLID) or called-number authentication fails.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit returns `user busy` (decimal 17) when CLID or called-number authentication fails.
- `no` (the default) 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`

Dependencies For `auth-id-fail-return-busy` to apply, you must set `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

auth-id-max-retry-time

Description Specifies the maximum number of seconds the unit tries to contact a Remote Authentication Dial-In User Service (RADIUS) server for external authentication.

Usage Specify an integer from 0 through 10. The default is 0 (zero), which sets the unit to its internal default value.

Example `set auth-id-max-retry-time = 5`

Dependencies For `auth-id-max-retry-time`, the internal default depends on the following:

- The number of RADIUS authentication servers you have configured.
- The value of the `auth-timeout` parameter.

The internal default is calculated as 3 * (the number of configured RADIUS servers) * (the value of `auth-timeout`).

Location `EXTERNAL-AUTH:rad-auth-client`

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 Integrated Services Digital Network (ISDN) Disconnect packets when calling line ID (CLID) or called-number authentication times out.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit returns `user busy` (decimal 17) when CLID or called-number authentication times out.
- `no` (the default) 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`

Dependencies For `auth-id-timeout-return-busy` to apply, you must set `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

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 Consider the following:

- For `auth-keep-user-name` to apply, you must set `auth-type` to `radius`.
- 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`

auth-key

Description Specifies an authentication key that appears in Open Shortest Path First (OSPF), Simple Network Management Protocol version 3 user-based security model (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 SNMPv3 USM configurations, `auth-key` is an authentication key generated by the `snmpAuthPass` command.
- For Remote Authentication Dial-In User Service (RADIUS), the `auth-key` 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 The value you specify depends upon your configuration:

- For OSPF, specify a string of up to nine characters. The default is `ascend0`.
- For RADIUS, specify up to 22 characters. The default is null. For security purposes, the string is hidden when `auth-key` is displayed. If you specify a null value, the system logs the following warning:

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

- For most SNMPv3 USM configurations, do not set the string directly. Instead, use the `snmpAuthPass` command to generate the value. If you have permission to view passwords, the authentication key appears as a string with escape sequences for save and restore purposes. Otherwise, the authentication key appears as a row of asterisks. The default is null.

Example Suppose you use the snmpAuthPass command to generate the following 16-byte string for an SNMPv3 USM configuration:

```
27 0a dc 75 f8 98 e5 7c 4c 03 22 7d dd ac 0d ef
```

The system displays this value as the following auth-key value:

```
'\x0a\xdcu\xf8\x98\xe5|L\x03"}\xdd\xac\x0d\xef
```

Dependencies Consider the following:

- For OSPF routing, auth-key does not apply if authen-type is set to none.
- For auth-key to apply in a RADIUS configuration, you must set auth-type to radius.
- For SNMPv3 USM configurations, auth-key does not apply if auth-protocol is set to no-auth.
- You must generate the authentication key by means of the snmpAuthPass command before the snmpv3-usm-user profile can be used for communication with the SNMP manager.
- If you change the authentication protocol from 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.
- If you change the value of auth-key directly for SNMPv3 USM, keep in mind that the length of the escape sequence must be 10 (16D in hexadecimal) if 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.

Location CONNECTION/"":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/{ { any-shelf any-slot 0 } 0 }:ospf
SNMPV3-USM-USER/""

auth-netmask

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 For auth-netmask to apply, you must set rad-serv-enable to yes, set auth-type to radius, and specify an IP address for auth-client.

Location EXTERNAL-AUTH:rad-auth-server

auth-network-route-server

Description Specifies whether a TAOS unit adds the Framed-IP-Address attribute to a Remote Authentication Dial-In User Service (RADIUS) Access Request message or appends the destination IP address to the User-Name attribute.

Usage Specify one of the following settings:

- yes (the default) specifies that a TAOS unit adds the Framed-IP-Address attribute to a RADIUS Access Request message. This setting requires a nonstandard RADIUS server that can use the Framed-IP-address attribute to select a valid profile from multiple profiles with the same username.
- no specifies that a TAOS unit appends the destination IP address to the User-Name attribute in a RADIUS Access Request message. A standard RADIUS server uses the User-Name attribute and the destination IP address to reply with the appropriate profile.

Example `set auth-network-route-server = no`

Dependencies For auth-network-route-server to apply, you must set auth-type to radius.

Location EXTERNAL-AUTH:rad-auth-client

auth-pool

Description Enables or disables dynamic address assignment for RADIUS-authenticated IP-routing connections.

Usage Specify one of the following settings:

- yes enables the TAOS unit to assign dynamic IP addresses to RADIUS-authenticated IP-routing connections.
- no (the default) prevents dynamic address assignment for RADIUS-authenticated IP-routing connections.

Example `set auth-pool = no`

Dependencies Consider the following:

- Usage of the auth-pool parameter requires coordination with the RADIUS server. For details, see the *TAOS RADIUS Guide and Reference*.
- For auth-pool to apply, you must set auth-type to radius,
- The RADIUS server must be configured with at least one pool of addresses for assignment.

Location EXTERNAL-AUTH:rad-auth-client

auth-port

Description Specifies the User Datagram Protocol (UDP) port to use for communication with the external authentication server.

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. 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 accepting client requests. The default is `1700`.

Example `set auth-port = 1565`

Dependencies For `auth-port` to apply, you must set `auth-type` to `radius`, `tacacs`, or `tacacsplus`.

Location `EXTERNAL-AUTH:rad-auth-client`
`EXTERNAL-AUTH:rad-auth-server`
`EXTERNAL-AUTH:tac-auth-client`
`EXTERNAL-AUTH:tacplus-auth-client`

auth-protocol

Description Specifies whether or not the TAOS unit can authenticate Simple Network Management Protocol (SNMP) messages on behalf of the SNMP version 3 user-based security model (SNMPv3 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/""`

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 VSAs to the RADIUS server and does not recognize VSAs if the server sends them.
- `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. In addition, the unit uses the RFC-defined `User-Password` encryption algorithm. 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. In addition, the unit uses the RFC-defined `User-Password` encryption algorithm. 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.

Dependencies Consider the following:

- For `auth-radius-compat` to apply, you must set `auth-type` to `radius`,
- At this time, only NavisRadius™ supports 16-bit VSAs.

Example `set auth-radius-compat = vendor-specific`

Location `EXTERNAL-AUTH:rad-auth-client`

auth-realm-delimiters

Description Specifies the characters to be recognized as delimiters in a username. The delimiters are used to define realms in Remote Authentication Dial-In User Service (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 For `auth-realm-delimiters` to apply, you must set `auth-keep-user-name` to `keep-realm-name` and `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

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 Consider the following:

- For `auth-req-delim-count` to apply, you must set `auth-type` to `radius`.
- 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 Remote Authentication Dial-In User Service (RADIUS) `User-Name` attribute-value pair (AVP). 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`

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 (AVP).
- `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`

Dependencies For `auth-req-strip-side` to apply, you must set `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

auth-reset-time

Description Specifies the authentication time-out period in seconds, after which the TAOS unit returns to the primary Remote Authentication Dial-In User Service (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 a value for auth-host-1, auth-host-2, or auth-host-3, and you must set auth-type to radius.

Location EXTERNAL-AUTH: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`

Dependencies For auth-retries to apply, you must set auth-type to tacacsplus.

Location EXTERNAL-AUTH:tacplus-auth-client

auth-rsp-required

Description Specifies how the TAOS unit responds if an authentication request times out after a call has been calling line ID (CLID) authenticated.

Usage Specify one of the following settings:

- yes (the default) 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 form the external server.

Example `set auth-rsp-required = yes`

Dependencies For auth-rsp-required to apply, CLID authentication must be in use, clid-auth-mode must be set to required, and auth-type must be set to radius.

Location EXTERNAL-AUTH:rad-auth-client

auth-send67

Description Specifies whether the 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 Point-to-Point Protocol (PPP).

Usage Specify one of the following settings:

- yes specifies that if a user wants to initiate PPP, his or her RADIUS profile must include attributes 6 and 7.
- no (the default) 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`

Dependencies For auth-send67 to apply, you must set auth-type to radius.

Location EXTERNAL-AUTH:rad-auth-client

auth-server-1
auth-server-2
auth-server-3

Note These parameters have been replaced by the `auth-host-1`, `auth-host-2`, and `auth-host-3` parameters. The `auth-server-1`, `auth-server-2`, and `auth-server-3` parameters have been retained for compatibility with earlier TAOS versions.

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`

Dependencies For `auth-server-1`, `auth-server-2`, or `auth-server-3` to apply, you must set `auth-type` to `radius`, `tacacs`, or `tacacsplus`.

Location `EXTERNAL-AUTH:rad-auth-client`
`EXTERNAL-AUTH:tac-auth-client`
`EXTERNAL-AUTH:tacplus-auth-client`

auth-sess-interval

Description Specifies the number of seconds between Remote Authentication Dial-In User Service (RADIUS) authentication reports concerning the number of open sessions.

Usage Specify a number of seconds from `0` through `65535`. The default is `0` (zero), which turns off regular RADIUS open-session reports.

Example `set auth-sess-interval = 15`

Dependencies For `auth-sess-interval` to apply, you must set `auth-type` to `radius`.

Location `EXTERNAL-AUTH:rad-auth-client`

auth-session-key

Description Enables or disables session-key assignments.

Usage Specify one of the following settings:

- `yes` enables session-key assignments.
- `no` (the default) disables session-key assignments.

Example `set auth-session-key = no`

Dependencies For auth-session-key to apply, you must set auth-type to radius and rad-serv-enable to yes.

Location EXTERNAL-AUTH:rad-auth-server

auth-src-port

Description Identifies the User Datagram Protocol (UDP) source port to use for external authentication.

Usage Specify a value from 0 through 65535. The default is 0 (zero), which specifies that the source port is selected from the nonprivileged port range (1024–2000).

Example `set auth-src-port = 45`

Dependencies Consider the following:

- For auth-src-port to apply, you must set auth-type to radius, tacacs, or tacacsplus.
- 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

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 one of the following settings:

- yes (the default) 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`

Dependencies For auth-ts-secure to apply, you must set auth-type to radius and you must specify a value for the RADIUS Login-Service attribute. Login-Service defines the type of terminal-server connection to which auth-ts-secure applies.

Location EXTERNAL-AUTH: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-host-2`).

Usage Specify an integer from 1 through 60. The default is 1.

Example `set auth-timeout = 5`

Dependencies For `auth-timeout` to apply, you must set `auth-type` to `radius` or `tacacs`.

Location `EXTERNAL-AUTH:rad-auth-client`
`EXTERNAL-AUTH:tac-auth-client`

auth-timeout-time

Description Specifies the number of seconds that must elapse before the 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`

Dependencies For `auth-timeout-time` to apply, you must set `auth-type` to `tacacsplus`.

Location `EXTERNAL-AUTH:tacplus-auth-client`

auth-type

Description Specifies the type of external authentication server to access for incoming connections.

Usage Specify one of the following settings:

- `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.

Example `set auth-type = radius`

Dependencies If auth-type is set to a value other than none, you must specify at least one authentication server address.

Location EXTERNAL-AUTH

auto-logout

Description Specifies whether or not to log out of the current user profile and go back to default privileges upon loss of Data Transmit Ready (DTR) from the serial port.

Usage Specify one of the following settings:

- yes specifies that the TAOS unit automatically logs out of the current user profile if DTR is lost on the serial port.
- no (the default) specifies that the current user profile remains logged in.

Example `set auto-logout = yes`

Location SERIAL/{ any-shelf any-slot 0 }

auto-negotiate

Description Enables or disables negotiation by the LAN interface of its own operating speed and duplex mode.

Usage Specify one of the following settings:

- yes specifies that the interface determines the appropriate operating speed and duplex mode by using the autonegotiation protocol.
- no (the default) specifies that the duplex-mode and media-speed-mbit settings determine the operating speed and mode of the interface.

Example `set auto-negotiate = yes`

Location ETHERNET/{ any-shelf any-slot 0 }

autonomous-system

Description Specifies the local autonomous system number.

Usage Specify an integer from 1 through 65535. The default is 65534.

Example `set autonomous-system = 500`

Location BGP-GLOBAL
BGP-PEER/""

auto-telnet

Description Causes the terminal server to interpret an unknown command as the name of a host for a Telnet session.

Usage Specify one of the following settings:

- `yes` specifies that a user can omit the keyword `Telnet` and specify a hostname to initiate a Telnet session.
- `no` (the default) 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 For `auto-telnet` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration:telnet-options`

auto-update

Description Specifies whether the local Domain Name System (DNS) table is automatically updated by regular successful DNS queries.

Usage Specify one of the following settings:

- `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` (the default) 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`

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/"":mpp-options`

available-metric

Description Specifies a number 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` through `255`. The default is `1`.

Example `set available-metric = 5`

Location `TRANSACTION-SERVER`

B

back-to-back

Description Specifies whether the E1 line is connected back-to-back with another TAOS unit.

Usage Specify `true` or `false`. The default is `false`.

- `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/{ any-shelf any-slot 0 }`

backup

Description Specifies the name of a backup `connection` profile for a dedicated connection. The backup connection can be a switched Point-to-Point Protocol (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 dedicated interface specifies a backup interface, the routes to the dedicated interface never go down.
- Nested backups are not supported. (The profile for a backup interface cannot specify another backup interface.)
- The profile for a backup interface does not inherit attributes (such as filters) from the profile for the primary dedicated connection.

Location `CONNECTION/"":session-options`

bacp-enable

Description Enables or disables Bandwidth Allocation Control Protocol (BACP) for Multilink PPP (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/"":mp-options`

bandwidth-monitor-direction

Description Specifies the direction in which the TAOS unit monitors link utilization for Multilink Protocol Plus™ (MP+) calls.

Usage Specify one of the following settings:

- `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/"":mpp-options`

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 For `banner` to apply, you must enable terminal services.

Location `EXTERNAL-AUTH:password-profile`
`TERMINAL-SERVER:terminal-mode-configuration`

base-channel-count

Description Specifies the number of channels the TAOS unit uses when setting up a connection.

Usage Specify a number from 0 (zero) to the value of `maximum-channels`. The default is 1.

Example `set base-channel-count = 3`

Dependencies Consider the following:

- If the session uses Multilink PPP (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.
- If the `base-channel-count` value exceeds the `maximum-channels` value or falls below the `minimum-channels` value, an error results.

Location `CONNECTION/"":mp-options`

base-udp-port

Description For a Layer 2 Tunneling Protocol (L2TP) tunnel, specifies a User Datagram Protocol (UDP) port number or requires the system to select one dynamically.

Usage To specify a UDP port number, enter a value from 10000 through 60000. The default is 0 (zero), which specifies that the system dynamically selects a UDP port number.

Example `set base-udp-port = 200`

Location `L2-TUNNEL-GLOBAL:l2tp-config`

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`.

Usage Specify a text string. The default is null.

Example `set bay-id = 12ldj45`

Dependencies The TAOS unit does not interpret the value of `bay-id`. Interpretation on the signaling gateway is gateway dependent.

Location `SS7-GATEWAY`

bearer-capability

Description Specifies the request for a specific bearer service from the outbound switched circuit network for outbound Voice over IP (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 settings:

- `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/{ "" "" }:pstn-attribute`

bearer-type

Description Specifies the bearer type for the outgoing call.

Usage Specify one of the following values:

- `any` (the default) specifies any bearer type.
- `digital` specifies the digital bearer type.
- `analog` specifies the analog bearer type.

Example `set bearer-type = digital`

Location `TUNNEL-SERVER/"":dialout-options:default-call-mapping`

ber-receive

Description Indicates whether the bit-error rate (BER) threshold has been reached.

Usage The `ber-receive` value is read-only and can have one of the following settings:

- `True` indicates that the BER threshold has been reached.
- `False` indicates that the BERT threshold has not been reached.

Example `ber-receive = True`

Location `T1-STAT/{ any-shelf any-slot 0 }`

bi-directional-auth

Description Specifies whether Challenge Handshake Authentication Protocol (CHAP) authentication must be bidirectional.

Usage Specify one of the following settings:

- `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/"":ppp-options`

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 dedicated frame relay data-link 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/"":telco-options`
`FRAME-RELAY/""`

bit-rate

Description The `bit-rate` parameter has different uses, depending on the slot card to which it applies:

- For an E3-ATM slot card, `bit-rate` specifies the maximum sustainable effective bit rate (in Kbps) for transmitting traffic to the network.
- For a DS3-ATM or OC3-ATM slot card, `bit-rate` specifies the average bit rate (in Kbps).

Usage Specify an integer. Following are the valid ranges for each type of slot card:

- For a DS3-ATM slot card, the valid range is from 0 through 37920.
- For a E3-ATM slot card, the valid range is from 0 through 34368.
- For an OC3-ATM slot card, the valid range is from 0 through 135631.

For all slot cards, 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/{ any-shelf any-slot 0 }:line-config:traffic-shapers[`*n*`]`
`E3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[`*n*`]`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers[`*n*`]`

boot-file-path

Description Specifies the pathname of the directory containing Dynamic Host Configuration Protocol (DHCP) client configuration files on the Trivial File Transfer Protocol (TFTP) server.

Usage Specify a pathname. The default is null.

Example `set boot-file-path = /tftpboot/config`

Location `IP-GLOBAL:dhcp-server`

bootp-enabled

Description Specifies whether the TAOS unit uses BOOTP to get settings and check for a new software load.

Usage Specify one of the following settings:

- `yes` enables the TAOS unit to use BOOTP to get settings and check for a new software load.
- `no` (the default) disables the use of BOOTP to get settings and check for a new software load.

Example `set bootp-enabled = yes`

Location `IP-GLOBAL`

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 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`

boot-sr-version

Description Displays the version of the current `tntsrb.bin` 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 restart.

Example `boot-sr-version = 2.1`

Location `SYSTEM`

bottom-status

Description Specifies the default contents of the bottom-right portion of the status window.

Usage Specify one of the following settings:

- `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/""`

bpv-error-count

Description Indicates the number of bipolar violation (BPV) errors received. These errors can indicate any of the following:

- The line sent consecutive one bits with the same polarity.
- Three or more consecutive zeroes were sent.
- Line polarity is incorrect.

Usage The `bpv-error-count` value is read-only.

Example bpv-error-count = 3

Location DS3-ATM-STAT/{ any-shelf any-slot 0 }
E3-ATM-STAT/{ any-shelf any-slot 0 }
UDS3-STAT/{ any-shelf any-slot 0 }

bridging-enabled

Description *Not supported.*

bridging-group

Description *Not supported.*

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 one of the following settings:

- yes (the default) specifies that the TAOS unit buffers input characters for 100ms.
- no specifies that the TAOS unit processes each input character as you enter it.

Example **set buffer-chars = yes**

Dependencies For buffer-chars to apply, terminal services must be enabled.

Location TERMINAL-SERVER:terminal-mode-configuration

C

call-ack-decrement

Description Specifies a number by which to decrease a transaction server's metric if a Quick Transaction Protocol (QTP) connection attempt succeeds.

Usage Specify a number from 0 through 255. The default is 1.

Example **set call-ack-decrement = 5**

Location TRANSACTION-SERVER

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 one of the following settings:

- `yes` causes the TAOS unit to hang up on a dial-in connection and dial back the device specified in the profile.
- `no` (the default) specifies that the TAOS unit does not hang up and call back, but authenticates the connection as usual.

Example `set callback = yes`

Dependencies Consider the following:

- If you are using dedicated call types, or if `answer-originate` does not enable outgoing calls, `callback` does not apply.
- When you set `callback` to `yes`, you must also specify a value for `dial-number`.

Location `CONNECTION/"":telco-options`

callback-clid-prefix

Description Specifies the prefix to add to the dial number when callback is performed using the calling line ID (CLID).

Usage Specify a text string of up to 40 characters, composed of the following: `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, `9`, `0`, `(`, `)`, `[`, `]`, `!`, `z`, `-`, `*`, `#`, `,`, `.`, and `+`. The default is null.

Example `set callback-clid-prefix = 123`

Dependencies Be aware of the following caveats when using this feature:

- The callback type must be set to CLID or Dialed Number Information Service (DNIS), Ascend callback, or Callback Control Protocol (CBCP).
- Local or external authentication must be Point-to-Point Protocol (PPP), Multilink PPP (MP), or Multilink Protocol Plus™ (MP+).
- The system does not consider the trunk group number when it retrieves the CLID provided by the network. If the trunk-group feature is enabled for your system, you must include the trunk-group number in the value that you specify for the `callback-clid-prefix` parameter.
- You must verify that the concatenation of the number of characters specified for the `callback-clid-prefix` parameter and the CLID received from the network does not exceed the maximum number of 40 characters.

If the callback number exceeds the maximum length or the received CLID is null, the system generates the following log message:

```
LOG warning, Shelf 1, Controller, Time: 18:55:05--
Callback register failed, profile: TEST-2 [MBID 10]
```

If you use the `diag` command for callback diagnostics, the system displays the following output:

```
CALLBACK: _setPhoneNumber, invalid phone number length
CALLBACK: _setPhoneNumber, empty clid
```

Location `ANSWER-DEFAULTS`

callbackrequest-enable

Description *Not supported.*

call-by-call

Description The `call-by-call` parameter has different uses, depending on the profile in which it is found:

- In a `connection` profile, `call-by-call` specifies the call-by-call signaling value for T1 Primary Rate Interface (PRI) lines.
- In a `t1` profile, `call-by-call` specifies the call-by-call signaling value to set for routing calls from a local device through the TAOS unit to the network.

Usage Specify a number from `0` through `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/"":telco-options`
`T1/{ any-shelf any-slot 0 }:line-interface`

call-by-call-id

Description Specifies the T1 Primary Rate Interface (PRI) service to use when placing a call.

Usage Specify a number from `0` through `65535`, corresponding to the type of service in use. The default is `0`, which disables call-by-call ID service. The following 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 services are available if the service provider is Sprint:

- 0—Reserved
- 1—Private
- 2—Inwatts
- 3—Outwatts
- 4—FX
- 5—Tie Trunk

The following 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/""`

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/""`

called-number-type

Description Specifies the type of telephone number.

Usage Specify one of the following settings:

- `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 Consider the following:

- When the TAOS unit dials an outgoing call on a T1 Primary Rate Interface (PRI) line, the carrier uses the value of `called-number-type` in a `connection` profile to interpret the dialed telephone number.
- When you write a `connection` profile with `circuit-type` set to `svc`, the unit automatically sets `called-number-type` to `international`.
- `called-number-type` does not apply to dedicated connections.

Location `CONNECTION/""`
`FRAME-RELAY/""`

caller-id

Description Specifies whether the unit requests the calling line ID (CLID) from the switch.

Usage Specify one of the following settings:

- `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/{ any-shelf any-slot 0 }:line-interface`

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 restart 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 dedicated, or if the `filter-name` setting does not specify a call filter, `call-filter` does not apply.

Location `ANSWER-DEFAULTS:session-info`
`CONNECTION/"":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 one of the following settings:

- `yes` specifies that the TAOS unit connects calls by means of the PSTN if it cannot register with a MultiVoice® gatekeeper.
- `no` (the default) 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 slot card or on a second slot card.

Location `VOIP/{ "" "" }`

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 = ("cjones-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 Specify one of the following settings:

- `end-of-call` specifies that the TAOS unit reports the information to `syslog`.
- `none` (the default) specifies that the unit does not report the information to `syslog`.

Dependencies Use `call-info` only for diagnosing session problems. The reports to `syslog` rely on the User Datagram Protocol (UDP) protocol, which does not guarantee delivery. Therefore, you should not use `call-info` for billing purposes.

Location `LOG`

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 through 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 `call-inter-digit-timeout` applies to PIN entries and digits dialed after the telephone number has been entered.

Location `VOIP/{ "" "" }`

call-keep-alive-timeout

Description Specifies how often a MultiVoice® gateway polls a remote device during a Voice over IP (VoIP) call 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 through 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/{ "" "" }`

call-log-connection-packets-enable

Description Specifies that call-logging Start and Stop packets are sent when a connection is established or ended, in contrast to line statistics call logging, which is always enabled.

Usage Specify one of the following values:

- `yes` specifies that call-logging Start and Stop packets are sent when a connection is established or ended.
- `no` (the default) specifies that call-logging Start and Stop packets are not sent. To optimize operations, accept the default.

Example `set call-log-connection-packets-enable = yes`

Location `CALL-LOGGING`

call-log-csm-modem-diag

Description Specifies whether CSM modem diagnostics are sent in call-logging packets.

Usage Specify one of the following settings:

- `yes` specifies that CSM modem diagnostics are sent in call-logging packets.
- `no` (the default) specifies that CSM modem diagnostics are not sent in call-logging packets.

Example `set call-log-csm-modem-diag = yes`

Location `CALL-LOGGING`

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 one of the following settings:

- `yes` (the default) 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 Consider the following:

- For `call-log-dropped-pkt-enabled` to apply, you must set `call-log-enable` to `yes`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `TRAP/""`

call-log-enable

Description Enables or disables call logging.

Usage Specify one of the following settings:

- `yes` enables call logging.
- `no` (the default) 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` setting.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

call-log-host-1
call-log-host-2
call-log-host-3

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:

- For `call-log-host-1`, `call-log-host-2`, or `call-log-host-3` to apply, you must set `call-log-enable` to `yes`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

call-log-id-base

Description Specifies whether the TAOS unit presents a session ID to the call-log host in base 10 or base 16.

Usage Specify one of the following settings:

- `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:

- For `call-log-id-base` to apply, you must set `call-log-enable` to `yes`.
- 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`

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:

- For `call-log-key` to apply, you must set `call-log-enable` to `yes`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

call-log-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:

- For `call-log-limit-retry` to apply, you must set `call-log-enable` to `yes`.
- 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`

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 one of the following settings:

- `yes` specifies that multiple call-logging requests are sent in a single packet.
- `no` (the default) specifies that multiple call-logging requests are not sent in a single packet.

Example `set call-log-multi-packet = yes`

Dependencies Consider the following;

- For `call-log-multi-packet` to apply, you must set `call-log-enable` to `yes`.
- If you specify `yes` for `call-log-multi-packet`, you must set `call-log-radius-compat` to `16-bit-vendor-specific`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

call-log-port

Description Specifies the User Datagram Protocol (UDP) destination port to use for call-logging requests.

Usage Specify a UDP port number from 1 through `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:

- For `call-log-port` to apply, you must set `call-log-enable` to `yes`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

call-log-radius-compat

Description *Not supported.*

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.

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`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

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 one of the following settings:

- `yes` specifies that the unit generates a trap when the call-logging server changes.
- `no` (the default) specifies that the unit does not generate a trap when the call-logging server changes.

Example `set call-log-serv-change-enabled = yes`

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

Location `TRAP/""`

call-log-server-index

Description Specifies which call-logging 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:

- For `call-log-server-index` to apply, you must set `call-log-enable` to `yes`.
- 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`

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 one of the following settings:

- `yes` (the default) 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 Consider the following:

- For `call-log-stop-only` to apply, you must set `call-log-enable` to `yes`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

call-log-stream-period

Description Specifies the interval (in minutes) at which streaming call-logging packets are logged.

Usage Specify an integer from 2 through 15. The default is 2.

Example `set call-log-stream-period = 5`

Dependencies Consider the following:

- For `call-log-stream-period` to apply, `call-log-enable` must be set to `yes`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

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`. 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 through 10. The default is 0 (zero), which disables the timer.

Example `set call-log-timeout = 5`

Dependencies Consider the following:

- For `call-log-timeout` to apply, `call-log-enable` must be set to `yes`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

Location `CALL-LOGGING`

call-reject-increment

Description Specifies a number by which to increase a transaction server's current metric if a Quick Transaction Protocol (QTP) connection attempt fails.

Usage Specify a number from 0 through 255. The default is 4.

Example `set call-reject-increment = 10`

Location `TRANSACTION-SERVER`

call-route-empty-phone-number-acceptable

Description In the additional call-route database search related to call switching, specifies whether to include entries with a null `phone-number` setting.

Usage Specify one of the following values:

- `yes` specifies that a null `phone-number` setting in a `call-route` profile matches any dialed number. Depending on your `call-route` profile setup, specifying `yes` can result in a high number of matches.
- `no` (the default) specifies that the dialed number of a call must match an explicit `phone-number` value in a `call-route` profile.

Example `set call-route-empty-phone-number-acceptable = yes`

Location `CALL-SWITCHING:comparison-rule`

call-route-type

Description Specifies the type of call that the TAOS unit can route to a host device.

Usage For non-IP Device Control (IPDC) configurations, specify one of the following settings:

- `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 3.1Khz audio, to a host device.
- `digital-call-type` specifies that the TAOS unit can route general digital calls, including 3.1Khz audio bearer channel calls, to a host device. As far as the TAOS unit is concerned, 3.1Khz 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` 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. The `voip-call-type` setting allows routing of Voice over IP (VoIP) calls using the G.711 codec and transparent fax and modem calls ("G.711 fallback") to a device with this call route type.
- `phs-call-type` specifies Personal Handyphone System (PHS) 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 slot cards in the system.

When IPDC is the protocol in use, specify one of the following settings to route VoIP calls:

- `rtfax-call-type` specifies that VoIP calls using T.38 fax can be routed to a device with this call route type.
- `g729-call-type` specifies that VoIP calls using the G.729(A) codec can be routed to a device with this call route type.

- `g728-call-type` specifies that VoIP calls using the G.728 codec can be routed to a device with this call route type.
- `g723-call-type` specifies that VoIP calls using the G.723.1 codec can be routed to a device with this call route type.
- `frgsm-call-type` specifies that VoIP calls using the Full-Rate GSM codec can be routed to a device with this call route type.
- `rt24-call-type` specifies that VoIP calls using the RT-24 codec can be routed to a device with this call route type.

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 VoIP license has been enabled, the system creates a new `call-route` profile for each installed MultiDSP slot 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 slot card.
- The `rtfax-call-type` is not supported when the 288-port slot card is configured to use 480 ports.

Location `CALL-ROUTE/{ { { any-shelf any-slot 0 } 0 } 0 }`

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 or digital calls.

When the system restarts, 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 restart.

Usage Specify one of the following settings:

- `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`

Dependencies For DNIS routing to work, you must set `call-routing-sort-method` to `slot-first`.

Location `SYSTEM`

call-type

Description The `call-type` parameter has different uses, depending on the profile in which it is set:

- In the `telco-options` subprofile of a `connection` profile, the `call-type` setting specifies dedicated channel usage for a connection.
- In the `dnis` profile, the `call-type` setting specifies the call type to use for incoming inband, R1, and R2 calls.

Usage In the `telco-options` subprofile of a `connection` profile, specify one of the following settings:

- `off` (the default) specifies that the connection does not use any dedicated channels.
- `ft1` specifies that the connection uses only dedicated channels.
- `ft1-mpp` specifies that the TAOS unit might augment dedicated channels with switched channels for increased bandwidth during a Multilink Protocol Plus™ (MP+) call.
- `ft1-bo` specifies that a dedicated connection can use switched channels, both for additional bandwidth and for a backup method of reaching the site if the dedicated connection is down.

In a `dnis` profile, specifying one of the following settings:

- `digital` specifies incoming digital calls.
- `voice` specifies incoming voice calls.

Example `set call-type = ft1`

Dependencies If `nailed-groups` is set to 0 (zero), `call-type` does not apply.

Location `CONNECTION/"":telco-options`
`DNIS/""`

capadsl

Description *Not supported.*

carrier-established

Description Indicates whether error conditions exist on the T1 line.

Usage The `carrier-established` value is read-only and can have one of the following settings:

- `True` indicates that no error conditions exist.
- `False` indicates error conditions on the line.

Example `carrier-established = True`

Location `T1-STAT/{ any-shelf any-slot 0 }`

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 one of the following settings:

- `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` (the default) 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 `h323-voice-ann-enabled` is set to `yes`.

Location `VOIP/{ "" "" }:pstn-attribute`

cbcp-enabled

Description Specifies whether Callback Control Protocol (CBCP) callback is enabled.

Usage Specify one of the following settings:

- `yes` enables CBCP callback.
- `no` (the default) disables CBCP callback.

Example `set cbcp-enabled = yes`

Location `CONNECTION/"":ppp-options`

cell-level

Description Specifies the modem cellular-communications transmit and receive level.

Usage Specify one of the following settings:

- `-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 For `cell-level` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:modem-configuration`

cell-mode-first

Description Determines whether the TAOS unit attempts a cellular connection before a land-based connection.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit attempts a cellular connection first.
- `no` (the default) specifies that the TAOS unit attempts a land-based connection before attempting a cellular connection.

Example `set cell-mode-first = no`

Dependencies For `cell-mode-first` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:modem-configuration`

cell-payload-scramble

Description Enables or disables scrambling of the payload in transmitted cells.

Usage Specify one of the following settings:

- `yes` (the default) disables scrambling of the payload in transmitted cells.
- `no` enables scrambling of the payload in transmitted cells.

Example `set cell-payload-scramble = no`

Dependencies Set `cell-payload-scramble` to `yes` only if the receiving switch has disabled the corresponding descramble function.

Location `DS3-ATM/{ any-shelf any-slot 0 }:line-config`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`

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 from 1 through 24.

Usage Following is a sample listing of a `channel-state` array:

```
[in T1-STAT/{ shelf-1 slot-14 28 }:channel-state]
channel-state[1] = disabled
channel-state[2] = disabled
channel-state[3] = disabled
channel-state[4] = disabled
channel-state[5] = disabled
channel-state[6] = disabled
channel-state[7] = disabled
channel-state[8] = disabled
channel-state[9] = disabled
channel-state[10] = disabled
channel-state[11] = disabled
channel-state[12] = disabled
channel-state[13] = disabled
channel-state[14] = disabled
channel-state[15] = disabled
channel-state[16] = disabled
channel-state[17] = disabled
channel-state[18] = disabled
channel-state[19] = disabled
channel-state[20] = disabled
channel-state[21] = disabled
channel-state[22] = disabled
channel-state[23] = disabled
channel-state[24] = disabled
```

Dependencies The values in the `channel-state` array are read-only.

Location `T1-STAT/{ any-shelf any-slot 0 }`

channel-state *n*

Description Indicates the individual state of a channel in a T1 line. The index to each component is a channel number from 1 through 24.

Usage The channel-state *n* value is read-only and can have one of the following settings:

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 dedicated (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).

Example channel-state[1] = nailed-up

Location T1-STAT/{ any-shelf any-slot 0 }

channel-usage

Description Specifies the usage for a channel.

Usage For a T1 or E1 channel, specify one of the following settings:

- 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.
- d-channel specifies a channel used for Integrated Services Digital Network (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 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 = nailed-64-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 dedicated usage.

Location `E1/{ any-shelf any-slot 0 }:line-interface:channel-config[`*n*`]`
`T1/{ any-shelf any-slot 0 }:line-interface:channel-config[`*n*`]`

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 For `circuit-name` to apply, you must set `fr-direct-enabled` to `no`.

Location `CONNECTION/"":fr-options`

circuit-type

Description Specifies the type of virtual circuit in use.

Usage Specify one of the following settings:

- 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/"":fr-options`

cir-timer

Description Specifies the committed information rate (CIR) timer value, in milliseconds, that the unit uses to fine-tune the accuracy of the `rx-data-rate-limit` and `tx-data-rate-limit` values.

Usage Specify a value from 10 through 5000. The default is 5000.

Example `set cir-timer = 500`

Location `CONNECTION/"":session-options`

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 settings:

- `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`

cl1-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 1 has been exceeded.

Usage Specify a number from 0 through 1000. The default is 60.

Example `set cl1-level = 100`

Location `SS7-GATEWAY:congestion-control`

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 settings:

- `reject-new-call` (the default) specifies that the TAOS unit rejects new calls and sends a Request Test Echo (RTE) message to the signaling gateway with the appropriate congestion level indicator.
- `send-info-to-mgc` specifies that the TAOS unit sends a congestion indicator to the media gateway controller.
- `ignore` specifies that no action is taken.

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 an RTE message without a congestion indicator.

Location `SS7-GATEWAY:congestion-control`

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 through 1000. The default is 120.

Example `set cl2-level = 100`

Location `SS7-GATEWAY:congestion-control`

clear-call

Description Specifies whether the TAOS unit clears a dial-in connection when an interactive Telnet, `rlogin`, or TCP session terminates.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit clears a dial-in connection when an interactive Telnet, `rlogin`, or TCP session terminates.
- `no` (the default) 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 For `clear-call` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration`

clear-screen

Description Specifies whether the TAOS unit clears the screen when a terminal-server session begins.

Usage Specify one of the following settings:

- `yes` (the default) 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 For `clear-screen` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration`

clid

Description The `clid` parameter has different uses, depending on your configuration:

- For an Integrated Services Digital Network (ISDN) call, `clid` specifies the telephone number of the remote station.
- For a frame relay link, `clid` specifies the E.164 address of the local end of the switched virtual circuit (SVC).
- In the `password-profile` subprofile, `clid` specifies the calling line ID (CLID) specified as the password in a Remote Authentication Dial-In User Service (RADIUS) profile.

Usage The value you can enter for `clid` depends upon your configuration:

- For the calling party's telephone number in an ISDN call, you can enter up to 24 characters. The default is null.
- For the E.164 subaddress in a frame relay configuration, you can enter up to 15 digits. The default is null.
- For the CLID value specified as the password in a RADIUS profile, you can specify up to 21 characters. The default is `Ascend-CLID`.

Example `set clid = 510-555-1213`

Dependencies Consider the following:

- For CLID callback, you must specify a value for `clid`.
- 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/""`
`EXTERNAL-AUTH:password-profile`

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 settings:

- `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.

- `dnis-fallback` specifies that the TAOS unit requires DNIS on the line and uses RADIUS to authenticate the call. However, if the RADIUS server does not respond, the TAOS unit performs password authentication instead of dropping 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`.

If the `clid-auth-mode` parameter is set to `dnis-fallback`, the TAOS unit takes a given action when it encounters one of the following situations:

Situation	Action
No DNIS is received on the line.	The TAOS unit drops the call.
RADIUS authentication fails.	The TAOS unit drops the call.
RADIUS authentication passes.	The TAOS unit proceeds with call setup.
RADIUS authentication times out.	The TAOS unit proceeds with call setup.

Location `ANSWER-DEFAULTS`

clid-selection

Description Specifies which calling line ID (CLID) to use for an incoming call.

Usage Specify one of the following settings:

- `first` (the default) specifies that the TAOS unit uses the first CLID provided by the public switched telephone network (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`

Dependencies A CLID provided by the 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.

Location `ANSWER-DEFAULTS`

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 one of the following settings:

- `yes` specifies that the local TAOS unit blocks transmission of the CLID received from the remote TAOS unit.
- `no` (the default) 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/{ "" "" }`

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/"":tunnel-options`
`TUNNEL-SERVER/""`

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/"":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 one of the following settings:

- `yes` specifies that the TAOS unit makes the client DNS server addresses available to the connection.
- `no` (the default) specifies that TAOS unit makes the client DNS server addresses unavailable.

Example `set client-dns-addr-assign = no`

Location `CONNECTION/"":ip-options`

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 Point-to-Point Protocol (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 For `client-dns-primary-addr` to apply, you must set `client-dns-addr-assign` to `yes`.

Location `CONNECTION/"":ip-options`

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 For `client-dns-secondary-addr` to apply, you must set `client-dns-addr-assign` to `yes`.

Location `CONNECTION/"":ip-options`

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 Point-to-Point Protocol (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/""`

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 Point-to-Point Protocol (PPP) connections, and a connection-specific configuration. The `client-secondary-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/""`

client-wins-addr-assign

Description Specifies whether the TAOS unit presents client Windows Internet Name Service (WINS) server addresses to the dial-in client while negotiating the session.

Usage Specify one of the following settings:

- `yes` (the default) 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 following two conditions must be met:

- The PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings.
- A WINS server must be specified by the `client-wins-primary-addr` setting.

As an option, you can also specify a backup WINS server by setting the `client-wins-secondary-addr` value.

Location `CONNECTION/"":ip-options`

client-wins-primary-addr

Description Specifies the IP address of the primary Windows Internet Name Service (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. The default is `0.0.0.0`.

Example `set client-wins-primary-addr = 10.1.1.1`

Dependencies For the client WINS feature to work, the following two conditions must be met:

- The PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings.
- `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/"":ip-options`

client-wins-secondary-addr

Description Specifies the IP address of the secondary Windows Internet Name Service (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. The default is `0.0.0.0`.

Example `set client-wins-secondary-addr = 20.1.1.1`

Dependencies For the client WINS feature to work, the following two conditions must be met:

- The PC dialing in must have Dynamic Host Configuration Protocol (DHCP) for WINS enabled in its Network settings.
- `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/"":ip-options`

cli-user-auth

Description Specifies whether the TAOS unit authenticates a command-line-interface user by means of local profiles or an external authentication server, and if the authentication is to be in any specific order.

Usage Specify one of the following settings:

- `local-then-external` (default) specifies that the TAOS unit uses local `user` profiles for the first authentication attempt. If that attempt fails, the unit attempts authentication through an external server, if an external authentication server exists.
- `local-only` specifies that the TAOS unit uses only local `user` profiles.
- `external-only` specifies that the TAOS unit uses only an external authentication server and ignores local `user` profiles.
- `external-then-local` specifies that the TAOS unit authenticates by means of an external authentication server. If authentication fails or times out, the unit uses local `user` profiles to make another attempt.
- `external-then-local-if-timeout` specifies that the TAOS unit authenticates by means of an external authentication server. If authentication times out, the unit uses local `user` profiles to make another attempt.

Example `set cli-user-auth = local-only`

Location `EXTERNAL-AUTH`

clock-mode

Description Specifies whether the Serial WAN (SWAN) slot card generates an internal clock.

Usage Specify one of the following settings:

- `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/{ any-shelf any-slot 0 }:line-config:clocking`

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. When 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.

Usage Specify one of the following settings:

- `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.

Example `set clock-priority = middle-priority`

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config`
`T1/{ any-shelf any-slot 0 }: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 settings:

- `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/{ any-shelf any-slot 0 }:line-interface`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config`
`T1/{ any-shelf any-slot 0 }:line-interface`

cluster-id

Description Identifies this TAOS unit as a Border Gateway Protocol (BGP) route reflector in a cluster of internal peers.

Usage Specify an IP address on this TAOS unit. Specifying the default of `0.0.0.0`, removes the cluster ID.

Example `set cluster-id = 1.2.3.4`

Dependencies You must set the same cluster ID on each route reflector in a cluster, but cluster IDs are not set on the reflector clients in the cluster.

Location `BGP-GLOBAL`

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 one of the following settings:

- `yes` (the default) 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/""`

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 one of the following settings:

- `yes` specifies that the DSP decodes the DTMF digits.
- `no` (the default) specifies that the DSP does not decode the DTMF digits.

Example `set collect-incoming-digits = yes`

Dependencies For `collect-incoming-digits` to apply, you must set `signaling-mode` to `inband`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

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/{ "" "" }:rt-fax-options`

community-name

Description Specifies the Simple Network Management Protocol (SNMP) community name associated with SNMP traps. 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/""`

comp-neq

Description Specifies the type of comparison to make between a packet's contents and the filter's `value` setting.

Usage Specify one of the following settings:

- `yes` specifies that the comparison succeeds when the values are not equal.
- `no` (the default) specifies that the comparison succeeds when the values are equal.

Example `set comp-neq = no`

Dependencies For `comp-neq` to apply, you must set `type` to `generic-filter`.

Location `FILTER/"":input-filters[`*n*`]:gen-filter`
`FILTER/"":output-filters[`*n*`]:gen-filter`

confederation-member

Description Specifies whether a peer is a member of a Border Gateway Protocol (BGP) confederation.

Usage Specify one of the following settings:

- `yes` specifies that the peer is a member of a BGP confederation.
- `no` (the default) specifies that the peer is not a member of a BGP confederation.

Example `set confederation-member = yes`

Location `BGP-PEER/""`

config-change-enabled

Description Specifies whether the unit generates a trap whenever the system configuration is modified or a new software version is loaded. This 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 one of the following settings:

- `yes` (the default) 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/""`

congested-metric

Description Specifies a number to use as a transaction server's current metric when the server sends a Quick Transaction Protocol (QTP) status message with a flow control attribute set to `congested`.

Usage Specify a number from `0` through `255`. The default is `10`.

Example `set congested-metric = 15`

Location `TRANSACTION-SERVER`

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`

connect-retry-interval

Description Specifies the number of seconds during which this TAOS unit attempts to open sessions to Border Gateway Protocol (BGP) peers that are not fully established.

Usage Specify a number of seconds in the range from `30` through `1000`. The default is `120`.

Example `set connect-retry-interval = 180`

Dependencies Changing the value of `connect-retry-interval` does not cause BGP to restart.

Location `BGP-GLOBAL`

conn-route-redist-policy

Description Specifies the policy containing the routes for which the TAOS unit automatically creates Border Gateway Protocol (BGP) summarizations.

Usage Specify a single policy name or the keyword `all` . The `all` value specifies that the unit automatically creates BGP summarizations for all connected routes. The default is null.

Example `set conn-route-redist-policy = all`

Location `BGP-GLOBAL`

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 one of the following settings:

- `yes` (the default) 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/""`

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`

context-prefix

Description Specifies a prefix for a given context.

Usage Specify a string. The default is null.

Example `set context-prefix = abc`

Dependencies The `match-method` value determines whether the context name is matched exactly or whether the prefix alone is used.

Location `VACM-ACCESS/{"" "" v1 none }:access-properties`

control-connect-establish-timer

Description Specifies the maximum number of seconds during which the TAOS unit can 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 0 through 600. The default is 60.

Example `set control-connect-establish-timer = 60`

Dependencies For `control-connect-establish-timer` to apply, you must set `l2tp-mode` to `lac`.

Location `L2-TUNNEL-GLOBAL:l2tp-config`

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 Access SS7 Gateway Control 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 IP Device Control (IPDC) support for SS7 gateways. It specifies XCOM/Level 3 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 nonvolatile RAM (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 restart the unit.
- Although the control protocol is configurable in real time, you must restart the TAOS unit to begin using the new protocol. After the unit is restarted, 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`

cost

Description The `cost` parameter has different uses, depending on the configuration:

- For an Open Shortest Path First (OSPF) configuration, `cost` specifies the cost of an OSPF link. The lower the cost, the more likely OSPF will use the interface to forward data traffic.
- For call routing, the unit uses the `cost` value to determine the sort order of the call route database. Routes with a lower value appear earlier in the database. As the system traverses the database searching for a best-match terminating resource for an incoming call, it finds those with the least `cost` value first.

Usage The value you can enter for `cost` depends upon your configuration:

- For an OSPF configuration, specify a number from `1` through `16777214`. The default is `1` on the Ethernet interface, or `10` on a WAN link. With the exception of links to stub networks, the output cost must always be nonzero. A link with a cost of `0xFFFFFF` (`16777215`) is considered nonoperational.
- For call routing, specify a number from `0` through `65535`.

Example `set cost = 50`

Dependencies Consider the following:

- 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 autonomous system.
- With priority-based call routing, the `cost` value in a call route overrides the sort method specified by the `call-routing-sort-method` and `digital-call-routing-sort-method` parameters in the `system` profile. For example, with the default `item-first` sort method, if you assign a cost of 0 to a Hybrid Access card in slot 1 and a cost of 10 to a Hybrid Access card in slot 2, the system will always attempt to use the devices in slot 1 first. In addition, load balancing occurs among slot cards with equal costs, even if the slot cards are not the same type.
- The system assigns default values for each type of call supported by a slot card. Currently, the default settings for the `cost` parameter result in efficient device resource usage, and are probably sufficient for most sites. However, priority-based call routing is configurable and can be used to set a specific slot sort order for different `call-route-type` values. Different call types can be sorted independently on the basis of how the `cost` values are set. The following table shows the defaults created for Hybrid Access, Series56, and MultiDSP slot cards:

Host slot card	Type of call	Default cost of call route
Hybrid Access	`digital-call-type`	`cost = 0`
Series56	`digital-call-type`	`cost = 10`
	`voice-call-type`	`cost = 0`
MultiDSP	`digital-call-type`	`cost = 20`
	`voice-call-type`	`cost = 10`
	`phs-call-type`	`cost = 0`
	`voip-call-type`	`cost = 0`
	`v110-call-type`	`cost = 0`

Location `CALL-ROUTE/{ { { any-shelf any-slot 0 } 0 } 0 }`
`CONNECTION/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`
`IP-ROUTE/""`

countries-enabled

Description Contains a bit set identifying the enabled countries.

Usage The `countries-enabled` value is read-only.

Example `countries-enabled = 0`

Location `BASE`

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 settings 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 `323-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`

cp-bit-error-count

Description For C-bit parity lines, indicates the number of parity errors occurring since the last restart.

Usage The `cp-bit-error-count` value is read-only.

Example `cp-bit-error-count = 3`

Location `DS3-ATM-STAT/{ any-shelf any-slot 0 }`
`E3-ATM-STAT/{ any-shelf any-slot 0 }`
`UDS3-STAT/{ any-shelf any-slot 0 }`

crc-threshold

Description Specifies the threshold value of cyclic redundancy check (CRC) errors per second.

Usage For an E1 system, specify a number from `0` through `1000`. For a T1 system, specify a number from `0` through `300`. For each system, the default is `0` (zero), which specifies that the system does not consider CRC errors when determining whether to switch to a new clock source.

Example `set crc-threshold = 30`

Location `DS1-CLOCK-ERROR`

csm-modem-diag

Description Specifies whether central site modem (CSM) diagnostics are enabled.

Usage Specify one of the following settings:

- `yes` specifies that CSM diagnostics are enabled.
- `no` (the default) specifies that CSM diagnostics are disabled.

Example `set csm-modem-diag = yes`

Location `SNMP`

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 settings:

- 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/{ any-shelf any-slot 0 }:line-interface

current-state

Description Indicates the current operational state of the slot.

Usage The current-state value is read-only and can have one of the following settings:

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.
oper-state-post	The slot is running a self-test.
oper-state-none	The slot is empty.

Location SLOT-STATE { any-shelf any-slot 0 }

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-Primary Rate Interface (PRI) trunks.

Usage Specify one of the following settings:

- `yes` (the default) 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/{ "" "" }`

D

data

Description *Not supported*.

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 through 30000. The default is 10000.

Example `set data-ack-timeout = 5000`

Location `TRANSACTION-SERVER`

data-call-enabled

Description Indicates whether the TAOS unit supports data calls over Integrated Services Digital Network (ISDN) lines.

Usage The `data-call-enabled` value is read-only and can have one of the following settings:

- `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`

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/"":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`

data-pkt-udp-cksum

Description Enables or disables the TAOS unit from performing a User Datagram Protocol (UDP) checksum on transmitted Layer 2 Tunneling Protocol (L2TP) data packets.

Usage Specify one of the following settings:

- `yes` (the default) specifies that the system performs a UDP checksum on transmitted L2TP data packets.
- `no` specifies that the system does not perform a UDP checksum on *transmitted* L2TP data packets. When you specify `no` and the system receives an L2TP data packet with a nonzero UDP checksum field, the unit performs a UDP checksum on the received packet.

Dependencies For `data-pkt-udp-cksum` to apply, you must set `udp-cksum` to `yes`.

Location `L2-TUNNEL-GLOBAL:l2tp-config`

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 settings:

- `normal` (the default) specifies noninverted data.
- `inv` specifies inverted data.

Example `set data-sense = normal`

Location `T1/{ any-shelf any-slot 0 }:line-interface`

data-service

Description For a switched connection, specifies the type of service requested of the switch. For a dedicated 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 56Kbps of the bandwidth of the data channel.

Setting	Specifies
`64k-restricted`	The call should be set up as a data call at a rate of 64Kbps on an AMI-encoded line on which the sender transmits only non-zero data. Use this setting with Link Access Procedure on the D channel (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 384Kbps.
`dws-384-clear` (switched calls only)	A 384-Kbps call coded as Multi-Rate, not H0.
`1536k-clear` (switched calls only)	The call should be set up as a data call that connects to the Switched-1536 data service at 1536Kbps. Non-facility associated signaling (NFAS) is required for the Switched-1536 data service. (Because all 24 channels of the T1 Primary Rate Interface (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.

Setting	Specifies
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 slot 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/"":telco-options`
`TUNNEL-SERVER/"":dialout-options:default-call-mapping`

day

Description Specifies a day in the month.

Usage Specify a number from 1 through 31.

Example `set day = 6`

Location `TIMEDATE:date`

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 through 10. The value you specify must be less than `dceN393-val`. The default is 3.

Example `set dceN392-val = 7`

Dependencies For `dceN392-val`to apply, you must set `link-type` is set to `dce`.

Location `FRAME-RELAY/""`

dceN393-val

Description Specifies the DCE-monitored event count.

Usage Specify a value from 1 through 10. The value you specify must be greater than dceN392-val. The default is 4.

Example `set dceN393-val = 8`

Dependencies For dceN393-valto apply, you must set link-type is set to dce.

Location FRAME-RELAY/""

d-channel-enabled

Description Indicates whether the unit enables D-channel signaling.

Usage The d-channel-enabled value is read-only and can have one of the following settings:

- yes indicates that the unit supports D-channel signaling.
- no indicates that the unit does not support D-channel signaling.

Location BASE

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 through 65535. The default is 40 for a connected route, and 120 for a WAN connection.

Example `set dead-interval = 40`

Location CONNECTION/"":ip-options:ospf-options
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf

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 through 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/"":mpp-options

default-call-type

Description Specifies a default call type for calls on non-Integrated Services Digital Network (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 settings:

- `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.
- `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 Consider the following:

- For the `voip` setting to apply, you must set `voip-enabled` 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/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }: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`

default-gateway-metric

Description Specifies the metric to use when injecting this peer as a gateway to the default route.

Usage Specify an integer from 0 through 15. The default is `0` (zero), which specifies that no default route is created. You must assign a value to the default routes of different peers to specify a preferred default gateway. When multiple peers are configured with `default-gateway-metric`, the one with the lowest metric is the preferred router for default-route forwarding.

Example `set default-gateway-metric = 7`

Location `BGP-PEER/""`

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`

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`

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`

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`

default-status

Description Specifies whether or not the TAOS unit displays the status screen by default when the user logs in.

Usage Specify one of the following settings:

- yes specifies that the TAOS unit displays the status screen when it authenticates the profile.
- no (the default) 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/""

default-tunnel-server

Description Specified the name of the default tunnel-server profile.

Usage Specify a text string. The default is null.

Example `set default-tunnel-server = myserver`

Dependencies The specified profile must be used only for dial-out. The system uses the profile you specify if no tunnel-server profile matching the Layer 2 Tunneling Protocol (L2TP) network server (LNS) name has been defined.

Location L2-TUNNEL-GLOBAL:l2tp-config

delay

Description Specifies the number of seconds the TAOS unit waits for Point-to-Point Protocol (PPP) packets before it changes to terminal-server mode on an incoming modem or V.120 call.

Usage Specify an integer from 1 through 60. The default is 5.

Example set delay = 15

Dependencies Consider the following:

- For delay to apply, terminal services must be enabled.
- 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.

Location TERMINAL-SERVER: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 through 60. The unit treats values of 0 through 3 as 3 seconds. The default is 0 (zero).

Example `set delay-callback = 5`

Dependencies For `delay-callback` to apply, you must set `callback` to `yes`.

Location `CONNECTION/"":telco-options`

desired-state

Description Specifies the desired administrative state of a device.

Usage Specify one of the following settings:

- `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 Consider the following:

- 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.
- You can change the administrative state of a device by using the Simple Network Management Protocol (SNMP) `set` commands, or the TAOS unit's `slot -d` and `slot -u` commands.

Example `set desired-state = admin-state-up`

Location `ADMIN-STATE-PERM-IF/""`
`ADMIN-STATE-PHYS-IF/{ any-shelf any-slot 0 }`

desired-trap-state

Description Indicates the desired up/down enable state of the interface.

Usage The desired-trap-state value is read-only and can have one of the following settings:

- `trap-state-enabled` indicates that an operator has specified that `linkUp` and `linkDown` traps should be generated for the interface.
- `trap-state-disabled` indicates that an operator has specified that `linkUp` and `linkDown` traps should not be generated for the interface.

Example `desired-trap-state = trap-state-enabled`

Location `ADMIN-STATE-PERM-IF/""`
`ADMIN-STATE-PHYS-IF/{ any-shelf any-slot 0 }`

dest-address

Description Specifies a destination IP address.

Usage Specify an IP address. The default is 0.0.0.0.

Example `set dest-address = 10.2.3.4`

Dependencies Consider the following:

- In a `filter` profile, `dest-address` applies only if `type` is set to `ip-filter` or `tos-filter`.
- In a `filter` profile, the TAOS unit compares `dest-address` to a packet's destination address after applying the `dest-address-mask` value.
- In an `ip-route` profile or a `route-description-list` 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.

Location `FILTER/"":input-filters[n]:ip-filter`
`FILTER/"":output-filters[n]:ip-filter`
`FILTER/"":input-filters[n]:tos-filter`
`FILTER/"":output-filters[n]:tos-filter`
`IP-ROUTE/""`
`PRIVATE-ROUTE-TABLE/"":route-description-list`

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/"":input-filters[n]:ip-filter`
`FILTER/"":output-filters[n]:ip-filter`
`FILTER/"":input-filters[n]:tos-filter`
`FILTER/"":output-filters[n]:tos-filter`

dest-net-address

Description Specifies an Internetwork Packet Exchange (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 For dest-net-address to apply, you must set type to ipx-filter.

Location FILTER/"":input-filters[*n*]:ipx-filter
FILTER/"":output-filters[*n*]:ipx-filter

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 Internetwork Packet Exchange (IPX) network number by the network administrator.

Example `set dest-network = 00000001`

Location IPX-ROUTE/""

dest-node-address

Description Specifies an Internetwork Packet Exchange (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 For dest-node-address to apply, you must set type is set to ipx-filter.

Location FILTER/"":input-filters[*n*]:ipx-filter
FILTER/"":output-filters[*n*]:ipx-filter

dest-port

Description Specifies a value to compare with a packet's destination-port field.

Usage Specify a number from 0 through 65535. The default is 0 (zero), which matches any port. Port 25 is reserved for Simple Mail Transfer Protocol (SMTP), and is dedicated to receiving mail messages. Port 20 is reserved for File Transfer Protocol (FTP) data messages, port 21 for FTP control sessions, and port 23 for Telnet.

Example `set dest-port = 25`

Dependencies Consider the following:

- For dest-port to apply, you must set type to ip-filter or tos-filter.
- Only Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets contain destination-port fields.
- The dst-port-cmp setting specifies the type of comparison the TAOS unit makes.

Location FILTER/"":input-filters[*n*]:ip-filter
FILTER/"":output-filters[*n*]:ip-filter
FILTER/"":input-filters[*n*]:tos-filter
FILTER/"":output-filters[*n*]:tos-filter

dest-socket

Description Specifies an Internetwork Packet Exchange (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 For dest-socket to apply, you must set type to ipx-filter.

Location FILTER/"":input-filters[*n*]:ipx-filter
FILTER/"":output-filters[*n*]:ipx-filter

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 one of the following settings:

- 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 time-out specified by flush-time, or until the data reaches the maximum packet length specified by flush-length, whichever occurs first.
- no (the default) 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 CONNECTION/"":tcp-clear-options

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 indicate `modem`, `hdlc`, or `unknown`.

Example `device-class = modem`

Location `DEVICE-SUMMARY`

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`

device-state

Description Indicates the current operational state of a device.

Usage The `device-state` value is read-only and can have one of the following settings:

- `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/{ { any-shelf any-slot 0} 0}`

dialed-number

Description Specifies the number dialed for the incoming call.

Usage Specify a telephone number of up to 40 characters. The default is null.

Example **`set dialed-number = 555-1212`**

Location `DNIS`

dial-number

Description Specifies the 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/""`

dial-number-lookup

Description Specifies whether the unit uses the dial number passed by the Layer 2 Tunneling Protocol (L2TP) network server (LNS) to look up a `connection` profile.

Usage Specify one of the following settings:

- `yes` specifies that the unit uses the dial number to look up a `connection` profile.
- `no` (the default) specifies that the unit does not use the dial number to look up a `connection` profile.

Example `set dial-number-lookup = yes`

Location `TUNNEL-SERVER/"":dialout-options`

dial-number-prefix

Description Specifies a text string to be prepended to the dial-out number to provide a locally required prefix (such as a trunk number).

Usage Specify a text string of up to 23 characters. The default is null.

Example `set dial-number-prefix = 3`

Location `TUNNEL-SERVER/"":dialout-options`

dialout-allowed

Description Specifies whether the connection can use the TAOS unit's digital modems to dial out.

Usage Specify one of the following settings:

- `yes` specifies that the user can dial out on digital modems.
- `no` (the default) specifies that the user cannot dial out on digital modems.

Example `set dialout-allowed = yes`

Location `CONNECTION/"":telco-options`

dialout-auth-lns

Description Specifies whether a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) must accept dial-out requests from an L2TP network server (LNS) on authenticated tunnels only.

Usage Specify one of the following values:

- `yes` specifies that a LAC must accept dial-out requests on authentication tunnels only.
- `no` (the default) specifies that a LAC can accept dial-out requests on any tunnels.

Example `set dialout-auth-lns = yes`

Location `L2-TUNNEL-GLOBAL:l2tp-config`

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 one of the following settings:

- `yes` specifies that the TAOS unit stops advertising its IP dial-out routes if no trunks are available.
- `no` (the default) 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 do not use dial-out routes.

Example `set dialout-poison = no`

Location `IP-GLOBAL`

dialout-send-profile-name

Description Specifies whether the Layer 2 Tunneling Protocol (L2TP) network server (LNS) sends to the L2TP access concentrator (LAC) the name of the `connection` profile that initiated the dial-out. The LAC uses the profile to dial the call.

Usage Specify one of the following values:

- `yes` specifies that the LNS sends the name of the `connection` profile that initiated the dial-out.
- `no` (the default) specifies that the LNS does not send the name of the `connection` profile that initiated the dial-out.

Example `set dialout-send-profile-name = yes`

Dependencies For the `yes` setting to have any effect, the LAC must be a TAOS unit.

Location `L2-TUNNEL-GLOBAL:l2tp-config`

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 one of the following settings:

- `yes` specifies that the TAOS unit brings up a connection.
- `no` (the default) 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 Internetwork Packet Exchange (IPX) route for even one remote server, it brings up that connection instead.
- For `dial-query` to apply, the TAOS unit must route IPX for the connection or have IPX routing globally enabled.

Location `CONNECTION/"":ipx-options`

digital-call-routing-sort-method

Description *Not supported*.

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 one of the following settings:

- `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/""`

direct

Description Specifies whether Point-to-Point Protocol (PPP) negotiation is initiated immediately after an interactive user enters the PPP command in the terminal-server interface.

Usage Specify one of the following settings:

- `yes` enables direct PPP negotiation.
- `no` (the default) specifies that the terminal server waits to receive a PPP packet before beginning PPP negotiation.

Example `set direct = no`

Dependencies For `direct` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:ppp-mode-configuration`

direct-access

Description Enables or disables the direct-access dial-out feature.

Usage Specify one of the following settings:

- `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` (the default) 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`

directed-broadcast-allowed

Description Specifies whether the TAOS unit forwards directed broadcast traffic onto the interface and its network.

Usage Specify one of the following settings:

- `yes` (the default) 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/{ { any-shelf any-slot 0 } 0 }`

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

disconnect-on-auth-timeout

Description Instructs the TAOS unit to disconnect a Point-to-Point Protocol (PPP) connection if it times out while waiting for Remote Authentication Dial-In User Service (RADIUS) authentication.

Usage Specify one of the following settings:

- yes causes the TAOS unit to hang up a PPP connection upon a RADIUS time-out.
- no (the default) causes the TAOS unit to shut down cleanly after a RADIUS time-out.

Example **set disconnect-on-auth-timeout = yes**

Location ANSWER-DEFAULTS:ppp-answer

divider

Description Specifies the number by which the 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 through 256. The default is 1.

Example **set divider = 5**

Dependencies If clock-mode is set to external-clock, divider does not apply.

Location SWAN/{ any-shelf any-slot 0 }:line-config:clocking

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 through 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:

- For `dlci` to apply, `fr-direct-enabled` must be set to `no`.
- The T1 FrameLine slot card supports a maximum of 240 active DLCIs.
- The Serial WAN (SWAN) slot 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 a switched virtual circuit (SVC), the DLCI value is assigned to the circuit by the network. The range of DLCI values for circuits is shared between permanent virtual circuits (PVCs) and SVCs, and is managed between the network and user entities.

Location `CONNECTION/"":fr-options`

dmtadsl

Description *Not supported.*

dnis

Description Specifies the Dialed Number Information Service (DNIS) value specified as the password in a Remote Authentication Dial-In User Service (RADIUS) profile.

Usage Specify up to 21 characters. The default is `Ascend-DNIS`.

Example `set dnis = my_dnis`

Location `EXTERNAL-AUTH:password-profile`

dns-auto-update-interval

Description Specifies the time interval (in seconds) between successive updates of permanent entries in the Domain Name System (DNS) cache.

Usage Specify a value from 300 through 65535. The default is 300.

Example `set dns-auto-update-interval = 600`

Dependencies For `dns-auto-update-interval` to apply, you must set `dns-cache-enabled to yes`.

Location `IP-GLOBAL/""`

dns-cache-enable

Description Enables or disables Domain Name System (DNS) caching.

Usage Specify one of the following settings:

- `yes` (the default) specifies that DNS caching is enabled.
- `no` specifies that DNS caching is disabled. This value does not apply if there are permanent entries in the DNS cache.

Example `set dns-cache-enable = no`

Location `IP-GLOBAL/""`

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 one of the following settings:

- `yes` specifies that the TAOS unit returns the number of addresses it finds for the host, up to the limit specified by `dnis-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 `dnis-list-size`.
- `no` (the default) 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 `set dns-list-attempt = yes`

Dependencies Consider the following:

- If Telnet and immediate Telnet are both disabled, `dns-list-attempt` does not apply.
- A TAOS unit operating as a Layer 2 Tunneling Protocol (L2TP) network server (LNS) can use the 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`

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 through 35. The default is 6.

Example `set dns-list-size = 10`

Location IP-GLOBAL

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/""

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/""

dns-server-query-type

Description Specifies how to query a Domain Name System (DNS) server.

Usage Specify one of the following settings:

- `udp` (the default) specifies that the unit queries the DNS server first by means of User Datagram Protocol (UDP), and then, if the TC-bit is set and a retry is necessary, by means of Transmission Control Protocol (TCP).
- `udp-ignore-tc-bit` specifies that the unit queries the DNS server only by means of UDP.
- `tcp` specifies that the unit queries the DNS server only by means of TCP.
- `tcp-keep-open` specifies that the unit queries the DNS server by means of TCP only and then attempts to keep the TCP session established, rather than opening a new TCP session for each additional query.

Example `set dns-server-query-type = tcp`

Location `IP-GLOBAL`

domain-name

Description Specifies the 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/""`

down-cost

Description Specifies the cost to be applied to the interface when it is unavailable.

Usage Specify an integer from `1` through `1677215`. In an `ospf` subprofile, the default is `1677215`. In an `ospf-options` subprofile, the default is `1000`.

Example `set down-cost = 20`

Location `CONNECTION/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

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 through 214748364. The lower the preference, the more likely the TAOS unit will bring the route online.

Example `set down-preference = 255`

Location `CONNECTION/"":ip-options`

down-trans-delay

Description Specifies the transition delay time, in tenths (0.1) of a second, during which the unit keeps a T1 line connected after detecting a loss of carrier on the line.

Usage Specify a number from 25 (the default) through 250.

Example `down-trans-delay = 100`

Location `T1/{ any-shelf any-slot 0 }:line-interface`

dr-capable

Description Specifies whether the neighboring router can be the designated router.

Usage Specify one of the following settings:

- `yes` specifies that the neighboring router can be the designated router.
- `no` (the default) specifies that the neighboring router cannot be the designated router.

Example `set dr-capable = yes`

Location `OSPF-NBMA-NEIGHBOR/""`

drop-source-routed-ip-packets

Description Specifies whether the TAOS unit forwards IP packets with the source-route option set.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit drops all packets that have a Loose or a Strict source route among their IP options.
- `no` (the default) 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`

ds2-state

Description An array listing the state of each DS2 line in a DS3 line.

Usage The index to each array component is an integer from 1 through 7. The `ds2-state` value is read-only and can have one of the following settings:

- `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.

Example `ds2-state[1] = idle`

Location `T3-STAT/{ any-shelf any-slot 0 }`

ds3-atm

Description Specifies the action to take when the code image for a DS3-ATM slot card is present in a `tar` file.

Usage The `ds3-atm` value is read-only and can have one of the following settings:

- `auto` (the default) indicates that the system loads images for slot cards that are installed in the TAOS unit, and skips images for slot cards that are not installed.
- `load` indicates that the system loads the image, even if no slot card of that type is installed.
- `skip` indicates that the system skips the image, even if a slot card of that type is installed.

Example `ds3-atm = skip`

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

dscp

Description Specifies the differentiated services code point (DSCP) value.

Usage Specify a value from 00 through 3F (hexadecimal). DSCP marking, as defined in RFC 2474, uses the first six bits in the second octet in the IP datagram to create values (from 00 through 3F) specifying different classes of service:

Bit positions	TOS-precedence (RFC 791) indication	DSCP (RFC 2474) indication
0-2	Precedence (8 levels of priority)	DSCP value
3	Delay (normal or low)	DSCP value (continued)
4	Throughput (normal or high)	DSCP value (continued)
5	Reliability (normal or high)	DSCP value (continued)
6-7	Reserved	Reserved

Example `set dscp = 3F`

Dependencies Consider the following:

- For `dscp` to apply, you must set `marking-type` to `dscp`.
- When the `marking-type` parameter is set in the `voip` profile, the DSCP is set in H.323 signaling packets.
- When the `marking-type` parameter is set in the `ss7-gateway` profile, the DSCP is set in Signaling System 7 (SS7) signaling packets.
- The full byte (that is, 8 bits) of the DSCP field can be specified and will be set in the IP type of service (TOS) byte of the IP header. Even though only the most significant 6 bits are used and matched to select a per-hop behavior (PHB) by the differentiated services (DS) domains in the network, the system is flexible so that you can set the entire 8 bits in any desired way and experiment with the two unused bits.

Location `CONNECTION/"":ip-options:tos-options`
`FILTER/"":input-filters[`*n*`]:tos-filter`
`SS7-GATEWAY:transport-options:tos`
`QOS:tag-map`
`VOIP/{ "" "" }:signaling-tos`
`VOIP/{ "" "" }:tos-options`

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 settings:

- `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 Consider the following:

- For `dest-port-cmp` to apply, you must set `type` to `ip-filter` or `tos-filter`.
- Only Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets contain destination ports.

Location `FILTER/"":input-filters[`*n*`]:ip-filter`
`FILTER/"":output-filters[`*n*`]:ip-filter`
`FILTER/"":input-filters[`*n*`]:tos-filter`
`FILTER/"":output-filters[`*n*`]:tos-filter`

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 settings:

- `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/"":input-filters[`*n*`]:ipx-filter`
`FILTER/"":output-filters[`*n*`]:ipx-filter`

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 settings:

- 1-133 (the default)
- 134-266
- 267-399
- 400-533
- 534-655

Example `set dsx-line-length = 134-266`

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/{ any-shelf any-slot 0 }: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 settings:

- `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 User Datagram Protocol (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.
- `rfc2833` specifies that DTMF tones are transferred and passed via another channel to the decoding Digital Signal Processor (DSP), according to the RFC2833 standard. This setting is available when the `packet-audio-mode` parameter has been set to use the G.711 or G.729(A) codec.

Example `set dtmf-tone-passing = outofband`

Dependencies Changes to `dtmf-tone-passing` are effective with the next Voice over IP (VoIP) call.

Location `VOIP/{ "" "" }`

duplex-mode

Description Specifies whether the physical Ethernet interface of the 100BaseT port on the Ethernet-2 slot 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-duplex`

Dependencies When the unit uses the Ethernet-2 slot card to support Voice over IP (VoIP) call processing, the slot card must operate in full-duplex mode.

Location `ETHERNET/{ any-shelf any-slot 0 }`

duration

Description Specifies the length of time that connections will be maintained.

Usage Specify a value from `0` through `2147483647`, indicating the number of milliseconds that the call can be held, pending the restoration of the digital line, before being dropped. The default is `0` (zero).

Example `set duration = 60`

Location `SS7-GATEWAY:resilience-options`

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 settings:

- `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/"":mpp-options`

E

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/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr`

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 through 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 is especially important for Voice over IP (VoIP) calls with `single-stage-dial`.

Example `set e1-inter-digit-timeout = 2000`

Dependencies For `e1-inter-digit-timeout` to apply, you must set `collect-incoming-digits` to `yes`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`

early-queue-discard

Description Specifies whether the unit filters and discards Simple Network Management Protocol (SNMP) requests from unauthorized hosts before they enter the SNMP queue at User Datagram Protocol (UDP) port 161.

Usage Specify one of the following values:

- `yes` specifies that the unit filters and discards SNMP requests from unauthorized hosts before they enter the SNMP queue at UDP port 161.
- `no` (the default) specifies that the unit queues all incoming SNMP requests, and later discards those from unauthorized hosts.

Example `set early-queue-discard = yes`

Dependencies If you set `early-queue-discard` to `yes`, you must also set `enforce-address-security` to `yes`.

Location `SNMP`

early-ringback-enable

Description Enables or disables generation of an early ringback tone on networks experiencing long call setup times.

Usage Specify one of the following settings:

- `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` (the default) 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/{ "" "" }`

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 one of the following settings:

- `yes` (the default) 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/{ "" "" }:rt-fax-options`

ena-adap-jitter-buffer

Description Specifies whether the jitter buffer mode is adaptive for Voice over IP (VoIP) calls.

Usage Specify one of the following settings:

- `yes` (the default) 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/{ "" "" }`

enable

Description The `enable` parameter has different uses, depending on the profile in which it is set:

- In the `bgp-global` profile, `enable` globally enables or disables Border Gateway Protocol (BGP) operation.
- In a `bgp-peer` profile, `enable` activates or deactivates a BGP peer relationship.
- In a `bgp-summarization` profile, `enable` activates or deactivates BGP summarization.
- In the `ospf-global` subprofile, `enable` globally enables or disables Open Shortest Path First (OSPF) operation.

Usage Specify one of the following settings:

- `yes` (the default) globally enables OSPF or BGP, or enables a BGP peer relationship or BGP summarization.
- `no` globally disables OSPF or BGP, or disables a BGP peer relationship or BGP summarization.

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 `BGP-GLOBAL`
`BGP-PEER/""`
`BGP-SUMMARIZATION/{ 0.0.0.0/0 }`
`IP-GLOBAL:ospf-global`

enabled

Description Enables or disables a feature, interface, or line.

Usage In all profiles except the sntp-info subprofile, 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.

In the sntp-info subprofile, specify one of the following settings:

- sntp-enabled specifies that the time is updated at each request to a server no matter what the time offset between the Simple Network Time Protocol (SNTP) server and the TAOS unit.
- sntp-passive specifies that an update occurs only when the update-threshold value has been reached.
- sntp-disabled specifies that no updates occur.

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 to 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

```
ANSWER-DEFAULTS:fr-answer
ANSWER-DEFAULTS:priority-answer
ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }
CALL-SWITCHING
CONNECTION/""
CONNECTION/"":priority-options
DS1-CLOCK-ERROR
DS3-ATM/{ any-shelf any-slot 0 }
E1/{ any-shelf any-slot 0 }
E3-ATM/{ any-shelf any-slot 0 }
ETHERNET/{ any-shelf any-slot 0 }
FRAME-RELAY/""
IP-GLOBAL
IP-GLOBAL:mbone-backup
OC3-ATM/{ any-shelf any-slot 0 }
```

```
PRIVATE-ROUTE-TABLE/"":route-description-list
QOS
SNMP
SS7-GATEWAY
STACKING
STM-PATH/{ any-shelf any-slot 0 }
SWAN/{ any-shelf any-slot 0 }
T1/{ any-shelf any-slot 0 }
T3/{ any-shelf any-slot 0 }
TERMINAL-SERVER
TRANSACTION-SERVER
TUNNEL-SERVER/""
TUNNEL-SERVER/"":dialout-options
```

enable-vacm

Description Enables or disables the view-based access control model (VACM).

Usage Specify `yes` or `no`.

- `yes` specifies that each object in each incoming Get, Set, GetNext, and GetBulk request, and each object in the `sysTrapOID` of each outgoing trap, is verified for VACM access.
- `no` (the default) disables VACM, enabling access to all objects in the system. However, security based on Simple Network Management Protocol Version 1 (SNMPv1) community strings and the SNMP version 3 user-based security model (SNMPv3 USM) is still used to determine access.

Example `set enable-vacm = yes`

Location `SNMP`

encapsulation-protocol

Description Specifies the encapsulation method to use for 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 settings:

- `ppp` (Point-to-Point Protocol) for single-channel 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.
- `slip` for an asynchronous Serial Line Internet Protocol (SLIP) connection.

- `cslip` for a Compressed SLIP connection that uses Van Jacobson header compression.
- `atm` for an Asynchronous Transfer Mode (ATM) connection.
- `atm-frame-relay-circuit` for an ATM-to-frame relay link.
- `hdlc-nrmfor` 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` specifies that IP-over-ATM is used on the virtual circuit.

Location `CONNECTION/""`

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 settings:

- `ami` (the default) specifies alternate mark inversion (AMI) encoding.
- `b8zs` specifies bipolar encoding with 8-zero substitution (B8ZS). B8ZS is often required for Integrated Services Digital Network (ISDN) lines.
- `none` specifies encoding identical to AMI, but without density enforcement.

Example `set encoding = b8zs`

Location `T1/{ any-shelf any-slot 0 }:line-interface`

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 Transmission Control Protocol (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 For `end-of-packet-pattern` to apply, you must set `detect-end-of-packet` to `yes`.

Location `CONNECTION/"":tcp-clear-options`

enet2

Description Specifies the action to take when the code image for an Ethernet-2 slot card is present in a `tar` file.

Usage The `enet2` value is read-only and can have one of the following settings:

- `auto` (the default) indicates that the system loads images for slot cards that are installed in the TAOS unit, and skips images for slot cards that are not installed.
- `load` indicates that the system loads the image, even if no slot card of that type is installed.
- `skip` indicates that the system skips the image, even if a slot card of that type is installed.

Example `enet2 = skip`

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

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 one of the following settings:

- `yes` specifies that, before allowing access, the TAOS unit validates the source IP address of an SNMP manager.
- `no` (the default) specifies that the TAOS unit does not validate IP addresses, but uses only the community name to validate SNMP access.

Example `set enforce-address-security = yes`

Location `SNMP`

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/{ { { any-shelf any-slot 0 } 0 } 0 }`

error-count

Description Indicates the number of errors experienced, since the last restart, by a T1 line.

Usage The `error-count` value is read-only.

Example `error-count[1] = 0`

Location `T1-STAT/{ any-shelf any-slot 0 }`

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). The `esi` value 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/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address:aesa-address:dsp-portion`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa-address:dsp-portion`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa-address:dsp-portion`

ether-if-type

Description Indicates the type of physical Ethernet interface in use.

Usage The `ether-if-type` value is read-only and can have one of the following settings:

- `utp` indicates unshielded twisted pair 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/{ any-shelf any-slot 0 }`

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`

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 one of the following settings:

- `yes` (the default) 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/""`

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 one of the following settings:

- `yes` specifies that the TAOS unit drops calls for which it has no explicit call-routing information.
- `no` (the default) 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`

exp

Description Specifies the exponent used to calculate the internal clock speed on a Serial WAN (SWAN) line.

Usage Specify a value from `0` through `9`. The default is `2`.

Example `set exp = 5`

Dependencies If `clock-mode` is set to `external-clock`, `exp` does not apply.

Location `SWAN/{ any-shelf any-slot 0 }:line-config:clocking`

expect-callback

Description Specifies whether the TAOS unit expects outgoing calls to result in a call back from the remote device.

Usage Specify one of the following settings:

- `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` (the default) specifies that the TAOS unit does not expect callback.

Example `set expect-callback = yes`

Location `CONNECTION/"":telco-options`

F

f1-bit-state

Description Indicates the current state of the F1 bit for the virtual tributary.

Usage The `f1-bit-state` setting is read-only and can have the value 0 or 1. A change in the value of this parameter indicates that the Peripheral Control Timing Facilities Interface (PCTFI) driver will read bits F2, F3, and F4.

Example `f1-bit-state = 1`

Location `PCTFI-STAT/{ any-shelf any-slot 0 }:virtual-ds1-line-status`

f4-bit-state

Description Indicates the signaling mode of the trunk.

Usage The `f4-bit-state` setting is read-only and can have one of the following values:

- `cas` indicates channel-associated signaling (CAS).
- `non-cas` indicates channeling types other than CAS, such as T1 Primary Rate Interface (PRI) signaling.

Example `f4-bit-state = 1`

Location `PCTFI-STAT/{ any-shelf any-slot 0 }:virtual-ds1-line-status`

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 settings:

- local0 (the default)
- local1
- local2
- local3
- local4
- local5
- local6
- local7

Example `set facility = local2`

Dependencies Consider the following:

- For facility to apply, you must enable syslog.
- 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 each auxiliary-syslog subprofile affect an individual syslog stream, and override the values specified in the log profile.

Location LOG
LOG:auxiliary-syslog

fantray-lownoise-rpm

Description Specifies the speed in revolutions per minute (RPM) of the fan tray when the low noise speed has been selected.

Usage Specify a number from 2000 through 3000. The default is 2500.

Example `set fantray-lownoise-rpm = 2000`

Location THERMAL

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/{ "" "" }:voip-index`

fast-path-enabled

Description Specifies whether the frame relay link is used to carry incoming voice packets.

Usage Specify one of the following values:

- `yes` specifies that the frame relay link carries incoming voice packets.
- `no` (the default) specifies that the frame relay link does not carry incoming voice packets.

Example `set fast-path-enabled = yes`

Location `FRAME-RELAY`

faststart-enable

Description Enables or disables the fast-connect procedure.

Usage Specify one of the following settings:

- `yes` (the default) enables the fast-connect procedure.
- `no` disables the fast-connect procedure.

Example `set faststart-enable = no`

Location `VOIP/{ "" "" }`

f-bit-error-count

Description Specifies the number of framing bit errors received since the last restart.

Usage The `f-bit-error-count` value is read-only.

Example `f-bit-error-count = 3`

Location `DS3-ATM-STAT/{ any-shelf any-slot 0 }`
`E3-ATM-STAT/{ any-shelf any-slot 0 }`
`UDS3-STAT/{ any-shelf any-slot 0 }`

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 settings:

- `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 (superframe format) and extended superframe format (ESF) performance statistics in the FDL Stats windows.

Location `T1/{ any-shelf any-slot 0 }:line-interface`

feb-error-count

Description Indicates the number of far-end block errors received since the last restart.

Usage The `feb-error-count` value is read-only.

Example `feb-error-count = 3`

Location `DS3-ATM-STAT/{ any-shelf any-slot 0 }`
`E3-ATM-STAT/{ any-shelf any-slot 0 }`
`UDS3-STAT/{ any-shelf any-slot 0 }`

febe-threshold

Description Specifies the threshold value of far end block errors (FEBEs) per second.

Usage Specify a number from `0` through `1000`. The default is `0` (zero), which specifies that the system does not consider FEBEs when determining whether to switch to a new clock source.

Example `set febe-threshold = 30`

Location `DS1-CLOCK-ERROR`

fer-threshold

Description Specifies the threshold value of framing errors per second.

Usage For an E1 system, specify a number from 0 through 127. For a T1 system, specify a number from 0 through 30. For each system, the default is 0 (zero), which specifies that the system does not consider framing errors when determining whether to switch to a new clock source.

Example `set fer-threshold = 30`

Location DS1-CLOCK-ERROR

fgd-signaling-enabled

Description Indicates whether Feature Group D (FGD) signaling is enabled on a MultiVoice® gateway.

Usage The `fgd-signaling-enabled` value is read-only and can have one of the following settings:

- `yes` indicates that FGD signaling is enabled.
- `no` indicates that FGD signaling is disabled.

Example `fgd-signaling-enabled = yes`

Location BASE

filter-name

Description Specifies the name of a `filter` profile. The filter-name value can appear in a `filter` profile or an `ethernet` 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 36 characters. The default is null.

Example `set filter-name = ip-spoof`

Location ETHERNET/{ any-shelf any-slot 0 }
FILTER/""

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 one of the following settings:

- `yes` specifies that filters persist across state changes.
- `no` (the default) specifies that filters do not persist across state changes.

Example `set filter-persistence = yes`

Location ANSWER-DEFAULTS:session-info
CONNECTION/"":session-options

filter-required

Description Specifies whether 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 one of the following settings:

- `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` (the default) 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/"":session-options`

finger

Description Specifies whether the TAOS unit accepts Finger queries and returns active session details to a remote client.

Usage Specify one of the following settings:

- `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` (the default) 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

firewalls-enabled

Description *Not supported.*

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/"":visa2-options

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 through 5000. The default is 1000.

Example `set first-retry-timer = 1000`

Dependencies For `first-retry-timer` to apply, you must set `l2tp-mode` to `lac`.

Location L2-TUNNEL-GLOBAL:l2tp-config

fixed-packets

Description Enables or disables the pre-TAOS-9.0 fax packet scheme for real-time fax processing.

Usage Specify one of the following settings:

- `yes` (the default) enables the pre-TAOS-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-TAOS-9.0 fax packet scheme. Jitter buffering and packet redundancy for real-time fax processing are enabled.

Example `set fixed-packets = no`

Dependencies When you set fixed-packets to yes, the packet-redundancy setting does not apply.

Location VOIP/{ "" "" }:rt-fax-options

flow-control

Description Specifies the flow control method used on the serial port.

Usage Specify one of the following settings:

- none (the default)
- xon-xoff
- hardware-handshake

Example `set flow-control = xon-xoff`

Location SERIAL/{ any-shelf any-slot 0 }

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 through 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 For flush-length to apply, you must set detect-end-of-packet to yes.

Location CONNECTION/"":tcp-clear-options

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 through 1000. The default is 20.

Example `set flush-time = 300`

Dependencies For flush-time to apply, you must set detect-end-of-packet to yes.

Location CONNECTION/"":tcp-clear-options

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.

Usage Specify one of the following settings:

- `yes` causes the TAOS unit to use only the 56-Kbps portion of a channel. The default bandwidth for data calls coming in over E1 channels using R2 signaling is 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.
- `no` (the default) specifies that the TAOS unit uses the full 64-Kbps bandwidth, if it is available.

Example `set force-56kbps = no`

Location `ANSWER-DEFAULTS`
`CONNECTION/"":telco-options`

force-fragmentation

Description Specifies whether or not the TAOS unit prefragments incoming packets that have the Don't Fragment 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 Don't Fragment 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.
- `no` (the default) specifies that the TAOS unit does not fragment an incoming packet that has the Don't Fragment bit set.

Dependencies Consider the following:

- Setting the `force-fragmentation` setting to `yes` causes the TAOS unit to bypass the standard maximum transmission unit (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) interoperation with outdated client software that does not handle fragmentation properly.
- You must set `mtu-limit` to a nonzero value when you set `force-fragmentation` to `yes`.

Location `ATMP`

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/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address:aesa-address`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa-address`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa-address`

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 restart the session timer or bring up a connection.

Usage Specify one of the following settings:

- `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.

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.

Example `set forward = yes`

Location `FILTER/"":input-filters`
`FILTER/"":output-filters`

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/"":visa2-options`

fr-08-mode

Description Specifies whether frame relay traffic can be switched across a DS3-ATM slot 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-o8-mode = transparent`

Dependencies For `fr-08-mode` to apply, you must set `encapsulation-protocol` to `atm-frame-relay-circuit` .

Location `CONNECTION/"":atm-options`

fr-address

Description Specifies the E.164 address for this data link.

Usage Specify an E.164 address. E.164 addresses are Integrated Services Digital Network (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/"":svc-options`

framed-only

Description Specifies whether a terminal server profile should be restricted to the framed commands (`ppp`, `mpp`, `slip`, and `quit`).

Usage Specify one of the following settings:

- `yes` specifies specifies that the profile should be restricted.
- `no` (the default) specifies that the profile should not be restricted.

Example `set framed-only = yes`

Location `ANSWER-DEFAULTS`
`CONNECTION/""`

frame-length

Description For incoming V.120 calls, specifies the frame length.

Usage For V.120 calls, specify an integer from 30 through 260, or accept the default of 256, which enables the TAOS unit to operate with an AT&T Integrated Services Digital Network (ISDN) telephone without reconfiguration.

Example `set frame-length = 260`

Location `ANSWER-DEFAULTS:v120-answer`

frame-relay-enabled

Description Indicates whether frame relay is enabled on the TAOS unit.

Usage The `frame-relay-enabled` value is read-only and can have one of the following settings:

- `yes` indicates that frame relay is enabled.
- `no` indicates that frame relay is not enabled.

Example `frame-relay-enabled = no`

Location `BASE`

frame-relay-profile

Description Specifies the name of the `frame-relay` profile to use.

Usage Specify the name of a `frame-relay` profile, exactly as specified by the `fr-name` value, including case changes.

Example `set frame-relay-profile = att-dce`

Dependencies For `frame-relay-profile` to apply, you must set `fr-direct-enabled` to `no`.

Location `CONNECTION/"":fr-options`

framer-mode

Description Specifies the DS3-ATM, E3 ATM, OC3-ATM, OC3-ATM2, or Sonet framer mode.

Usage In a `ds3-atm` profile, specify one of the following settings:

- `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 settings:

- 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/{ any-shelf any-slot 0 }:line-config`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config`

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 155.52Mbps interface in the U.S. as well as the equivalent European 155Mbps interface (STM-1).

Location `OC3-ATM/{ any-shelf any-slot 0 }:line-config`

frame-slips-threshold

Description Specifies the threshold value of frame slip errors per second.

Usage For an E1 system, specify a number from 0 through 100. For a T1 system, specify a number from 0 through 50. For each system, the default is 0 (zero), which specifies that the system does not consider frame slip errors when determining whether to switch to a new clock source.

Example `set frame-slips-threshold = 30`

Location `DS1-CLOCK-ERROR`

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 through 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/{ "" "" }`

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 line, specify one of the following settings:

- `d4` specifies the superframe format, which consists of 12 consecutive frames, separated by framing bits. Do not use this setting with Integrated Services Digital Network (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`).

For an E1 line, specify one of the following settings:

- `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`).
- `g703` specifies that the trunk interface uses CRC-4.
- `2ds` specifies that the trunk interface does not use CRC-4.

For a DS3 line, specify one of the following settings:

- `m13` specifies the standard M12/M23 (M13) asynchronous multiplexing format.
- `c-bit-parity` specifies that the C-bits are not to be used for bit-stuffing control.

Example `set frame-type = esf`

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`
`T3/{ any-shelf any-slot 0 }`

framing-type

Description Specifies the framing type for the outgoing call.

Usage Specify one of the following values:

- `any` (the default) specifies any framing type.
- `sync` specifies the synchronous framing type.
- `async` specifies the asynchronous framing type.

Example `set framing-type = sync`

Location `TUNNEL-SERVER/"":dialout-options:default-call-mapping`

fr-direct-dlci

Description Specifies the data link connection identifier (DLCI) in a frame relay direct configuration.

Usage Specify an integer from 16 through 991. The default value is 16.

Example `set fr-direct-dlci = 25`

Dependencies For `fr-direct-dlci` to apply, you must set `fr-direct-enabled` to `yes`.

Location `CONNECTION/"":fr-options`

fr-direct-enabled

Description Specifies that the TAOS unit uses the connection for frame relay direct.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit uses the connection for frame relay direct.
- `no` (the default) 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/"":fr-options`

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 For `fr-direct-profile` to apply, you must set `fr-direct-enabled` to `yes`.

Location `CONNECTION/"":fr-options`

fr-dlci

Description Specifies a frame relay data link connection identifier (DLCI) number to use for frame relay direct connections.

Usage Specify the DLCI obtained from the frame relay administrator for frame relay direct links. The default is null. More than one direct Point-to-Point Protocol (PPP) connection can share an `fr-dlci` number.

Example `set fr-dlci = 72`

Dependencies Consider the following:

- For `fr-dlci` to apply, you must set `fr-direct-enabled` to `yes`.
- The T1 FrameLine slot card supports a maximum of 240 active DLCIs.
- The Serial WAN (SWAN) slot card supports a maximum of 120 active DLCIs.

Location `CONNECTION/"":fr-options`

fr-linkdown-enabled

Description Specifies whether a trap is sent whenever a data link connection identifier (DLCI) is brought down.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

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 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 data link connection identifier (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/"":fr-options`

fr-linkup-enabled

Description Specifies whether a trap is sent whenever a data link connection identifier (DLCI) is brought up.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

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/""`

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 settings:

- `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 settings:

- `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/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

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/"":fr-options`

ft1-caller

Description Specifies whether the TAOS unit initiates fractional T1 calls.

Usage Specify one of the following settings:

- `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` (the default) specifies that the TAOS unit cannot originate the FT1 call.

Example `set ft1-caller = yes`

Dependencies The `ft1-caller` value applies when both dedicated 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/"":telco-options`

G

g711-transparent-data

Description Enables or disables transparent modem mode for a Voice over IP (VoIP) configuration.

Usage Specify one of the following settings:

- `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` (the default) 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 IP Device Control (IPDC) messages override corresponding call management settings in the default `voip` profile.

Location `VOIP/{ "" "" }`

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.
- 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/{ "" "" }`

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/{ "" "" }`

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 through 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/{ "" "" }`

gateway-access-number

Description Specifies the Dialed Number Information Service (DNIS) number passed from the public switched telephone network (PSTN) associated with the incoming 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/{ "" "" }:voip-index`

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/""`
`PRIVATE-ROUTE-TABLE/"":route-description-list`

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 one of the following settings:

- `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 Voice over IP (VoIP) call.
- `no` (the default) 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/{ "" "" }`

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`

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 Simple Network Time Protocol (SNTP) server.

Usage Specify one of the following settings 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`

Dependencies 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`

Location `IP-GLOBAL: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-1`

Location `E1/{ any-shelf any-slot 0 }: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 International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendations Q.400 to Q.490 and Israeli multifrequency carrier register 2 (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`. For information about the proper settings for other countries, please contact your carrier.

Example `set group-b-answer-signal = signal-b-1`

Location `E1/{ any-shelf any-slot 0 }:line-interface`

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 International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendations Q.400 to Q.490 and Israeli multifrequency carrier register 2 (MFC-R2) Register Signaling documentation.

Example `set group-b-busy-signal = signal-b-1`

Location `E1/{ any-shelf any-slot 0 }:line-interface`

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 For `group-b-collect-signal` to apply, you must set `signaling-mode to e1-brazil-signaling`.

Example `set group-b-collect-signal = signal-b-7`

Location `E1/{ any-shelf any-slot 0 }:line-interface`

group-b-no_match-signal

Description Specifies the signaling tone the unit uses to reject a call to a vacant number.

Usage Specify one of the following settings:

- `signal-b-5` specifies a line for which there is no fee.
- `signal-b-7` (the default) 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.

Example `set group-b-no_match-signal = signal-b-5`

Dependencies `E1/{ any-shelf any-slot 0 }:line-interface`

group-name

Description Specifies a group name for a view-based access control model (VACM) configuration.

Usage Specify a group name. The default is null.

Example `set group-name = groupNY`

Location `VACM-ACCESS/{"" "" v1 none }:access-properties`
`VACM-SECURITY-GROUP/{ v1 "" }`

H

h323-voice-ann-enabled

Description Specifies whether the TAOS unit plays voice announcements for callers to indicate call progress.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit plays voice announcements.
- `no` (the default) 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 personal identification number (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/{ "" "" }`

hardware-level

Description Indicates a one- or two-character string representing the hardware revision level of the slot card.

Usage The `hardware-level` setting is read-only. A value of `0` (zero) indicates that the revision level is unknown.

Location `BASE`
`SLOT-INFO/{ any-shelf any-slot 0 }`

hardware-rework-count

Description Indicates the number of times the slot card has been reworked.

Usage The `hardware-rework-count` setting is read-only.

Example `hardware-rework-count = 2`

Location `SLOT-INFO/{ any-shelf any-slot 0 }`

hdlc2

Description Specifies the action to take when the code image for a Hybrid Access II slot card is present in a `tar` file.

Usage Specify one of the following settings:

- `auto` (the default) causes the system to load images for slot cards that are installed in the TAOS unit, and to skip images for slot cards that are not installed.
- `load` causes the system to load the image, even if there is no slot card of that type installed.
- `skip` causes the system to skip the image, even if there is a slot card of that type installed.

Example `hdlc2 = load`

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

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 one of the following settings:

- `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 restarts the signaling link.
- `no` (the default) disables detection of a physical link failure.

Example `set heart-beat = yes`

Location `SS7-GATEWAY:transport-options`

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/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

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 through 600. The default is 60. If you specify 0 (zero), the TAOS unit sends no Hello messages.

Example `set hello-timer = 60`

Dependencies For `hello-timer` to apply, you must set `l2tp-mode` to `lac`.

Location `L2-TUNNEL-GLOBAL:l2tp-config`

high-temperature-threshold

Description Specifies the high-temperature threshold setting for the fan tray.

Usage Specify a number from 0 through 60 degrees Celsius. The default is 40.

Example `set high-temperature-threshold = 45`

Dependencies If `operation-mode` is set to `auto-regulation`, and the `high-temperature-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-threshold` setting, the system displays an error message when you attempt to write the profile.

Location `THERMAL`

high-tx-output

Description Specifies whether the DS3 or E3 cable length is more than 255 feet.

Usage Specify one of the following settings:

- `yes` specifies that the cable length is more than 255 feet.
- `no` (the default) specifies that the cable length less than 255 feet.

Example `set high-tx-output = yes`

Location `DS3-ATM/{ any-shelf any-slot 0 }:line-config`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`

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/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address:aesa-address:dsp-portion`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa-address:dsp-portion`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa-address:dsp-portion`

hold-time

Description Specifies the interval that this TAOS unit waits between keepalive, update, or notification messages from a Border Gateway Profile (BGP) peer before identifying that peer as no longer operational and dropping all information learned from that peer.

Usage Specify a number of seconds in the range from 30 through 1000. The default is 90.

Example `set hold-time = 120`

Dependencies Changing the value of `hold-time` does not cause BGP to restart.

Location `BGP-GLOBAL`

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. The default is null.

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`

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/"":tunnel-options`

hops

Description Specifies the distance to the destination network, in hops.

Usage Specify a value from 1 through 8. The default is 8.

Example `set hops = 3`

Location `IPX-ROUTE/""`

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 Simple Network Time Protocol (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 `suxiliary-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 null.

Example `set tcp-clear-options host = mercury`

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/"":tcp-clear-options`
`LOG`
`LOG:auxiliary-syslog`
`IP-GLOBAL:sntp-info`
`TERMINAL-SERVER:immediate-mode-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 `set tcp-clear-options host2 = venus`

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/"":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 `set tcp-clear-options host3 = neptune`

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/"":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 `set tcp-clear-options host4 = pluto`

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/"":tcp-clear-options`

host-1
host-2
host-3
host-4

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 `0.0.0.0/0`.

Example `set host-1 = 10.1.2.3/29`

Dependencies For the host-1, host-2, host-3, and host-4 settings to apply, you must enable terminal services. 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

host-address

Description Specifies the address to which the TAOS unit sends traps.

Usage Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example `set host-address = 10.2.3.4/24`

Dependencies Consider the following:

- If host-address is set to 0.0.0.0 and Domain Name System (DNS) or Yellow Pages/Network Information Signal (YP/NIS) is supported, the TAOS unit looks up the host address and sends traps.
- If host-address is set to 0.0.0.0 and community-name is null, traps are disabled.

Location TRAP/""

host-name

Description The host-name parameter has different uses, depending on the profile:

- In an ospf-nbma-neighbor profile, the host-name parameter specifies the station name of a local connection profile that defines the connection to the neighboring router.
- In a table-config subprofile, the host-name parameter specifies a hostname for a local Domain Name System (DNS) table entry.
- In the trap profile, the host-name parameter specifies the hostname of a station running Simple Network Management Protocol (SNMP) manager utilities.

Usage Enter a text string:

- In an 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 Yellow Pages/Network Information Signal (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
OSPF-NBMA-NEIGHBOR/""
TRAP/""

host-port

Description Specifies the port to which traps are sent.

Usage Specify a number from 1 through 65535. The default is 162.

Example **set host-port = 20**

Location TRAP/""

hour

Description Specifies the current hour.

Usage The hour parameter is read-only.

Example hour = 8

Location TIMEDATE:time

hunt-grp-phone-number-1
hunt-grp-phone-number-2
hunt-grp-phone-number-3

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 E1/{ any-shelf any-slot 0 }:line-interface
T1/{ any-shelf any-slot 0 }: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

I

icmp-reply-directed-bcast

Description Specifies whether the TAOS unit responds to directed-broadcast Internet Control Message Protocol (ICMP) echo requests.

Usage Specify one of the following settings:

- `yes` (the default) 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`

id

Description Specifies an IP address on this TAOS unit that identifies the unit as a Border Gateway Protocol (BGP) router.

Usage Specify an IP address in dotted decimal notation. The default is `0.0.0.0`, which removes the BGP ID.

Example `set id = 100.1.0.1`

Location `BGP-GLOBAL`

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`

id-auth-prefix-x25

Description Specifies the string inserted as a prefix to the username portion of a DNIS authentication request for X25 calls.

Usage Specify up to 23 characters. The default is null.

Example `set id-auth-prefix-x25 = test`

Location `EXTERNAL-AUTH:rad-auth-client`

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/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address:aesa-address:idp-portion`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa-address:idp-portion`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa-address:idp-portion`

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 through 30000. The default is 10000.

Example `set idle-character-delay = 20000`

Location `CONNECTION/"":visa2-options`

idle-logout

Description Specifies the number of seconds a Telnet session can remain logged in with no keyboard activity.

Usage Specify a number of seconds. The default is 0 (zero), which specifies that the station can remain logged in indefinitely.

Example `set idle-logout = 60`

Location `SYSTEM`
`USER/""`

idle-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 settings:

- `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 = mark-idle`

Location `T1/{ any-shelf any-slot 0 }:line-interface`

idle-pattern

Description Specifies the idle pattern for a channel.

Usage Specify any decimal value from `0` (all zeros) to `255` (all ones). The default value is `255`.

Example The following command specifies a pattern of alternating ones and zeros:

```
admin> set idle-pattern = 170
```

Dependencies Consider the following:

- The idle pattern is transmitted on the configured channel when the channel is in the idle state. Channel idle-pattern transmission is currently enabled on the T1 slot card and the T3 slot card. It applies to all T1 channels except channel 24, the D channel. For all other pattern types, it applies to all T1 channels.
- The new idle pattern takes effect when the profile is saved.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

idle-timer

Description The `idle-timer` parameter has different uses, depending on the profile:

- In the `answer-defaults` and `connection` profiles, the `idle-timer` value specifies the number of seconds the TAOS unit waits before clearing a call when a session is inactive.
- In the `atmp` profile, the `idle-timer` value specifies the number of minutes that the Home Agent maintains an idle tunnel before disconnecting it.

Usage Specify a number from 0 through 65535.

- In the `answer-defaults` and `connection` profiles, the default is `120`.
- 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.
- For Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F) calls, any data packet is considered activity, including Link Control Protocol (LCP) Echo packets or other Point-to-Point Protocol (PPP) link-level packets.
- `idle-timer` does not apply to dedicated 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 does not 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/"":session-options`

idsl

Description *Not supported*.

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/"":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.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit ignores advertised default routes. 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. Lucent Technologies recommends that you specify `yes`.
- `no` (the default) 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`

ignore-icmp-redirects

Description Specifies whether the TAOS unit processes incoming Internet Control Message Protocol (ICMP) redirect packets.

Usage Specify one of the following settings:

- `yes` causes the TAOS unit to ignore 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.
- `no` (the default) causes the TAOS unit to process ICMP redirect packets.

Example `set ignore-icmp-redirects = yes`

Location `IP-GLOBAL`

igp-lockstep

Description Specifies whether, before advertising the route to external peers, this TAOS unit is forced to match a route learned from internal Border Gateway Protocol (BGP) peers with a route learned from Open Shortest Path First (OSPF), Routing Information Protocol (RIP), static routing, or Remote Authentication Dial-In User Service (RADIUS).

Usage Specify one of the following settings:

- `yes` enables the matching feature. Normally, when a TAOS unit learns a route from its internal peers, it forwards the information to any external peers as soon as possible. Enabling the matching feature forces the unit to wait until it finds a suitable Interior Gateway Protocol (IGP) route (an OSPF, RIP, or static route, or a static route by means of RADIUS) that supports the route before advertising it. An IGP route supports a BGP route if it has the same IP address and prefix as the BGP route.
- `no` (the default) disables the matching feature.

Example `set igp-lockstep = yes`

Dependencies Exact matches only are allowed because simple default routes to support BGP can lead to network instability or lost packets.

Location `BGP-GLOBAL`

incoming-call-handling

Description Specifies how the TAOS unit processes incoming calls on this line.

Usage Specify one of the following settings:

- `internal-processing` (the default) specifies that the unit itself processes incoming calls. For a T1 line, only the default setting is supported.
- `ss7-gateway-processing` specifies that the unit passes incoming call requests to an external signaling gateway.

Example `set incoming-call-handling = internal-processing`

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

incoming-procedure

Description Specifies the type of incoming continuity checks to perform for all channels on a line.

Usage Specify one of the following settings:

- `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/{ any-shelf any-slot 0 }:line-interface:ss7-continuity`
`T1/{ any-shelf any-slot 0 }:line-interface:ss7-continuity`

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 through 32. The default is 1.

Example `set increment-channel-count = 3`

Location `ANSWER-DEFAULTS:mpp-answer`
`CONNECTION/"":mpp-options`

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.

Usage 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`.) 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.

Example `set index entry-number = 1`

Location CALL-ROUTE/{ { { any-shelf any-slot 0 } 0 } 0 }

inet-profile-type

Description Specifies whether the dedicated profile is a local profile or a Remote Authentication Dial-In User Service (RADIUS) profile.

Usage The inet-profile-type value is read-only. A setting of 0 (zero) indicates a local profile. A setting of 1 (one) indicates a RADIUS profile.

Example inet-profile-type = 1

Location ADMIN-STATE-PERM-IF/""

info

Description Specifies the Point-to-Point Protocol (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 settings:

- 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 For info to apply, terminal services must be enabled.

Location TERMINAL-SERVER:ppp-mode-configuration
TERMINAL-SERVER:slip-mode-configuration

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 through 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 then 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/{ "" "" }`

inject-policy

Description Specifies the `bgp-policy` profile that defines an injection policy.

Usage Specify a string of up to 15 characters. The default is null.

Example `set inject-policy = three_networks`

Location `BGP-PEER/""`

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 of the following settings:

- `one-sample` (the default) specifies one input sample.
- `two-samples` specifies two input samples. A setting of `two-samples` creates a more accurate result.

Example `set input-sample-count = two-samples`

Dependencies For `input-sample-count` to apply, you must set `signaling-mode` to `inband`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

insert-calling-party-addr

Description Enables or disables insertion of the calling-party address in outgoing calls.

Usage Specify one of the following settings:

- `yes` (the default) 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/{ { any-shelf any-slot 0 } 0 }:svc-options`

inter-digit-time-out

Description Specifies how long (in milliseconds) a MultiVoice® gateway waits after receiving the last digit of a dial string before declaring Dialed Number Information service (DNIS)/automatic number identification (ANI) collection complete.

Usage For all configurations except those using E1 multifrequency carrier register 2 (MFC-R2) signaling, specify a number from 100 through 6000. For configurations supporting E1 MFC-R2 signaling, specify a number from 200 through 6000. The default is 3000 (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/{ any-shelf any-slot 0 }:line-interface`

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 from 1 through 24.

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.

Example `set interface-address logical-item = 11`

Dependencies In an `atmsvc-route` profile, the `interface-address` setting specifies the interface address of the `atm-interface` profile.

Location `ATM-INTERFACE { { any-shelf any-slot 0 } 0 }`
`ATMSVC-ROUTE/""`
`ETHER-INFO/{ any-shelf any-slot 0 }`
`ETHERNET/{ any-shelf any-slot 0 }`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }`
`IPX-GLOBAL`

interface-version

Description Specifies a version name for a Peripheral Control Timing Facilities Interface (PCTFI) link. The PCTFI slot card communicates directly with a 5ESS switch across a proprietary link. When the slot card is being provisioned by the switch, a set of diagnostics are run, one of which is an inquiry of `interface-version`.

Usage Specify `first-office` or `pelts` as instructed by your provider. The default is `pelts`.

Example `set interface-version = first-office`

Location `PCTFI/{ any-shelf any-slot 0 }`

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/{ any-shelf any-slot 0 }:line-interface`

interval

Description Specifies the number of seconds between signaling heartbeat messages.

Usage Specify a number from 0 through 86400. The default is 3.

Example `set interval = 5`

Location `SS7-GATEWAY:signaling-heartbeat`

inter-vrouter

Description Specifies the name of a virtual router (VRouter) to use as the route's next hop. Packets destined for `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 For the `inter-vrouter` setting to apply, you must set `gateway-address` to `0.0.0.0`.

Location `IP-ROUTE/""`

ip-add-msg

Description Specifies a string that precedes the IP address when a terminal-server user initiates a Point-to-Point Protocol (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 For `ip-add-msg` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration`

ip-address

Description Specifies an IP address in several different profiles:

- In an `ip-interface` profile, `ip-address` assigns an IP address to an Ethernet interface.
- In an `ospf-nbma-neighbor` profile, `ip-address` specifies the IP address of the neighboring router.
- In a `static-address` subprofile, `ip-address` specifies the IP address to be assigned to a client with the associated `ethernet-address`.
- In a `table-config` subprofile, `ip-address` specifies an IP address for a local Domain Name System (DNS) table entry.

Usage Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

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 0 (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 IP-GLOBAL:dns-local-table:table-config
IP-GLOBAL:dhcp-server:static-address
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }
OSPF-NBMA-NEIGHBOR/""

ipdc-source-address

Description Specifies the IP address to be used as a source address for outgoing packets.

Usage Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example `set ipdc-source-address = 1.1.1.1`

Dependencies For `ipdc-source-address` to apply, you must set, `use-system-ip-address-as-source` to `yes`.

Location SS7-GATEWAY

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.

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 Consider the following:

- If you enable Routing Information Protocol (RIP) updates in both directions, the unit forwards all RIP packets to the IP address you specify.
- When you use IP-direct routing, a remote user cannot establish a Telnet session directly to the TAOS unit.

Location CONNECTION/"":ip-options

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 one of the following settings:

- `yes` (the default) 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 slot card.

Example `set ipport-cache-enable = no`

Location IP-GLOBAL

iproute-cache-enable

Description Enables or disables route caches.

Usage Specify `yes` or `no`.

- `yes` (the default) enables the router on the shelf controller to offload some route processing to the slot cards, and is the recommended setting.
- `no` specifies that all route processing occurs on the shelf controller.

Example `set iproute-cache-enable = yes`

Location `IP-GLOBAL`

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`

ip-routing-enabled

Description Enables or disables the routing of IP data packets for the connection.

Usage Specify one of the following settings:

- `yes` (the default) 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/"":ip-options`

ipx-dialin-pool

Description Specifies a virtual Internetwork Packet Exchange (IPX) network that the TAOS unit assigns to dial-in NetWare clients.

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/""`

ipx-frame

Description Specifies the type of packet frame the TAOS unit routes on an Ethernet connection.

Usage Specify one of the following settings:

- `none` (the default) disables Internetwork Packet Exchange (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/{ any-shelf any-slot 0 }`

ipx-header-compression

Description Specifies whether the TAOS unit should use Internetwork Packet Exchange (IPX) header compression on the connection if the encapsulation method in use supports it.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit should use IPX header compression if the encapsulation method supports it.
- `no` (the default) 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/"":ipx-options`

ipx-net-number

Description Specifies the Internetwork Packet Exchange (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 For `ipx-net-number` to apply, the TAOS unit must route IPX on the specified interface and IPX routing must be globally enabled.

Location `IPX-INTERFACE/{ any-shelf any-slot 0 }`

ipx-routing-enabled

Description Enables or disables the routing of Internetwork Packet Exchange (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.
- 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 one of the following settings:

- `yes` enables IPX routing.
- `no` (the default) 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.
- To enable the TAOS unit to route IPX on an Ethernet interface, you must set both the `ipx-routing-enabled` and `ipx-frame` values.

Location
```
CONNECTION/"":ipx-options
IPX-GLOBAL
IPX-INTERFACE/{ any-shelf any-slot 0 }
VROUTER/""
```

ipx-sap-filter-name

Description Specifies an Internetwork Packet Exchange (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 For `ipx-sap-filter-name` to apply, the TAOS unit must route IPX on the specified interface and IPX routing must be globally enabled.

Location
```
IPX-INTERFACE/{ any-shelf any-slot 0 }
IPX-SAP-FILTER/""
```

ipx-sap-hs-proxy

Description Enables or disables the home-server proxy feature.

Usage Specify one of the following settings:

- `yes` enables the home-server proxy feature.
- `no` (the default) disables the home-server proxy features.

Example `set ipx-sap-hs-proxy = yes`

Dependencies Consider the following:

- 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.
- If you set `ipx-sap-hs-proxy` to `yes`, you must use `ipx-sap-hs-proxy-net` to configure from one to six Internetwork Packet Exchange (IPX) network numbers. The unit then directs the client's SAP queries to the specified networks.

Location `CONNECTION/"":ipx-options`

ipx-sap-hs-proxy-net

Description Specifies from one to six Internetwork Packet Exchange (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 For `ipx-sap-hs-proxy-net` to apply, you must set `ipx-sap-hs-proxy` to `yes`.

Location `CONNECTION/"":ipx-options`

ipx-type-20

Description Specifies whether Internetwork Packet Exchange (IPX) Type 20 (NetBIOS) packets are propagated on the IPX interface.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit forwards IPX Type 20 packets.
- `no` (the default) specifies that the TAOS unit does not forward IPX Type 20 packets.

Example `set ipx-type-20 = yes`

Dependencies Consider the following:

- 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.
- For `ipx-type-20` to apply, the TAOS unit must route IPX on the specified interface and IPX routing must be globally enabled.

Location `IPX-INTERFACE/{ any-shelf any-slot 0 }`

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 Integrated Services Digital Network (ISDN) connections.

Usage Specify one of the following settings:

- `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 `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

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 through 65535. The default is 0 (zero), which denotes the entire slot.

Example `set item-number = 24`

Location `ADMIN-STATE-PHYS-IF/{ shelf-1 slot-2 9 }:device-address`
`DEVICE-STATE/{ { shelf-1 slot-14 9 } 2 }:device-address`
`DS3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info`
`DS3-ATM/{ any-shelf any-slot 0 }:physical-address`
`E1/{ any-shelf any-slot 0 }: line-interface: channel-config[`*n*`]:`
`call-route-info`
`E1/{ any-shelf any-slot 0 }:physical-address`
`E3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info`
`E3-ATM/{ any-shelf any-slot 0 }:physical-address`
`E3-ATM-STAT/{ any-shelf any-slot 0 }:physical-address`
`LAN-MODEM/{ any-shelf any-slot 0 }:physical-address`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info`
`OC3-ATM/{ any-shelf any-slot 0 }:physical-address`
`SERIAL/{ any-shelf any-slot 0 }:physical-address`
`SWAN/{ any-shelf any-slot 0 }:line-config:call-route-info`
`SWAN/{ any-shelf any-slot 0 }:physical-address`
`T1/{ any-shelf any-slot 0 }: line-interface: channel-config[`*n*`]:`
`call-route-info`
`T1/{ any-shelf any-slot 0 }:physical-address`
`T1-STAT/{ any-shelf any-slot 0 }:physical-address`
`T3/{ any-shelf any-slot 0 }:physical-address`
`T3-STAT/{ any-shelf any-slot 0 }:physical-address`

K

keepalive-time

Description Specifies the interval at which this TAOS unit sends keepalive messages to its Border Gateway Protocol (BGP) peers to let them know it is still reachable.

Usage Specify a number of seconds in the range from 30 through 1000. The default is 30.

Example `set keepalive-time = 45`

Dependencies Changing the value of `keepalive-time` does not cause BGP to restart.

Location `BGP-GLOBAL`

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 through 300. The default is 30.

Example `set keep-alive-timeout = 150`

Location `TRANSACTION-SERVER`

key-id

Description Specifies a value used to encrypt the secret key when `authen-type` is set to `md5`.

Usage Specify a number from 0 through 255. The default is 0 (zero).

Example `set key-id = 10`

Dependencies For `key-id` to apply, you must set `authen-type` to `md5`.

Location `CONNECTION/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

L

l2f-ignore-mid-sequence

Description Specifies whether a common sequence number is used for the L2F_PROTO protocol data units (PDUs) for both the tunnel and the client connection.

Usage Specify one of the following values:

- `yes` (the default) specifies that a common sequence number is used.
- `no` specifies that a common sequence number is not used.

Example `set l2f-ignore-mid-sequence = no`

Dependencies 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`

l2f-mode

Description Enables or disables Layer 2 Forwarding (L2F) operations.

Usage Specify one of the following settings:

- `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.

Dependencies 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`

l2f-retry-count

Description The number of times the TAOS unit resends Layer 2 Forwarding (L2F) control packets.

Usage Specify a number from 1 through 16. The default is 4.

Example `set l2f-retry-count = 8`

Dependencies Consider the following:

- For `l2f-retry-count` to apply, you must set `l2f-mode` to `nas`.
- 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`

l2f-retry-interval

Description Specifies the retry interval in seconds.

Usage Specify a number from `0` through `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 Consider the following:

- For `l2f-retry-interval` to apply, you must set `l2f-mode` to `nas`.
- 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`

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 Consider the following:

- For `l2f-system-name` to apply, you must set `l2f-mode` to `nas`.
- 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`

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 settings:

- `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-secret` 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 Consider the following:

- For `l2f-tunnel-secret` to apply, you must set `l2f-mode` to `nas`.
- 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`

l2tp-auth-enabled

Description Enables or disables Layer 2 Tunneling Protocol (L2TP) tunnel authentication.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit authenticates the L2TP network server (LNS) with a `shared-secret` before passing calls to the system.
- `no` (the default) 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`

l2tp-mode

Description Specifies the systemwide type of Layer 2 Tunneling Protocol (L2TP) functionality the TAOS unit supports.

Usage Specify one of the following settings:

- `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 a 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

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 incoming L2TP payloads.

Example `set l2tp-rx-window = 10`

Location L2-TUNNEL-GLOBAL

l2tp-system-name

Description Specifies a name to be passed to the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) when the TAOS unit initiates an 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

l2tp-tunnel-trap-enabled

Description Specifies whether a Simple Network Management Protocol (SNMP) trap is generated when a Layer 2 Tunneling Protocol (L2TP) tunnel-setup attempt fails or when an established L2TP tunnel is deactivated.

Usage Specify one of the following settings:

- `yes` (the default) specifies that a trap is generated when an L2TP tunnel-setup attempt fails or when an established L2TP tunnel is deactivated.
- `no` specifies that a trap is not generated when an L2TP tunnel-setup attempt fails or when an established L2TP tunnel is deactivated.

Example `l2tp-tunnel-trap-enabled = no`

Location `TRAP/""`

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 through 600. The default is 60.

Example `set lac-incoming-call-timer = 60`

Dependencies For `lac-incoming-call-timer` to apply, you must set `l2tp-mode` to `lac`.

Location `L2-TUNNEL-GLOBAL:l2tp-config`

lan-modem-enabled

Description Specifies whether the system generates a trap when a digital modem is moved to the suspect list.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

layer3-end

Description Specifies whether International Telecommunication Union Telecommunication Standardization Sector (ITU-T) layer 3 favors the outgoing call when a call collision occurs.

Usage Specify one of the following settings:

- `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 = y-side`

Location `E1/{ any-shelf any-slot 0 }:line-interface`

lcv-threshold

Description Specifies the threshold value of line code violation (LCV) errors per second.

Usage For an E1 system, specify a number from 0 through 8000. For a T1 system, specify a number from 0 through 4000. For each system, the default is 0 (zero), which specifies that the system does not consider LCV errors when determining whether to switch to a new clock source.

Example `set lcv-threshold = 1000`

Location `DS1-CLOCK-ERROR`

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`

left-status

Description Specifies the default content of the left side of the status window.

Usage Specify one of the following settings:

- `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/""`

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` through `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 `set len = 5`

Location `FILTER/"":input-filters[`*n*`]:gen-filter`
`FILTER/"":output-filters[`*n*`]:gen-filter`

line-coding

Description Specifies the type of zero code suppression used for the DS3 line.

Usage Only the `b3zs` setting is supported.

Example `set line-coding = b3zs`

Location `UDS3/{ any-shelf any-slot 0 }:line-config`

line-length

Description Specifies the length of the receive and transmit lines to a DSX-3 Cross Connect.

Usage Specify either of the following values:

- `0-225` (0 through 225 feet, or 0m through 68.6m)
- `226-450` (226 through 450 feet, or 68.9m through 137.2m)

For a direct connection, double the values.

Location `T3/{ any-shelf any-slot 0 }`

line-rate

Description Specifies the internal clock speed (in bps) for a Serial WAN 2 (SWAN2) slot card.

Usage Specify a value from 50 through 2048000. The default is 2048000. Although TAOS accepts any line rate up to 10 Mbps, the SWAN2 slot card is capable of generating only a limited number of discrete rates. If you enter a line rate that is not supported by the slot card, it defaults to the nearest supported rate.

Example `set line-rate = 921600`

Dependencies If you set the `line-rate` parameter to a nonsupported rate, the TAOS unit logs a message stating that the requested rate is different from the actual rate generated by the slot card. The message has the severity of `warning`. Following is an example of a log message:

```
SWAN: requested line rate 900000 differs from actual line rate of 921600
```

Location `SWAN/{ any-shelf any-slot 0 }:line-config:clocking`

line-state

Description Reports the state of an E3-ATM, T1 Primary Rate Interface (PRI), or T3 line.

Usage The `line-state` value is read-only. For an E3-ATM line, `line-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-signal`	The near end has lost the signal.
`loss-of-frame`	The near end has lost framing (also known as a red alarm).
`yellow-alarm`	A device on the line is detecting framing errors in the signal.
`ais-receive`	The line is receiving a keepalive signal.
`active`	Multipoint is established.

For a T1 PRI line, `line-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, `line-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.
`active`	Multipoint is established.
`idle-receive`	The line is receiving an idle signal.
`wrong-frame`	The remote end is configured for a different T3 application.

Example `line-state = active`

Location `DS3-ATM-STAT/{ any-shelf any-slot 0 }`
`E3-ATM-STAT/{ any-shelf any-slot 0 }`
`STM-STAT/{ any-shelf any-slot 0 }`
`T1-STAT/{ any-shelf any-slot 0 }`
`T3-STAT/{ any-shelf any-slot 0 }`
`UDS3-STAT/{ any-shelf any-slot 0 }`

line-type

Description Specifies the type of DS3 C-bit or E3 application for the line.

Usage Only the `c-bit-parity` setting is supported.

Example **`set line-type = c-bit-parity`**

Location `UDS3/{ any-shelf any-slot 0 }:line-config`

link

Description *Not supported.*

link-0-status

Description Indicates the status of link 0 of the Peripheral Control Timing Facilities Interface (PCTFI).

Usage The `link-0-status` setting is read-only and can have one of the following values:

- `disabled` indicates that the link is disabled.
- `available` indicates that link is available.
- `unavailable` indicates that the link is unavailable.

Example `link-0-status = available`

Location `PCTFI-STAT/{ any-shelf any-slot 0 }`

link-1-status

Description Indicates the status of link 1 of the Peripheral Control Timing Facilities Interface (PCTFI).

Usage The `link-1-status` setting is read-only and can have one of the following values:

- `disabled` indicates that the link is disabled.
- `available` indicates that link is available.
- `unavailable` indicates that the link is unavailable.

Example `link-1-status = available`

Location `PCTFI-STAT/{ any-shelf any-slot 0 }`

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 settings:

- `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 Internetwork Packet Exchange (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.
- `mppc` specifies Microsoft point-to-point compression (MPPC).

Example `set link-compression = stac-9`

Dependencies Only PPP, Multilink PPP (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/"":ppp-options`

linkdown-enabled

Description Specifies whether the system generates a trap when a failure occurs in a communication link between the unit and the Simple Network Management Protocol (SNMP) manager.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

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 settings:

- `none` (the default) 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.
- `ansi-t1.617d` specifies the link management protocol defined in ANSI T1.617 Annex D.
- `ccitt-q.933a` specifies the link management protocol defined Q.933 Annex A.

Example `set link-mgmt = ansi-t1.617d`

Location `FRAME-RELAY/""`

link-mgmt-dlci

Description Specifies the data link connection identifier (DLCI) to use for link management on the frame relay data link.

Usage Specify one of the following settings:

- `dlci0` (the default) specifies DLCI 0.
- `dlci1023` specifies DLCI 1023.

Example `set link-mgmt-dlci = dlci1023`

Dependencies When switched virtual circuit (SVC) signaling is enabled, `link-mgmt-dlci` must be set to its default value of `dlci0`.

Location `FRAME-RELAY/""`

link-state

Description Indicates the physical state of the LAN interface.

Usage The `link-state` value is read-only and can have one of the following settings:

- `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.

Example `set link-state = up`

Dependencies The `link-state` value can only be set by the Ethernet driver.

Location `E3-ATM-STAT/{ any-shelf any-slot 0 }`
`ETHER-INFO/{ any-shelf any-slot 0 }`

link-state-enabled

Description Specifies whether the value of `link-state` affects the IP routing tables.

Usage Specify one of the following settings:

- `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` (the default) 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/{ any-shelf any-slot 0 }`

link-type

Description Specifies the kind of logical interface between the TAOS unit and the frame relay network on the data link.

Usage Specify one of the following settings:

- `dce` specifies a User-to-Network Interface for data circuit-terminating equipment (UNI-DCE) connection. The TAOS unit operates as the network side, communicating with the user side of a frame relay terminating unit.
- `dte` specifies a User-to-Network Interface for data terminal equipment (UNI-DTE) connection. The TAOS unit operates as the user side, communicating with the network-side DCE switch.
- `nni` specifies a Network-to-Network Interface (NNI) connection. The TAOS unit performs both data terminal equipment (DTE) and data circuit-terminating equipment (DCE) link management.

Example `set link-type = dte`

Location `FRAME-RELAY/""`

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 one of the following settings:

- `yes` (the default) 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/""`

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. The default is `0.0.0.0`, which indicates an unnumbered interface.

Example `set local-address = 10.2.3.4/24`

Dependencies Consider the following:

- 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 `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/"":ip-options`

local-echo

Description Enables or disables 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 one of the following settings:

- `yes` turns on local echo.
- `no` (the default) disables local echo.

Example `set local-echo = yes`

Dependencies For `local-echo` to apply, you must enable terminal services. 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`

local-pref-default

Description Specifies a default degree-of-preference metric that this TAOS unit assigns to every external Border Gateway Protocol (BGP) route it advertises to an internal or confederation-member BGP peer.

Usage Specify a 32-bit integer. The default is `0` (zero).

Example `set local-pref-default = 5`

Dependencies Consider the following:

- Because higher numbers indicate an increased preference for a specific route when more than one route exists, you can use this metric to screen a particular autonomous system from your map of routes.
- You can assign a degree of preference in a BGP acceptance policy rule that overrides this global value.
- You can assign a degree of preference in a `bgp-summarization` profile that overrides this global value.
- If you do not assign a degree-of-preference value in this parameter, in a BGP acceptance policy, or in a `bgp-summarization` profile, one of the following values is assigned to a route by default:
  - If the route comes from an internal peer, the learned local preference number is assigned.
  - If the route comes from an external peer, the degree-of-preference number is based on the autonomous system path length, with a shorter path preferred.

Location `BGP-GLOBAL`

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 sends a negative acknowledgment (NAK) to 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 sends a NAK to 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 time-out might take longer than the time-out specified for the connection and could cause all connection attempts to fail. Therefore, set the authentication time-out value low enough to guard against the line going down, but high enough to permit the unit to respond if it can. The recommended time is 3 seconds.

Location `EXTERNAL-AUTH`

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 one of the following settings:

- `yes` (the default) 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/{ "" "" }:rt-fax-options`

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`

log-call-progress

Description Enables or disables all `syslog` progress-related Incoming Call messages. except for the End-of-Call message.

Usage Specify one of the following settings:

- `yes` enables all call-progress messages.
- `no` (the default) disables all call-related messages except End-of-Call.

Dependencies The `log-call-progress` parameter controls output of the following call-progress messages:

- Incoming Call
- Call Answered
- Assigned to Port
- Call Connected
- LAN Session Up
- Call Terminated
- LAN Session Down
- Call Cleared

For `log-call-progress` to apply, you must enable Remote Authentication Dial-In User Service (RADIUS) accounting. This parameter does not affect any call-related warning or error messages.

Location `LOG`

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).

Setting	Lowest-level message indicates
info	State and status changes that are commonly not of general interest have occurred.
debug	Helpful debugging information is displayed.

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/""`

logical-item

Description Specifies a number that represents a logical entity in a physical address.

Usage Specify a number from `0` through `4294967295`. The default is `0` (zero).

Example `set logical-item = 5`

Location `ADMIN-STATE-PERM-IF/{ any-shelf any-slot 0 }:device-address`
`DEVICE-STATE/{ { any-shelf any-slot 0} 0}:device-address`

login-prompt

Description Specifies the string that acts as a prompt for a username in the terminal-server interface.

Usage If `prompt-format` is set 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.

Regardless of the `prompt-format` setting, the default setting for `login-prompt` is `Login:`.

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 For `login-prompt` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration`

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 from 0 through 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`

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 one of the following settings:

- `yes` enables hourly log messages reporting the current software version.
- `no` (the default) 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`

lookup-prefix

Description Specifies a short text string prepended to the username portion of a Remote Authentication Dial-In User Service (RADIUS) lookup request to distinguish between Dialed Number Information Service (DNIS) and calling line ID (CLID) authentication requests and Layer 2 Tunneling Protocol (L2TP) lookup requests.

Usage Specify a text string of up to 23 characters. The default is null.

Example `set lookup-prefix = l2tp`

Location `TUNNEL-SERVER/"":dialout-options`

loop-avoidance

Description Specifies the number of transit devices through which the TAOS unit can route a call.

Usage Specify an integer from 1 through 26. The default is 7.

Example `set loop-avoidance = 7`

Location `E1/{ any-shelf any-slot 0 }:line-interface`

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, OC3-ATM, OC3-ATM2, or unchannelized DS3 interface, specify one of the following settings:

- `no-loopback` (the default) specifies that the interface is operating normally.
- `facility-loopback` specifies that the interface returns the signal it receives on the line.
- `local-loopback` specifies that 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) specifies that the interface is operating normally.
- `line-loopback` specifies that the unit loops the DS3 outwards (downstream).
- `local-loopback` specifies that 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/{ any-shelf any-slot 0 }:line-config`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config`
`T3/{ any-shelf any-slot 0 }`
`UDS3/{ any-shelf any-slot 0 }:line-config`

loop-timing

Description Enables or disables deriving transmission timing from receiver inputs.

Usage Specify one of the following settings:

- `yes` specifies that loop timing is enabled.
- `no` (the default) specifies that loop timing is disabled.

Example `set loop-timing = yes`

Location `OC3-ATM/{ any-shelf any-slot 0 }:line-configSTM/{ any-shelf any-slot 0 }`

loss-of-carrier

Description Indicates a loss of the carrier signal on a T1 line.

Usage The loss-of-carrier value is read-only and can have one of the following settings:

- true indicates a loss of carrier.
- false indicates that the carrier is maintaining a connection.

Example loss-of-carrier = false

Location T1-STAT/{ any-shelf any-slot 0 }

loss-of-frame

Description Indicates a loss-of-frame signal on the line.

Usage The loss-of-frame value is read-only and can have one of the following settings:

- true indicates a loss of frame.
- false indicates no loss of frame.

Example loss-of-frame = false

Location DS3-ATM-STAT/{ any-shelf any-slot 0 }
E3-ATM-STAT/{ any-shelf any-slot 0 }
STM-STAT/{ any-shelf any-slot 0 }
T3-STAT/{ any-shelf any-slot 0 }
UDS3-STAT/{ any-shelf any-slot 0 }

loss-of-pointer

Description Indicates a loss of pointer on the line.

Usage The loss-of-pointer value is read-only and can have one of the following settings:

- true indicates a loss of pointer.
- false indicates no loss of pointer.

Example loss-of-pointer = false

Location STM-PATH-STAT/{ any-shelf any-slot 0 }

loss-of-signal

Description Indicates a loss of signal on the line.

Usage The `loss-of-signal` value is read-only and can have one of the following settings:

- `true` indicates a loss of signal.
- `false` indicates no loss of signal.

Example `loss-of-frame = false`

Location `DS3-ATM-STAT/{ any-shelf any-slot 0 }`
`E3-ATM-STAT/{ any-shelf any-slot 0 }`
`STM-STAT/{ any-shelf any-slot 0 }`
`T3-STAT/{ any-shelf any-slot 0 }`
`UDS3-STAT/{ any-shelf any-slot 0 }`

loss-of-sync

Description Indicates whether the T1 line has lost synchronization.

Usage The `loss-of-sync` value is read-only and can have one of the following settings:

- `true` indicates a loss of synchronization.
- `false` indicates that synchronization is intact.

Example `set loss-of-sync = false`

Location `T1-STAT/{ any-shelf any-slot 0 }`

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 one of the following settings:

- `yes` (the default) 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 to 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/{ "" "" }:rt-fax-options`

low-temperature-threshold

Description Specifies the low-temperature threshold setting for the fan tray.

Usage Specify a number from 0 through 60 degrees Celsius. The default is 34.

Example `set low-temperature-threshold = 40`

Dependencies If `operation-mode` is set to `auto-regulation` and the `low-temperature-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-threshold` setting, the system displays an error message when you attempt to write the profile.

Location `THERMAL`

lqm

Description Specifies whether the TAOS unit requests link quality monitoring (LQM) when answering a Point-to-Point Protocol (PPP) call.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit requests LQM.
- `no` (the default) specifies that the TAOS unit does not request LQM.

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 Link Control Protocol (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 slot 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/"":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 (LQM) packets when answering a Point-to-Point Protocol (PPP) call.

Usage Specify a number from 0 through 600. The default is 600.

Example `set lqm-maximum-period = 300`

Dependencies For `lqm-maximum-period` to apply, you must set `lqm` to `yes`.

Location `ANSWER-DEFAULTS:ppp-answer`
`CONNECTION/"":ppp-options`

lqm-minimum-period

Description Specifies the minimum period, in one-hundredths of a second, during which the TAOS unit will accept and send link quality monitoring (LQM) packets when answering a Point-to-Point Protocol (PPP) call.

Usage Specify a number from 0 through 600. The default is 600.

Example `set lqm-minimum-period = 200`

Dependencies For `lqm-minimum-period` to apply, you must set `lqm` to `yes`.

Location `ANSWER-DEFAULTS:ppp-answer`
`CONNECTION/"":ppp-options`

M

mac-address

Description Specifies the media access control (MAC) address of an Ethernet interface. An Ethernet MAC address is a 12-digit hexadecimal number denoting the physical address encoded in the controller.

Usage In most cases, the `mac-address` value is obtained from the system. However, you can clone a profile by reading an existing one and changing its physical address.

Example `set mac-address = 00:c0:6c:4e:ac:5a`

Location `ETHER-INFO/{ any-shelf any-slot 0 }`

maintenance-state

Description Allows you to busy out or take a T1 Primary Rate Interface (PRI) line out of service. 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 one of the following settings:

- `yes` makes the line available for maintenance when all active calls have been dropped.
- `no` (the default) makes the line available for active service.

Example `set maintenance-state = yes`

Dependencies If `signaling-mode` is not set to `isdn`, `maintenance-state` does not apply. When the TAOS unit reboots, all T1 PRI lines come up available for service.

Location `T1/{ any-shelf any-slot 0 }:line-interface`

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 slot card.

Usage Specify one of the following settings:

- `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` (the default) specifies that the management-only feature is disabled.

Example `set management-only-interface = yes`

Location `IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }`

marking-type

Description Specifies how TAOS uses the first six bits in the second octet of the IP header to indicate the precedence and type of service (TOS) of the packet.

Usage Specify one of the following settings:

- `precedence-tos` (the default) specifies RFC 791 as the standard to differentiate class of service.
- `dscp` specifies differentiated services code point (DSCP) marking, as defined in RFC 2474.

Example `set marking-type = dscp`

Dependencies When the marking-type parameter is set in the voip profile, the DSCP is set in H.323 signaling packets. When the marking-type parameter is set in the ss7-gateway profile, the DSCP is set in Signaling System 7 (SS7) signaling packets.

Location CONNECTION/"":ip-options:tos-options
FILTER/"":input-filters[*n*]:tos-filter
SS7-GATEWAY:transport-options:tos
VOIP/{ "" "" }:signaling-tos
VOIP/{ "" "" }:tos-options

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.

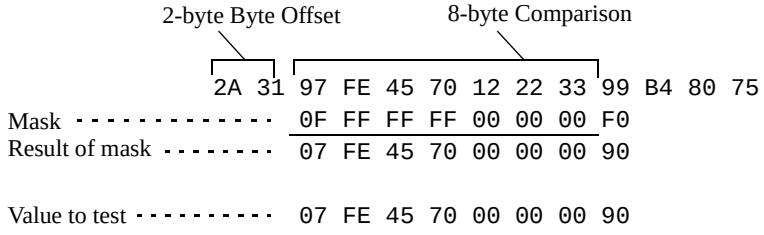
Usage Specify a hexadecimal number of up to 12 bytes. The default is 000000000000.

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.



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/"":input-filters[n]:gen-filter`
`FILTER/"":output-filters[n]:gen-filter`

match-method

Description Specifies the context match method for a view-based access control model (VACM) configuration.

Usage Specify one of the following settings:

- `exact-match` (the default) specifies that the entire context name must be matched.
- `prefix-match` specifies that only the prefix specified by `context-prefix` must be matched.

Example `set match-method = prefix match`

Location `VACM-ACCESS/{ "" "" v1 no+ }`

max-baud-rate

Description Specifies the highest baud rate that digital modems should attempt to negotiate.

Usage Specify one of the following settings:

- `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 Consider the following:

- Typically, a digital modem starts with the highest possible baud rate (33600) and negotiates 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`.
- For `max-baud-rate` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:modem-configuration`

max-bundle-members

Description Specifies the maximum number of data links allowed to join the multilink frame relay (MFR) bundle.

Usage Specify an integer. The default value is 1. 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/""`

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 through 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/{ any-shelf any-slot 0 }:line-config:traffic-shapers
E3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers
OC3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers

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 through 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.

Example `set max-call-duration = 60`

Location CONNECTION/"":session-options

maxcalls

Description Specifies the maximum number of Voice over IP (VoIP) calls a TAOS unit can process simultaneously.

Usage The number you specify depends on the unit you are configuring:

- For a MAX TNT unit, specify a number from 1 to the maximum number of DSPs installed. The default is 256.
- For an APX 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/{ "" "" }

max-calls-per-tunnel

Description Specifies the maximum number of calls for a tunnel.

Usage Specify a number from 0 through 65535. The default is 0 (zero), which specifies no limit on the number of calls for a tunnel.

Example `set max-calls-per-tunnel = 100`

Location L2-TUNNEL-GLOBAL:l2tp-config

max-cc

Description Specifies the maximum number of control protocol data unit (PDU) retransmissions (BGN, END, RESYNC).

Usage Specify an integer from 0 through 64. The default value is 4.

Example `set max-cc = 10`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: qsaal-options`

max-dialout-time

Description Specifies the maximum number of seconds the system waits for a Call Setup Complete message from the remote side when dialing out.

Usage Specify an integer from 0 through 255. The default is 20 seconds. If you set `max-dialout-time` to 0 (zero), the TAOS unit uses its internal default of 20 seconds.

Example `set max-dialout-time = 60`

Dependencies Consider the following:

- The `max-dialout-time` setting does not influence the modem time-out 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`

maximum-channels

Description Specifies the maximum number of channels in a multichannel call.

Usage Specify an integer from 1 through 32. The default is 2.

Example `set maximum-channels = 5`

Location `ANSWER-DEFAULTS:mp-answer`
`CONNECTION/"":mp-options`

maximum-rtp-port

Description Specifies the maximum User Datagram Protocol (UDP) port number in a range of UDP port numbers that the packet's UDP source port must match for it to be a high priority packet.

Usage Specify a value from 0 through 65535. The default is 0 (zero).

Example `set maximum-rtp-port = 2000`

Dependencies For `maximum-rtp-port` to apply, you must set `packet-classifcation` to `udp-port-range`.

Location `ANSWER-DEFAULTS:priority-answer`
`CONNECTION/"":priority-options`

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 through 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/{ "" "" }`

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 `maximum-leases` with `lease-duration` in the `ip-global` profile.

Location `CONNECTION/"":dhcp-options`

maxlink-client-enabled

Description Indicates whether the MAXLink client software is enabled.

Usage The maxlink-client-enabled value is read-only and can have one of the following settings:

- yes indicates that the MAXLink client software is enabled.
- no indicates that the MAXLink client software is not enabled.

Example maxlink-client-enabled = yes

Location BASE

max-multi-paths

Description Specifies the maximum number of equal-cost routes that can be listed in the routing table.

Usage Specify an integer from 1 through 4. The default is 1.

Example **set max-multi-paths = 2**

Location BGP-GLOBAL

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 through 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/"":ip-options
CONNECTION/"":ppp-options

max-pd

Description Specifies the maximum number of sequenced data protocol data units (PDUs) between poll intervals.

Usage Specify an integer from 1 through 64. The default value is 25.

Example **set max-pd = 32**

Location ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:
qsaal-options

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 through 1460. The default is 512.

Example `set max-qtp-pdu-size = 500`

Location TRANSACTION-SERVER

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/{ "" "" }:rt-fax-options`

max-restart

Description Specifies the maximum number of unacknowledged transmit RESTART messages.

Usage Specify an integer from 1 through 32. The default value is 2.

Example `set max-restart = 1`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: q93b-options`

max-retry-timer

Description Specifies (in milliseconds) the maximum time-out interval used by the Layer 2 Tunneling Protocol (L2TP) transport layer before retransmitting a packet.

Usage Specify an integer. The default is 0 (zero), which specifies no maximum time-out interval.

Example `set max-retry-timer = 100`

Location `L2-TUNNEL-GLOBAL:l2tp-config`

max-rtp-packet-delay

Description Specifies the maximum delay (in milliseconds) for Voice over IP (VoIP) packets. The value that you specify is used for calculating the fragment size for the non-Real-Time Transport Protocol (RTP) traffic using the same link.

Usage Specify a value from 0 through 1000. The default is 0 (zero).

Example `set max-rtp-packet-delay = 50`

Location `ANSWER-DEFAULTS:priority-answer`
`CONNECTION/"":priority-options`

max-shared-users

Description Specifies the number of users that can be simultaneously connected by means of a shared profile.

Usage Specify an integer from 0 through the maximum number of calls that can be handled by the TAOS unit. The default value of 0 (zero) specifies that any number of users can connect using the profile.

Example `set max-shared-users = 5`

Location `CONNECTION/""`

max-source-port

Description Specifies the highest `rlogin` source port value.

Usage Specify an integer from 128 to 1023. The default is 1023. The value you specify should be greater than or equal to the setting of `min-source-port`.

Example `set max-source-port = 250`

Dependencies For `max-source-port` to have any effect, `rlogin` must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration:rlogin-options`

max-stat

Description Specifies the maximum length of a STAT protocol data unit (PDU).

Usage Specify an integer from 32 to 128. The default value is 67.

Example `set max-stat = 64`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: qsaal-options`

max-statenq

Description Specifies the maximum number of unacknowledged transmit STATUS ENQ messages.

Usage Specify an integer from 1 through 32. The default is 1.

Example `set max-statenq = 2`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: q93b-options`

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/"":tunnel-options`

max-v92-receive-baud-rate

Description Specifies (in bits per second) the maximum upstream baud rate negotiated by the modems.

Usage Specify one of the following values:

- `48000-max-v92-baud` (the default) specifies a maximum upstream baud rate of 48000 bps.
- `46667-max-v92-baud` specifies a maximum upstream baud rate of 46667 bps.
- `45333-max-v92-baud` specifies a maximum upstream baud rate of 45333 bps.
- `44000-max-v92-baud` specifies a maximum upstream baud rate of 44000 bps.
- `42667-max-v92-baud` specifies a maximum upstream baud rate of 42667 bps.

- 41333-max-v92-baud specifies a maximum upstream baud rate of 41333 bps.
- 40000-max-v92-baud specifies a maximum upstream baud rate of 40000 bps.
- 38667-max-v92-baud specifies a maximum upstream baud rate of 38667 bps.
- 37333-max-v92-baud specifies a maximum upstream baud rate of 37333 bps.
- 36000-max-v92-baud specifies a maximum upstream baud rate of 36000 bps.
- 34667-max-v92-baud specifies a maximum upstream baud rate of 34667 bps.
- 33333-max-v92-baud specifies a maximum upstream baud rate of 33333 bps.
- 32000-max-v92-baud specifies a maximum upstream baud rate of 32000 bps.
- 30667-max-v92-baud specifies a maximum upstream baud rate of 30667 bps.
- 29333-max-v92-baud specifies a maximum upstream baud rate of 29333 bps.
- 28000-max-v92-baud specifies a maximum upstream baud rate of 28000 bps.
- 26667-max-v92-baud specifies a maximum upstream baud rate of 26667 bps.
- 25333-max-v92-baud specifies a maximum upstream baud rate of 25333 bps.
- 24000-max-v92-baud specifies a maximum upstream baud rate of 24000 bps.

Example `set max-v92-receive-baud-rate = 37333-max-v92-baud`

Dependencies For max-v92-receive-baud-rate to apply, you must set modem-mod to v92-modulation.

Location TERMINAL-SERVER:modem-configuration

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
IP-GLOBAL:mbone-backup

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`
`IP-GLOBAL:mbone-backup`

mbone-timeout

Description Specifies the number of seconds elapsed since that last receipt of an IGMP Host Membership Query packet. The router waits for this packet before considering the backup MBONE router to be dead and switching to another backup MBONE.

Usage Specify a number from `0` (the default) through `65535`. A setting of `0` (zero) disables the `mbone-timeout` feature.

Example `set mbone-timeout = 120`

Location `IP-GLOBAL`
`IP-GLOBAL:mbone-backup`

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 one of the following settings:

- `yes` (the default) 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/""`

md5-auth-key

Description Specifies the secret key to be used for the message-digest algorithm 5 (MD5) cryptographic authentication method.

Usage Specify a text string of up to 16 characters. The default value is `ascend0`.

Example `set md5-auth-key = 12!secret*34key`

Dependencies When `authen-type` is set to `md5`, you must supply a value for the `md5-auth-key` setting, because the `auth-key` value no longer applies.

Location `CONNECTION/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

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/{ any-shelf any-slot 0 }`

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 one of the following settings:

- `yes` specifies that a trap is generated to report the status of the link between the SS7 media gateway and the TAOS unit.
- `no` (the default) specifies that a trap is note 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/""`

menu-selection-string

Description In the terminal-server:menu-mode-options subprofile, specifies a text string that explains the menu options from which a user can choose.

Usage Specify a text string of up to 60 characters. The default is null.

Example `set menu-selection-string = "Select option [1-4, q-quit]: "`

Location TERMINAL-SERVER:menu-mode-options

metric

Description Specifies a Routing Information Protocol (RIP)-style metric for the route.

Usage Specify an integer from 1 through 15. In an ip-route profile, the default is 1. In a route-description-list 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/""
PRIVATE-ROUTE-TABLE/"":route-description-list

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 through 255. The default is 15.

Example `set metric-max = 25`

Location TRANSACTION-SERVER

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 systemwide.

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/"":fr-options`
`FRAME-RELAY/""`
`MULTI-LINK-FR/""`

mfr-bundle-type

Description Specifies the type of multilink frame relay (MFR) configuration.

Usage Only the `mfr-dte` type is supported.

Example `set mfr-bundle-type = mfr-dte`

Location `MULTI-LINK-FR/""`

min-bandwidth

Description Specifies the minimum aggregated bandwidth before 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/""`

minimum-channels

Description Specifies the minimum number of channels in a multichannel call.

Usage Specify an integer from `1` through `32`. The default is `1`.

Example `set minimum-channels = 1`

Location `ANSWER-DEFAULTS:mp-answer`
`CONNECTION/"":mp-options`

minimum-rtp-port

Description Specifies the minimum User Datagram Protocol (UDP) port number in a range of UDP port numbers that the packet's UDP source port must match for it to be a high priority packet.

Usage Specify a value from 0 through 65535. The default is 0 (zero).

Example `set minimum-rtp-port = 1000`

Dependencies For `minimum-rtp-port` to apply, you must set `packet-classifcation` to `udp-port-range`.

Location `ANSWER-DEFAULTS:priority-answer`
`CONNECTION/"":priority-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 For `min-source-port` to apply, `rlogin` must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration:rlogin-options`

minute

Description Specifies the current minute.

Usage The `minute` parameter is read-only.

Example `minute = 23`

Location `TIMEDATE:time`

mode

Description Specifies whether a Peripheral Control Timing Facilities Interface (PCTFI) link is provisioned in T1 mode or in E1 mode.

Usage Specify one of the following settings:

- `e1` specifies that the link is provisioned in E1 mode.
- `t1` specifies that the link is provisioned in T1 mode.

Example `set mode = e1`

Location `PCTFI/{ any-shelf any-slot 0 }`

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 settings:

- `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/"":ppp-options`

modem-dialout-enabled

Description Indicates whether modem dial-out is enabled for the unit.

Usage The `modem-dialout-enabled` value is read-only and can have one of the following settings:

- `yes` indicates that modem dial-out is enabled.
- `no` indicates that modem dial-out is disabled.

Example `modem-dialout-enabled = yes`

Location `BASE`

modem-disable-mode

Description Specifies the state of each of the digital modems in a slot card. The setting might also affect a B channel of a T1 Primary Rate Interface (PRI) line.

Usage Specify one of the following settings:

- `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 slot 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 deactivates a DS0 channel. Although the modem cannot be made available, changing this setting to `enable` restores the DS0 channel. If the unit has no T1 PRI lines enabled, the `dis-channel` setting has the same effect as `disable`.

Example `set modem-disable-mode = disable`

Location `LAN-MODEM/{ any-shelf any-slot 0 }`

modem-mod

Description Sets the modem modulation to use when answering calls on a 56Kbps modem.

Usage Specify one of the following settings:

- `k56-modulation` specifies that the slot card can operate at a normal rate.
- `v34-modulation` specifies that the slot card never exceeds V.34 speeds (33.6K) and does not send the V.8bis tone.
- `v90-modulation` (the default) specifies that the slot card operates at V.90 modulation.
- `v92-modulation` specifies that the slot card operates at V.92 modulation.

Example `set modem-mod = v34-modulation`

Location `TERMINAL-SERVER:modem-configuration`

modem-on-hold-timeout

Description Specifies the time that the server modem remains on hold after the client modem receives a call and requests that the data call be suspended.

Usage Specify one of the following settings:

Values	Result
`moh-disabled`	Disables modem on hold (default) (Valid for the `modem-configuration` subprofile only)
`10-sec-moh-timeout`	Sets the modem on hold time-out to 10 seconds
`20-sec-moh-timeout`	Sets the modem on hold time-out to 20 seconds
`30-sec-moh-timeout`	Sets the modem on hold time-out to 30 seconds
`40-sec-moh-timeout`	Sets the modem on hold time-out to 40 seconds
`1-min-moh-timeout`	Sets the modem on hold time-out to 1 minute
`2-min-moh-timeout`	Sets the modem on hold time-out to 2 minutes
`3-min-moh-timeout`	Sets the modem on hold time-out to 3 minutes
`4-min-moh-timeout`	Sets the modem on hold time-out to 4 minutes

Values	Result
6-min-moh-timeout	Sets the modem on hold time-out to 6 minutes
8-min-moh-timeout	Sets the modem on hold time-out to 8 minutes
12-min-moh-timeout	Sets the modem on hold time-out to 12 minutes
16-min-moh-timeout	Sets the modem on hold time-out to 16 minutes
no-limit-moh-timeout	Sets the modem on hold time-out to unlimited
conn-profile-use-global	Sets the value for all the modem sessions unless specified in the respective connection profiles. The value in the connection profile overrides this global value.

Example `set modem-on-hold-timeout = 10-sec-moh-timeout`

Dependencies Although V.92 allows for a maximum on-hold time of 16 minutes, time-out values in higher protocol stacks may interrupt data applications before the on-hold time is up. Network administrators should examine the implications of enabling modem on hold for their network applications. For example, the end user should not expect file transfers using File Transfer Protocol (FTP) or similar protocols to resume after the modems have reestablished connection.

You should generally set the value of the idle-timer parameter in a connection profile to be at least 30 seconds longer than the value of the modem-on-hold-timeout parameter in order to prevent calls that have been placed on hold from being disconnected prematurely.

Location CONNECTION/""
TERMINAL-SERVER:modem-configuration

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-phys-if profile.

Usage The modem-table-index setting is read-only.

Example `modem-table-index = 5`

Location `ADMIN-STATE-PHYS-IF/{ any-shelf any-slot 0 }`

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:

- `-10-db-mdm-trn-level` (-10 dB, the default)
- `-13-db-mdm-trn-level` (-13 dB)
- `-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 = -14-db-mdm-trn-level`

Dependencies For `modem-transmit-level` to apply, terminal services must be enabled. For a 56Kbps modem, accept the default of `-10-db-mdm-trn-level`.

Location `TERMINAL-SERVER:modem-configuration`

month

Description Specifies a month of the year.

Usage Specify a text string or a number representing a month of the year.

Example `set month = January`

Location `TIMEDATE:date`

more

Description Specifies whether the TAOS unit includes the next filter rule before determining whether the frame matches the generic filter.

Usage Specify one of the following settings:

- `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` (the default) 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/"":input-filters[`*n*`]:gen-filter`
`FILTER/"":output-filters[`*n*`]:gen-filter`

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/"":ppp-options
FRAME-RELAY/""

msg-proc-model

Description Specifies the message-processing model to use when generating Simple Network Management Protocol (SNMP) messages.

Usage Specify one of the following settings:

- v1 (the default) specifies SNMP version 1 (SNMPv1).
- v3 specifies SNMP version 3 (SNMPv3). For SNMPv3 notification support, specify v3.

Example `set msg-proc-model = v3`

Location SNMPV3-TARGET-PARAM/""

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/"":ppp-options

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. The default is `0` (zero),

- If you accept 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.
- If you set `mtu-limit` to a nonzero value, the task of fragmentation and reassembly is performed by the connection endpoints, lowering the overhead on the ATMP agents.

Example `set mtu-limit = 1472`

Location `ATMP`

multicast-address

Description Specifies the multicast destination address for multicast stacking control packets. The packets are sent to the specified multicast address and to the User Datagram Protocol (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. The specified address must be a valid multicast (class D) address.

Example `set multicast-address = 239.192.74.75`

Location `STACKING`

multicast-allowed

Description Enables or disables multicasting on the IP interface.

Usage Specify one of the following settings:

- yes enables the TAOS unit to respond to Internet Group Management Protocol (IGMP) client requests and responses.
- no (the default) 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 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/"":ip-options
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }

multicast-forwarding

Description Enables or disables multicast forwarding for the TAOS unit.

Usage Specify one of the following settings:

- yes enables multicast forwarding.
- no (the default) 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

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 through 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 through 20 seconds.

Example `set multicast-group-leave-delay = 15`

Dependencies For `multicast-group-leave-delay` to apply, you must set `multicast-forwarding` to `yes` and `multicast-allowed` to `yes`.

Location `CONNECTION/"":ip-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }`

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`

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

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`

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

multicast-hbeat-port

Description Specifies a User Datagram Protocol (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

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

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

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

multicast-interface-ip-address

Description Specifies the IP address of the Ethernet port to be used for stacking IP multicast control traffic.

Usage Specify an IP address in dotted decimal notation. The default is 0.0.0.0, which specifies that the unit uses the system's shelf-controller Ethernet interface.

Example `set multicast-interface-ip-address = 10.10.10.1`

Location STACKING

multicast-member-timeout

Description Specifies the time-out (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 through 65535. The default is 360.

Example `set multicast-member-timeout = 60`

Dependencies For `multicast-member-timeout` to apply, you must set `multicast-forwarding` to `yes`.

Location `IP-GLOBAL`

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`

Dependencies Consider the following:

- 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) packets on the interface but does not accept packets from clients.
- You must set `multicast-rate-limit` to a nondefault value before the unit can forward multicast traffic.

Location `CONNECTION/"":ip-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }`

multi-rate-enabled

Description Indicates whether the unit can make Dialable Wideband Service (DWS) calls.

Usage The `multi-rate-enabled` value is read-only and can have one of the following settings:

- `yes` indicates that the unit can make DWS calls.
- `no` indicates that the unit cannot make DWS calls.

Example `multi-rate-enabled = yes`

Location `BASE`

must-accept-address-assign

Description Instructs the TAOS unit to hang up if a caller rejects dynamic IP address assignment.

Usage Specify one of the following settings:

- `yes` specifies that the caller must accept dynamic IP address assignment.
- `no` (the default) 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`

my-ip-address

Description Specifies the IP address of the local Border Gateway Protocol (BGP) peer.

Usage Specify an IP address in dotted decimal notation. The default is `0.0.0.0`.

Example `set my-ip-address = 10.9.8.7`

Location `BGP-PEER/""`

N

n391-val

Description Specifies the number of T391 polling cycles between full status enquiry messages.

Usage Specify an integer from 1 through 255. The default is 6, which indicates that after six status requests spaced `t391-val` seconds apart, the User-to-Network Interface for data terminal equipment (UNI-DTE) device requests a full status report.

Example `set n391-val = 15`

Dependencies For `n391-val` to apply, `link-type` must be set to `dte`.

Location `FRAME-RELAY/""`

n392-val

Description Specifies the number of errors, during `dte-n393` monitored events, that cause the user side to declare the network side's procedures inactive.

Usage Specify an integer from 1 through 10. The value you enter must be less than `n393-val`. The default is 3.

Example `set n392-val = 5`

Dependencies For `n392-val` to apply, `link-type` must be set to `dte`.

Location `FRAME-RELAY/""`

n393-val

Description Specifies the data terminal equipment (DTE)-monitored event count.

Usage Specify an integer from 1 through 10. The value you enter must be greater than `n392-val`. The default is 4.

Example `set n393-val = 6`

Dependencies For `n393-val` to apply, `link-type` must be set to `dte`.

Location `FRAME-RELAY/""`

nailed-group

Description Assigns a group number to a T1, E1, DS3-ATM, E3-ATM, OC3-ATM, OC3-ATM2, Serial WAN (SWAN), or unchannelized DS3 line. You can then refer to the number in the `connection` profile's `nailed-groups` setting to specify the dedicated channels a connection uses.

Usage Specify a number from 0 through 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 dedicated group must be contiguous.

Location
```
DS3-ATM/{ any-shelf any-slot 0 }:line-config
E1/{ any-shelf any-slot 0 }:line-interface:channel-config
E3-ATM/{ any-shelf any-slot 0 }:line-config
OC3-ATM/{ any-shelf any-slot 0 }:line-config
SWAN/{ any-shelf any-slot 0 }:line-config
T1/{ any-shelf any-slot 0 }:line-interface:channel-config
UDS3/{ any-shelf any-slot 0 }:line-config
```

nailed-groups

Description Specifies one or more dedicated groups belonging to a session.

Usage Specify a number assigned to a group of dedicated 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 dedicated groups.

Location `CONNECTION/"":telco-options`

nailed-mode

Description Specifies how the TAOS unit uses the link's dedicated channels, and whether the link uses dedicated channels alone, or a combination of dedicated and switched channels.

Usage Specify one of the following settings:

- `ft1` (the default) specifies that the link uses only dedicated channels.
- `off` specifies that the TAOS unit does not use dedicated 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/""`

nailed-up-group

Description Specifies the group number assigned to dedicated channels in a line profile, such as a `t1` or `e1` profile.

Usage Specify a number assigned to a group of dedicated 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 dedicated 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/""`

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, Border Gateway Protocol (BGP) policy, or the TAOS unit itself.
- In the `snmpv3-usm-user profile`, the `name` value specifies the user for whom the TAOS unit exchanges a Simple Network Management Protocol version 3 user-based security model (SNMPv3 USM) message.

Usage Specify a descriptive name with no embedded spaces.

- For all profiles except the `atm-interface`, `bgp-policy`, `ip-route`, `ipx-route`, `private-route-table`, `snmpv3-notification`, `snmpv3-target-param`, `snmpv3-usm-user`, `stacking`, `trap`, and `vrouter` profiles, you can specify up to 24 characters.
- For the `atm-interface`, `bgp-policy`, `stm`, and `vrouter` profiles, you can specify up to 15 characters.

- For the `ip-route`, `ipx-route`, and `trap` profiles, you can specify up to 31 characters.
- For the `snmpv3-notification`, `snmpv3-target-param`, and `stacking` profiles, you can specify up to 16 characters.
- For the `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 `\x`*NN* format with the ASCII code for the character. For example, the value `test\x20\x21` represents the string `test!`.

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/{ { any-shelf any-slot 0 } 0 }`
```
ATMSVC-ROUTE/""
BGP-POLICY/""
DS3-ATM/{ any-shelf any-slot 0 }
E1/{ any-shelf any-slot 0 }
E3-ATM/{ any-shelf any-slot 0 }
FIREWALL/""
IP-ROUTE/""
IPX-ROUTE/""
OC3-ATM/{ any-shelf any-slot 0 }
OSPF-NBMA-NEIGHBOR/""
PCTFI/{ any-shelf any-slot 0 }
PRIVATE-ROUTE-TABLE/"":route-description-list
SNMP-MANAGER/""
SNMPV3-NOTIFICATION/""
SNMPV3-TARGET-PARAM/""
SNMPV3-USM-USER/""
STACKING
STM/{ any-shelf any-slot 0 }
STM-PATH/{ any-shelf any-slot 0 }
SWAN/{ any-shelf any-slot 0 }
SYSTEM
T1/{ any-shelf any-slot 0 }
```

```
T3/{ any-shelf any-slot 0 }
USER/""
VROUTER/""
```

nas-port-format

Description Specifies the format used to calculate the Remote Authentication Dial-In User Service (RADIUS) NAS-Port value.

Usage Specify one of the following values:

- not-applicable (the default) specifies that the unit uses the new-nas-port-id-format value.
- 2-4-5-5 specifies that the NAS-Port value is calculated using either the 2_4_5_5 or the 2_4_6_4 format.
  - 2_4_5_5 specifies a digital call or an analog call that does not come into an analog modem slot card. The shelf number is composed of 2 bits, the slot number is composed of 4 bits, the line number is composed of 5 bits, and the channel number is composed of 5 bits.
  - 2_4_6_4 specifies an analog call that comes into an analog modem slot card. The shelf number is composed of 2 bits, the slot number is composed of 4 bits, the line number is composed of 6 bits, and the channel number is composed of 4 bits.
- 6-5-5 specifies that the NAS-Port value is calculated using the 0_6_5_5 format. This format specifies no shelf number, a slot number composed of 6 bits, a line number composed of 5 bits, and a channel number composed of 5 bits. This setting is the only one supported by an APX unit.
- 1-2-2 specifies that the NAS-Port value is calculated using 1_2_2 format. 1_2_2 specifies that the first digit is 1 for a digital call and 2 for an analog call, that the next 2 digits indicate the slot and line number, and that the last 2 digits indicate the channel used by the call. Note that the lines are serially numbered. For example, on a MAX TNT unit, lines 1 through 8 are associated with slot 1, lines 9 through 16 are associated with slot 2, and so on.
- 1-2-3-3 specifies that the NAS-Port value is calculated using the 1_2_3_3 format. The shelf number is always 1, the slot number is an integer from 1 through 16 for a MAX TNT unit and from 1 through 40 for an APX unit, the line number is an integer from 1 through 999, and the channel number is an integer from 1 through 999.

For an analog modem slot card, the format is 2_4_6_4 and is not configurable.

Example `set nas-port-format = 1-2-3-3`

Dependencies The 2_4_5_5, 2_4_6_4, and 0_6_5_5 formats are bit-based. The digits are first converted from decimal to binary, parsed into segments, and converted back to decimal. Then, the system adds 1 to each segment. For example, for a digital call, the decimal value 6191 is converted to an equivalent binary value of 000110000010111. Then, the value is parsed in the following way:

```
00 0110 00001 0111
```

This binary value is equivalent to the following decimal value:

```
0 6 1 15
```

The system then adds 1 to each number to arrive at the following NAS-Port value:

`1 7 2 16`

The NAS-Port value provides the following information:

Shelf=1
Slot=7
Line=2
Channel=16

Note that the shelf number always translates to 1.

The 1_2_2 and 1_2_3_3 formats are digit-based. When you specify the 1_2_3_3 format, the NAS-Port value is calculated in the following manner:

NAS-Port = (*shelf-number* * 100000000) + (*slot-number* * 1000000) + (*line-number* * 1000) + (*channel-number*)

For example, if a call comes into channel 13 of line 2 of an E1 slot card in slot 1 and shelf 1, the NAS-Port value is calculated as follows:

NAS-Port = (1 * 100000000) + (1 * 1000000) + (2 * 1000) + 13 = 101002013

The following table shows which method is used to calculate the NAS-Port value for different combinations of the nas-port-format and new-nas-port-id-format settings in the system profile:

nas-port-format value	**new-nas-port-id-format value**	**Format for NAS-Port value**
not-applicable	yes	2_4_5_5
not-applicable	no	1_2_2
2-4-5-5	yes or no	2_4_5_5
1-2-2	yes or no	1_2_2
1-2-3-3	yes or no	1_2_3_3

Location SYSTEM

nas-port-type

Description Specifies the type of service for the session.

Usage Specify one of the following settings:

- 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/"":telco-options

net-alias

Description Specifies the Internetwork Packet Exchange (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 For net-alias to apply, the TAOS unit must route IPX for the connection or IPX routing must be globally enabled.

Location CONNECTION/"":ipx-options

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

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

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/"":route-description-list

net-number

Description Specifies the Internetwork Packet Exchange (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 For `net-number` to apply, the TAOS unit must route IPX for the connection or IPX routing must be globally enabled.

Location `CONNECTION/"":ipx-options`

network-loopback

Description Indicates whether the T1 line is looped back to the network.

Usage The `network-loopback` value is read-only and can have one of the following settings:

- `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.

Example `network-loopback = true`

Location `T1-STAT/{ any-shelf any-slot 0 }`

network-management-enabled

Description Indicates whether the network-management license is enabled.

Usage The `network-management-enabled` value is read-only and can have one of the following settings:

- `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 Simple Network Management Protocol version 3 user-based security model (SNMPv3 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.
- Encryption is not supported.

Location `BASE`

network-mgmt-voip-enabled

Description Indicates whether the license for network management with Voice over IP (VoIP) is enabled.

Usage The `network-management-voip-enabled` value is read-only and can have one of the following settings:

- `yes` indicates that the network management with VoIP option is enabled.
- `no` indicates that the network management with VoIP option is disabled.

Example `network-management-voip-enabled = yes`

Location `BASE`

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/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

new-nas-port-id-format

Description *Not supported.*

next-call

Description Specifies the string that a user must enter to initiate a new call while a current call is in any of the following stages: call proceeding, call alerting, call connected, or call busy. A new call can be initiated while a current call is in progress when a user dials a string that matches the pattern specified by the `next-call` parameter. When the dialing string has been entered, the user hears a dial tone and can then proceed to enter the entire 7- or 10-digit number.

Usage Specify a string of up to five digits. The string can contain the numbers 0 through 9 or the asterisk (*) character. The default is **9.

Example `set next-call = **999`

Dependencies While dialing, the user must enter the digits within the time limit specified by the `inter-digit-time-out` parameter. If the digits are not entered within the time limit, the user must reenter the entire sequence of digits again. By default, a caller has up to 6 seconds to enter each digit of a telephone number.

New calls can be initiated only when the following settings are specified in the `voip` profile:

- The `single-dial-enable` parameter is set to `no`.
- The `dtmf-tone-passing` parameter is set to `dtmf-tone-passed-outofband`.
- The `sequential-call-enable` parameter is set to `yes`.

Location `VOIP/{ "" "" }`

next-policy

Description Specifies the name of a Border Gateway Protocol (BGP) acceptance, injection, or advertisement policy that this TAOS unit applies immediately after the policy defined in a `bgp-policy` profile.

Usage Specify the name of an existing BGP policy. The default is null.

Example `next-policy = 194_network`

Location `BGP-POLICY/""`

nfas-group-id

Description Specifies the number of a non-facility associated signaling (NFAS) group.

Some sites require multiple NFAS groups on a single slot card to enable grouped DS1s. An NFAS group contains a minimum of two PRIs, so the T1 slot card supports up to four NFAS groups, and the T3 slot card supports up to 14 NFAS groups.

Usage For a T1 slot card, set `nfas-group-id` to a value from 0 through 3. For a T3 slot card, valid values are from 0 through 13. Lines with the same `nfas-group-id` value are in the same NFAS group.

Example `set line-interface nfas-group-id = 1`

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/{ any-shelf any-slot 0 }:line-interface`

nfas-id

Description Specifies a group ID for T1 lines that use non-facility associated signaling (NFAS).

Usage Specify a number from 0 through 31. You must ask your service provider about the NFAS ID number to specify for each line. For a Signaling System 7 (SS7) configuration, the `nfas-id` value specifies an interface ID for the T1 or E1 line used as an SS7 line.

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 Integrated Services Digital Network (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 `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

nl-value

Description Specifies the number of retransmissions the TAOS unit sends on the line.

Usage Specify an integer from 1 through 255. The default is 64. You must accept the default when the line connects to a Digital Private Network Signaling System (DPNSS) or Digital Access Signaling System 2 (DASS 2) switch.

Example `set nl-value = 64`

Location `E1/{ any-shelf any-slot 0 }:line-interface`

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 one of the following settings:

- `yes` (the default) 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 `set noattr6-use-termsrv = no`

Location `EXTERNAL-AUTH`

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 through 255. The default is 8.

Example `set no-conn-ack-increment = 100`

Location `TRANSACTION-SERVER`

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 time-out interval.

Usage Specify a number from 0 through 255. The default is 10.

Example `set no-first-status-metric = 100`

Location `TRANSACTION-SERVER`

no-high-prio-pkt-duration

Description Specifies the number of seconds during which the TAOS unit processes no high-priority packets before it discontinues IP fragmentation of low-priority packets.

Usage Specify a number from 0 through 65535. The default is 60. if you accept the default of 0 (zero), the TAOS unit does not check for a duration in which high-priority packets are no longer being processed, and continues to fragment low-priority packets.

Example `set no-high-prio-pkt-duration = 120`

Location `ANSWER-DEFAULTS:priority-answer`
`CONNECTION/"":priority-options`

non-multicast

Description Specifies whether all multicast packets are remapped to a directed neighbor address.

Usage Specify one of the following settings:

- `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` (the default) specifies that multicast packets are not remapped to a directed neighbor address.

Example `set non-multicast = yes`

Location `CONNECTION/"":ip-options:ospf-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

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 time-out interval.

Usage Specify a number from 0 through 255. The default is 16.

Example `set no-second-status-metric = 100`

Location `TRANSACTION-SERVER`

notification-log-age-out

Description Specifies the number of minutes that a Simple Network Management Protocol (SNMP) notification is kept in a log before it is automatically removed.

Usage Specify a number from 0 to 2147483647. The default is 1440 (4 hours). If you specify 0 (zero), a notification is kept in a log indefinitely.

Example `set notification-log-age-out = 2880`

Location SNMP

notification-log-enable

Description Specifies whether Simple Network Management Protocol (SNMP) notifications for this profile are to be logged.

Usage Specify one of the following settings:

- yes enables logging.
- no (the default) disables logging.

Example `notification-log-enable = yes`

Location TRAP/""

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/""

notify-view-name

Description Specifies the name of the view-based access control method (VACM) view for notify access.

Usage Specify a string. The default is null.

Example `set notify-view-name = notifyview1`

Location VACM-ACCESS/{ "" "" v1 no+ }

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 incoming dialed telephone numbers on MultiVoice® gateways using E1 trunks supporting inband Compelled Multiple Frequency (CMF) R2.

Usage Specify one of the following settings:

- `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 restarts 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 multifrequency carrier register 2 (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 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`, `e1-p7-signaling`, `dpnss`, or `none`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`

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 unsupported and have the same effect as the default value of `undefined`.

Example `set numbering-plan = ISDN`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr`

num-digits-trunk-groups

Description Specifies the number of digits to allow for trunk groups.

Usage Specify a number from 1 through 4. When you accept the default of 1, trunk-group numbers range from 2 through 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.
- For num-digits-trunk-groups to apply. you must set use-trunk-groups to yes.

Location SYSTEM

O

oam-ais-f5

Description Enables or disables sending operations, administration, and maintenance (OAM) Alarm Indication signal (AIS) F5 cells when a permanent virtual circuit (PVC) fails.

Usage Specify one of the following settings:

- disable (the default) specifies that the unit does not send any OAM AIS F5 cells.
- segment specifies that the unit sends OAM AIS F5 cells indicating segment failure.
- end-to-end specifies that the unit sends OAM AIS F5 cells indicating end-to-end failure.

Example `set oam-ais-f5 = segment`

Location CONNECTION/"":atm-options

offset

Description Specifies a byte-offset from the start of a frame to the data that the TAOS unit tests against the generic filter.

Usage Specify a number from 0 through 8. The default is 0 (zero), which indicates no offset.

Example `set offset = 2`

Dependencies 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.

Location `FILTER/"":input-filters[n]:gen-filter`
`FILTER/"":output-filters[n]:gen-filter`

oof-threshold

Description Specifies the threshold value of line out of frame (OOF) errors per second.

Usage Specify a number from 0 through 10. The default is 0 (zero), which specifies that the system does not consider OOF errors when determining whether to switch to a new clock source.

Example `set oof-threshold = 5`

Location `DS1-CLOCK-ERROR`

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`

operation-mode

Description Specifies the mode of operation in which to run the fan tray.

Usage Specify one of the following settings:

- `full-speed-only` (the default) specifies that the fans in the fan tray 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

ospf-approaching-overflow-enabled

Description Enables or disables generation of Open Shortest Path First (OSPF) trap 15 if the number of link state advertisements (LSAs) in the router's link-state database has exceeded 90 percent of OSPFExtLsdbLimit.

Usage Specify one of the following settings:

- yes enables generation of OSPF trap 15.
- no (the default) disables generation of OSPF trap 15.

Example `set ospf-approaching-overflow-enabled = yes`

Location TRAP/""

ospf-ase-pref

Description Specifies the preference value for Open Shortest Path First (OSPF) routes that the router learns about by means of Routing Information Protocol (RIP), Internet Control Message Protocol (ICMP), or another non-OSPF protocol.

When choosing the routes to put in the routing table, the router first compares their preference values, preferring the lowest number. If the preference values are equal, the router compares the metric values, using the route with the lowest metric.

Usage Specify a number from 0 through 255. A value of 255 prevents the use of the route. Following are the default preferences for different types of routes:

- 0 (zero)—Connected routes
- 10—OSPF routes
- 30—Routes learned from ICMP redirects
- 100—Routes learned from RIP
- 100—Static routes

Example `set ospf-ase-pref = 100`

Location IP-GLOBAL

ospf-enabled

Description Enables or disables generation of Open Shortest Path First (OSPF) traps 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 one of the following settings:

- yes specifies that trap generation depends on whether the specific OSPF trap is enabled.
- no (the default) specifies that OSPF traps are generated regardless of individual OSPF trap settings in the profile.

Example `ospf-enabled = yes`

Location TRAP/""

ospf-if-auth-failure-enabled

Description Enables or disables generation of Open Shortest Path First (OSPF) trap 6 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.

Usage Specify one of the following settings:

- 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 (the default) 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/""

ospf-if-config-error-enabled

Description Enables or disables generation of Open Shortest Path First (OSPF) trap 4 if a packet has been received on a nonvirtual interface from a router whose configuration conflicts with this router's configuration.

Usage Specify one of the following settings:

- `yes` specifies that OSPF trap 4 is generated if a packet has been received on a nonvirtual interface from a router whose configuration conflicts with this router's configuration.
- `no` (the default) specifies that OSPF trap 4 is not generated if a packet has been received on a nonvirtual interface from a router whose configuration conflicts with this router's configuration.

Example `set ospf-if-config-error-enabled = yes`

Dependencies The event `optionMismatch` causes a trap only if it prevents an adjacency from forming.

Location `TRAP/""`

ospf-if-rx-bad-packet

Description Enables or disables trap 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 one of the following settings:

- `yes` specifies that OSPF trap 8 is generated if an OSPF packet has been received on a nonvirtual interface that cannot be parsed.
- `no` (the default) specifies that OSPF trap 8 is not generated if an OSPF packet has been received on a nonvirtual interface that cannot be parsed.

Example `set ospf-if-rx-bad-packet = yes`

Location `TRAP/""`

ospf-if-state-change-enabled

Description Enables or disables trap 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 one of the following settings:

- `yes` specifies that OSPF trap 16 is generated if the state of a nonvirtual OSPF interface has changed.
- `no` (the default) specifies that OSPF trap 16 is not generated if the state of a nonvirtual OSPF interface has changed.

Example `set ospf-if-state-change-enabled = yes`

Location `TRAP/""`

ospf-lsdb-overflow-enabled

Description Enables or disables generation of Open Shortest Path First (OSPF) trap 14 if the number of link state advertisements (LSAs) in the router's link-state database has exceeded OSPFExtLsdbLimit.

Usage Specify one of the following settings:

- yes specifies that OSPF trap 14 is generated if the number of LSAs in the router's link-state database has exceeded OSPFExtLsdbLimit.
- no (the default) specifies that OSPF trap 14 is not generated if the number of LSAs in the router's link-state database has exceeded OSPFExtLsdbLimit.

Example `ospf-lsdb-overflow-enabled = yes`

Location TRAP/""

ospf-maxagelsa-enabled

Description Enables or disables generation of Open Shortest Path First (OSPF) trap 13 if a link state advertisement (LSA) in the router's link-state database has aged to MaxAge.

Usage Specify one of the following settings:

- yes specifies that OSPF trap 13 is generated if an LSA in the router's link-state database has aged to MaxAge.
- no (the default) specifies that OSPF trap 13 is not generated if an LSA in the router's link-state database has aged to MaxAge.

Example `ospf-maxagelsa-enabled = yes`

Location TRAP/""

ospf-max-lsa

Description Specifies the maximum number of link state advertisements (LSAs) allowed in the link-state database.

Usage Specify a number from 0 through 4294967295. The default is 0 (zero).

Example `set ospf-max-lsa= 1000`

Location IP-GLOBAL:ospf-global

ospf-nbr-state-change-enabled

Description Enables or disables generation of Open Shortest Path First (OSPF) trap 2 if the state of a nonvirtual OSPF neighbor has changed.

Usage Specify one of the following settings:

- `yes` specifies that OSPF trap 2 is generated if the state of a nonvirtual OSPF neighbor has changed.
- `no` (the default) specifies that OSPF trap 2 is not generated if the state of a nonvirtual OSPF neighbor has changed.

Example `ospf-nbr-state-change-enabled = yes`

Dependencies OSPF trap 2 is generated when the neighbor state regresses (for example, changes from `Attempt` or `Full` to `1-Way` or `Down`) or progresses to a terminal state (for example, `2-Way` or `Full`). When a neighbor transitions from or to `Full` on nonbroadcast multiaccess (NBMA) and broadcast networks, the trap is generated by the designated router. A designated router transitioning to `Down` is noted by `OSPFIfStateChange`.

Location `TRAP/""`

ospf-originatelsa-enabled

Description Enables or disables generation of Open Shortest Path First (OSPF) trap 12 if a new link state advertisement (LSA) has been originated by this router due to a topology change.

Usage Specify one of the following settings:

- `yes` specifies that the unit generates OSPF trap 12 if a new LSA has been originated by this router due to a topology change.
- `no` (the default) specifies that the unit does not generate OSPF trap 12 if a new LSA has been originated by this router due to a topology change.

Example `set ospf-originatelsa-Enabled = yes`

Location `TRAP/""`

ospf-pref

Description Specifies the preference for routes that the router learns about by means of the Open Shortest Path First (OSPF) protocol.

When choosing the routes to put in the routing table, the router first compares their preference values, preferring the lowest number. If the preference values are equal, the router compares the metric values, using the route with the lowest metric.

Usage Specify a number from 0 through 255. A value of 255 prevents the use of the route. Following are the default preferences for different types of routes:

- 0 (zero)—Connected routes
- 10—OSPF routes
- 30—Routes learned from Internet Control Message Protocol (ICMP) redirects
- 100—Routes learned from Routing Information Protocol (RIP)
- 100—Static routes
- 100—Ascend Tunnel Management Protocol (ATMP) routes

Example `set ospf-pref = 10`

Location IP-GLOBAL

ospf-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 one of the following settings:

- yes specifies that the unit generates OSPF trap 10 if an OSPF packet has been retransmitted on a nonvirtual interface.
- no (the default) specifies that the unit does not generate OSPF trap 10 if an OSPF packet has been retransmitted on a nonvirtual interface.

Example `set ospf-tx-retransmit-enabled = yes`

Location TRAP/""

ospf-virt-if-auth-failure-enabled

Description Enables or disables generation of Open Shortest Path First (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.

Usage Specify one of the following settings:

- 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 (the default) 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/""

ospf-virt-if-config-error-enabled

Description Enables or disables generation of Open Shortest Path First (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.

Usage Specify one of the following settings:

- `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` (the default) 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/""`

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 one of the following settings:

- `yes` specifies that the unit generates OSPF trap 9 if an OSPF packet has been received on a virtual interface that cannot be parsed.
- `no` (the default) specifies that the unit does not generate OSPF trap 9 if an OSPF packet has been received on a virtual interface that cannot be parsed.

Example `set ospf-virt-if-rx-bad-packet = yes`

Location `TRAP/""`

ospf-virt-if-state-change-enabled

Description Enables or disables trap generation if the state of an Open Shortest Path First (OSPF) virtual interface has changed (OSPF trap 1).

Usage Specify one of the following settings:

- `yes` specifies that the unit generates OSPF trap 1 if the state of an OSPF virtual interface has changed.
- `no` (the default) specifies that the unit does not generate OSPF trap 1 if the state of an OSPF virtual interface has changed.

Example `set ospf-virt-if-state-change-enabled = yes`

Location `TRAP/""`

ospf-virt-if-tx-retransmit-enabled

Description Enables or disables trap generation if an Open Shortest Path First (OSPF) packet has been retransmitted on a virtual interface (OSPF trap 11). All packets that are retransmitted are associated with a link-state database (LSDB) entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry.

Usage Specify one of the following settings:

- `yes` specifies that the unit generates OSPF trap 11 if an OSPF packet has been retransmitted on a virtual interface.
- `no` (the default) specifies that the unit does not generate OSPF trap 11 if an OSPF packet has been retransmitted on a virtual interface.

Example `set ospf-virt-if-tx-retransmit-enabled = yes`

Location `TRAP/""`

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 one of the following settings:

- `yes` specifies that the unit generates OSPF trap 3 if the state of an OSPF virtual neighbor has changed.
- `no` (the default) specifies that the unit does not generate OSPF trap 3 if the state of an OSPF virtual neighbor has changed.

Example `set ospf-virt-nbr-state-change-enabled = yes`

Location `TRAP/""`

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 settings:

- `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 settings:

- `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/{ any-shelf any-slot 0 }:line-interface:ss7-continuity`
`T1/{ any-shelf any-slot 0 }:line-interface:ss7-continuity`

overlap-receiving

Description Enables or disables overlap receiving for incoming calls on the Primary Rate Interface (PRI) line.

Usage Specify one of the following settings:

- `yes` enables overlap receiving.
- `no` (the default) disables overlap receiving.

Example `set overlap-receiving = yes`

Dependencies If `overlap-receiving` is set to `no`, the `pri-prefix-number`, `trailing-digits`, and `t302-timer` settings do not apply.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

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 settings:

- `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 RT-24 encoding. RT-24 is a Lucent Technologies proprietary codec, which is available only on MultiVoice® gateways running TAOS 8.0 or later. 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 g11-ulaw or g711-alaw.
- Changes to the packet-audio-mode setting take effect with the next call.

When a G.723 codec is selected:

- silence-det-cng can be enabled or disabled for 6.4Kbps processing only (packet-audio-mode is set to 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 rates.

Location VOIP/{ "" "" }

packet-classification

Description Specifies a method for prioritizing Point-to-Point Protocol (PPP) packets.

Usage Specify one of the following values:

- qos-tag (the default) classifies a PPP packet as high priority or low priority based on its quality of service (QoS) tag.
- udp-port-range classifies a PPP packet as high priority or low priority based on its User Datagram Protocol (UDP) port range. A packet has high-priority if its UDP source port number falls within the range of port numbers defined by the minimum-rtp-port and maximum-rtp-port parameters.

Example `set packet-classification = udp-port-range`

Dependencies The TAOS unit uses the qos-tag parameter setting in the qos:tag-map[*n*] subprofile. If the tag-map subprofile is enabled, the TAOS unit does the following:

- Classifies a packet as high priority when the qos-tag parameter is set to a value equal to 4, 5, or 6
- Classifies a packet as low priority when the parameter is set to 1, 2, or 3

Location ANSWER-DEFAULTS:priority-answer
CONNECTION/"":priority-options

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 settings:

- 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 For packet-redundancy to apply, you must set fixed-packets to no. 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/{ "" "" }:rt-fax-options

parallel-dialing

Description Specifies the number of call-setup requests that the system sends to the network side at any given time.

Usage For MAX TNT units, specify an integer from 1 through 64. For APX units, specify an integer from 1 through 65535. 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. For MAX TNT units, the default is 2. For APX units, the default is 65535.

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

partly-congested-metric

Description Specifies a number 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 through 255. The default is 4.

Example `set partly-congested-metric = 5`

Location TRANSACTION-SERVER

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 \x*NN* 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:

- For the password setting to apply in a tunnel-options subprofile, you must set agent-mode to home-agent.
- 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.
- 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/"":tunnel-options
SNMPV3-USM-USER/""
USER/""

password-enabled

Description Specifies whether failed Telnet login attempts generate a trap.

Usage Specify one of the following settings:

- yes (the default) specifies that failed Telnet login attempts generate a trap.
- no specifies that failed Telnet login attempts do not generate a trap.

Example `set password-enabled = no`

Dependencies When password-enabled is set to yes, you must also set security-enabled to yes for all failed Telnet login attempts to generate a trap.

Location TRAP/""

password-for-direct-access

Description Specifies the password that the user must enter when security-for-direct-access is set to global.

Usage Specify a password of up to 21 characters. The default is null.

Example `set password-for-direct-access = mypassword`

Dependencies For password-for-direct-access to apply, you must set security-for-direct-access to global and direct-access to yes.

Location TERMINAL-SERVER:dialout-configuration

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. Password: is the default.

Example set password-prompt = Your Password:

Dependencies For password-prompt to apply, you must enable terminal services.

Location TERMINAL-SERVER:terminal-mode-configuration

path-state

Description Indicates the state of the synchronous optical network (SONET) path.

Usage The path-state value is read-only.

Example path-state = sonet-path-active-no-defect

Location STM-PATH-STAT/{ any-shelf any-slot 0 }

p-bit-error-count

Description Indicates the number of P-bit errors received on the line. These errors indicate that the unit received a P-bit code on the M-frame that differs from the locally calculated code.

Usage The p-bit-error-count value is read-only.

Example p-bit-error-count = 3

Location DS3-ATM-STAT/{ any-shelf any-slot 0 }
E3-ATM-STAT/{ any-shelf any-slot 0 }
UDS3-STAT/{ any-shelf any-slot 0 }

pctfie

Description Indicates the action to take when the code image for a Peripheral Control Timing Facilities Interface (PCTFI) slot card is present in a tar file on a system with E1 lines.

Usage The pctfie value is read-only and can have one of the following settings:

- auto (the default) indicates that the system loads images for slot cards that are installed in the TAOS unit, and skips images for slot cards that are not installed.
- load indicates that the system loads the image, even if no slot card of that type is installed.
- skip indicates that the system skips the image, even if a slot card of that type is installed.

Example pctfie = skip

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

pctfit

Description Indicates the action to take when the code image for a Peripheral Control Timing Facilities Interface (PCTFI) slot card is present in a `tar` file on a system with T1 lines.

Usage The `pctfit` value is read-only and can have one of the following settings:

- `auto` (the default) indicates that the system loads images for slot cards that are installed in the TAOS unit, and skips images for slot cards that are not installed.
- `load` indicates that the system loads the image, even if no slot card of that type is installed.
- `skip` indicates that the system skips the image, even if a slot card of that type is installed.

Example `pctfit = skip`

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

pctfi-trunk-status-change-enabled

Description Specifies whether the system generates a trap when the trunk-status F1 bit changes on a Peripheral Control Timing Facilities Interface (PCTFI) virtual tributary.

Usage Specify one of the following settings:

- `yes` (the default) specifies that the system generates a trap when the trunk-status F1 bit changes on a PCTFI virtual tributary.
- `no` specifies that the system does not generate a trap when the trunk-status F1 bit changes on a PCTFI virtual tributary.

Example `set pctfi-trunk-status-change-enabled = no`

Location `TRAP/""`

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 interfaces, the valid range is from 0 through 34368.
- For OC3-ATM interfaces, the valid range is from 0 through 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 variable bit rate (VBR) traffic, the `peak-rate` value specifies the upper boundary of the variable bit rate.

Location
```
DS3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers
E3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers
OC3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers
```

peer-ip-address

Description Specifies the IP address of the remote Border Gateway Protocol (BGP) peer.

Usage Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example `set peer-ip-address = 10.9.8.7`

Location `BGP-PEER/""`

peer-mode

Description Specifies whether the remote Internetwork Packet Exchange (IPX) caller is an IPX router or a dial-in client.

Usage Specify one of the following settings:

- `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.
- For `peer-mode` to apply, the TAOS unit must route IPX for the connection or IPX routing must be globally enabled.

Location `ANSWER-DEFAULTS:ipx-answer CONNECTION/"":ipx-options`

peer-name

Description Specifies the name of the remote Border Gateway Protocol (BGP) peer.

Usage Specify a text string of up to 31 characters. The default is null.

Example `set peer-name = peer1`

Location `BGP-PEER/""`

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 settings:

- `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 dedicated 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`

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 dedicated frame relay data-link connection is in use, `phone-number` does not apply.

Location
```
CALL-ROUTE/{ { { any-shelf any-slot 0 } 0 } 0 }
E1/{ any-shelf any-slot 0 }:line-interface:channel-config
FRAME-RELAY/""
T1/{ any-shelf any-slot 0 }:line-interface:channel-config
```

phs-support

Description Indicates whether support for the Personal Handyphone System (PHS) is enabled.

Usage The phs-support value is read-only and can have one of the following settings:

- yes indicates that PHS support is enabled.
- no indicates that PHS support is disabled.

Example phs-support = yes

Location BASE

ping

Description Enables and disables the terminal-server ping command.

Usage Specify one of the following settings:

- yes enables terminal-server users to use the ping command.
- no (the default) disables the ping command in the terminal-server interface.

Example set ping = yes

Location TERMINAL-SERVER:terminal-mode-configuration

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/"":ip-options:ospf-options
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf

poll-rate

Description Specifies the number of milliseconds between polls.

Usage Specify a number from 500 through 5000. The default 5000.

Example set poll-rate = 2000

Location CONNECTION/"":hdlc-nrm-options

poll-retry-count

Description Specifies the number of times that the TAOS unit retries the poll after a response time-out.

Usage Specify a number from 0 through 255. The default is 2.

Example `set poll-retry-count = 5`

Location CONNECTION/"":hdlc-nrm-options

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 through 255000. The default is 60000.

Example `set poll-timeout = 50000`

Location CONNECTION/"":hdlc-nrm-options

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 restart the unit for the change to take effect.

Location IP-GLOBAL
VROUTER/""

pool-chaining

Description Enables or disables IP pool chaining.

Usage Specify one of the following settings:

- `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` (the default) 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`

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` through `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-users` 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`
`CONNECTION/"":ppp-options`

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.

Usage Specify a name of up to 11 characters. The default is null.

Example `set pool-name 1 = newyork`

Dependencies Consider the following:

- Each pool configuration consists of a base address (specified by `pool-base-address`), address count (specified by `assign-count`), and name (specified by `pool-name`).
- If TACACS+ authentication is not in use, the 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/""`

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/"":dhcp-options`

pool-ospf-adv-type

Description Specifies how to import summarized pool addresses into Open Shortest Path First (OSPF).

Usage Specify one of the following settings:

- `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

pool-summary

Description Specifies whether pool summarization is in use.

Usage Specify one of the following settings:

- yes enables pool summarization.
- no (the default) 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.

Location IP-GLOBAL
VROUTER/""

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.
- 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.

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 `set tcp-clear-options port 1 = 155`

Dependencies Consider the following:

- You can specify one port for each of four login hosts. If the Transmission Control Protocol (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 `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/"":tcp-clear-options`
`LOG`
`LOG:auxiliary-syslog`
`TERMINAL-SERVER:immediate-mode-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 `set tcp-clear-options port2 = 256`

Dependencies You can specify one port for each of four login hosts. If the Transmission Control Protocol (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/"":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 `set tcp-clear-options port3 = 170`

Dependencies You can specify one port for each of four login hosts. If the Transmission Control Protocol (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 unit returns a TCP connection error to the dial-in client.

Location `CONNECTION/"":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 `set tcp-clear-options port4 = 180`

Dependencies You can specify one port for each of four login hosts. If the Transmission Control Protocol (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/"":tcp-clear-options`

port-1
port-2
port-3
port-4

Description Specifies the port to use for contacting the Telnet host specified by the corresponding `host-1`, `host-2`, `host-3`, or `host-4` parameter.

Usage Specify a number from 0 through 65535. The default is 0 (zero).

Example `set port-1 = 50`

Dependencies The `port-1`, `port-2`, `port-3`, and `port-4` parameters apply only when the corresponding `service-1`, `service-2`, `service-3`, or `service-4` parameter is set to `telnet`.

Location `TERMINAL-SERVER:menu-mode-options`

port-enabled

Description Specifies whether the TAOS unit sends traps to the Simple Network Management Protocol (SNMP) manager.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit sends traps to the host specified by `host-address`.
- `no` (the default) specifies that the TAOS unit does not send traps.

Example `set port-enabled = yes`

Location `TRAP/""`

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 through 32767. The default is 5000.

Example `set port-for-direct-access = 5001`

Dependencies For `port-for-direct-access` to apply, you must enable terminal services and set `direct-access` to `yes`.

Location `TERMINAL-SERVER:dialout-configuration`

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). Transmission Control Protocol (TCP) and User Datagram Protocol (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/"":port-redirect-options`

power-supply-enabled

Description Specifies whether the system generates a trap when a power supply module is added or removed.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

ppp

Description Enables or disables the use of the ppp command in the terminal-server interface.

Usage Specify one of the following settings:

- yes enables the use of the ppp command in the terminal-server interface.
- no (the default) disables the use of the ppp command in the terminal-server interface.

Example `set ppp = yes`

Dependencies For ppp to apply, terminal services must be enabled.

Location TERMINAL-SERVER:ppp-mode-configuration

pptp-enabled

Description Enables or disables Point-to-Point Tunneling Protocol (PPTP) tunneling.

Usage Specify one of the following settings:

- yes enables PPTP tunneling.
- no (the default) disables PPTP tunneling.

Example `set pptp-enabled = yes`

Location L2-TUNNEL-GLOBAL

precedence

Description The precedence parameter has different uses, depending on the subprofile in which it is set:

- In a signaling-tos subprofile, the precedence parameter specifies the priority level of User Datagram Protocol (UDP) packets.
- In a tos subprofile, the precedence parameter specifies the priority level of Signaling System 7 (SS7) signaling traffic.
- In a tos-options or tos-filter subprofile, the precedence parameter 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 `signaling-tos`, `tos`, or `tos-options` subprofile, or `type` to `tos-filter` in the `input-filters` or `output-filters` subprofile.

Location `CONNECTION/"":ip-options:tos-options`
`FILTER/"":input-filters[n]:tos-filter`
`FILTER/"":output-filters[n]:tos-filter`
`SS7-GATEWAY:transport-options:tos`
`VOIP/{ "" "" }:signaling-tos`
`VOIP/{ "" "" }:tos-options`

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` through `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/"":ip-options`
`IP-ROUTE/""`

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/{ { { any-shelf any-slot 0 } 0 } 0 }`

prefix

Description Specifies an IP address number that, when paired with a subnet mask length, represents a range of addresses rather than a single IP network.

Usage Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example `set prefix = 10.9.8.7`

Location BGP-SUMMARIZATION/{ 0.0.0.0/0 }

primary

Description Specifies whether the dial-in unit is a primary station.

Usage Specify one of the following settings:

- 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 (the default) 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/"":hdlc-nrm-options

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.
- For primary-ip-address to apply, you must set enabled to yes in the ss7-gateway profile.

Location SS7-GATEWAY

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 through 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/{ "" "" }`

primary-tcp-port

Description Specifies the primary Transmission Control Protocol (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`.
- For `primary-tcp-port` to apply, you must set `enabled` to `yes` in the `ss7-gateway` profile.

Location `SS7-GATEWAY`

primary-tunnel-server

Description Specifies the IP address or hostname of one of the following:

- Ascend Tunnel Management Protocol (ATMP) primary Home Agent
- Layer 2 Tunneling Protocol (L2TP) network server (LNS) endpoint
- Point-to-Point Protocol (PPTP) network server (PNS) endpoint
- Layer 2 Forwarding (L2F) Home Gateway endpoint
- Intermediate destination that will decapsulate 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 253 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 User Datagram Protocol (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 `set primary-tunnel-server = 10.11.22.33:8877`

Dependencies Consider the following:

- For `primary-tunnel-server` to apply, you must set `profile-type` to `mobile-client`.
- 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/"":tunnel-options`

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 and backup designated-router 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 designated router or backup designated router. 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` through `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 (VBR)-nonreal time service. A value of `2` specifies unspecified bit rate (UBR) service.

Example `set priority = 10`

Dependencies Choose the designated-router and backup designated-router election priority on the basis of each device's processing power and reliability. Assigning a priority of 1 or greater places the TAOS unit on the list of possible designated routers and backup designated routers. A priority value of 0 (zero) excludes the unit from becoming a designated router or backup designated router. The higher the priority value of the TAOS unit relative to other OSPF routers on the network, the better the chances that it will become a designated router or backup designated router.

Location `CONNECTION/"":ip-options:ospf-options`
`DS3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers`
`E3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config:traffic-shapers`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf`

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 pressing the pound sign).

Usage Specify a prefix. Typically, the Primary Rate Interface (PRI) prefix is an Integrated Services Digital Network (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 For `pri-prefix-number` to apply, you must set `overlap-receiving` to `yes`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

private-route

Description Specifies whether the TAOS unit advertises route information by means of routing protocols.

Usage Specify one of the following settings:

- `yes` makes the route private. The TAOS unit uses the route internally, but does not advertise it.
- `no` (the default) specifies that the TAOS unit advertises the route by means of routing protocols.

Example `set private-route = yes`

Location `CONNECTION/"":ip-options`
`IP-ROUTE/""`

private-route-profile-required

Description Specifies whether the system drops a call if it cannot find a private-route-table profile.

- In the answer-defaults profile, the private-route-profile-required parameter 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, the private-route-profile-required parameter specifies whether the system drops the call if it cannot locate the private-route-table profile indicated in the connection profile.

Usage Specify one of the following settings:

- yes specifies that the system drops the call if it cannot locate a private-route-table profile.
- no (the default) specifies that the system establishes the link even if it cannot locate a 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/"":ip-options

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/"":ip-options

priv-key

Description Specifies a privacy key for Simple Network Management Protocol version 3 user-based security model (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
```

Dependencies Consider the following:

- You must generate the privacy key by means of the `snmpPrivPass` command before the `snmpv3-usm-user` profile can be used for communication with the SNMP manager.
- If you change the authentication protocol from MD5 to SHA (or vice versa), you must change the privacy key by means of the `snmpPrivPass` command. The previous protocol and key combination is used until you specify a new one.
- If `priv-protocol` is set to `no-auth`, `priv-key` does not apply.

Location `SNMPV3-USM-USER/""`

priv-protocol

Description Enables or disables encryption of messages sent on behalf of the user to or from the Simple Network Management Protocol (SNMP) engine, and if enabled, the type of privacy protocol to be used.

Usage Specify one of the following settings:

- `no-priv` (the default) specifies that no encryption is required and that privacy is disabled.
- `des-priv` specifies that Data Encryption Standard (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/""`

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.

Usage Specify one of the following settings:

- `no-progress-indicator` (the default) disables alert reporting of call-routing events on the outbound switched telephone network.
- `none-end2end-isdn` specifies that the outbound MultiVoice® gateway reports when calls are connected to an outbound switched telephone network that does not use Integrated Services Digital Network (ISDN) signaling. The outbound switched telephone network can support robbed-bit or detectable dual-tone multifrequency (DTMF).
- `dest-non-isdn` specifies that the outbound MultiVoice® gateway reports when calls are connected to an outbound 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 incoming 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 outbound 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 outbound MultiVoice® gateway reports whether interworking occurs upon connection to the switched telephone network. Such 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 outbound 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/{ "" "" }:pstn-attribute`

profile-name

Description Specifies the name of the `connection` profile that the TAOS unit uses to reach the Internetwork Packet Exchange (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/""`

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 one of the following settings:

- `yes` (the default) 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`

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 settings:

- `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`

Dependencies 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/"":tunnel-options`

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/""`

prompt-format

Description Specifies whether the TAOS unit interprets carriage-return/linefeed and tab characters in the string specified by `login-prompt`.

Usage Specify one of the following settings:

- `yes` causes the TAOS unit to interpret carriage-return/linefeed and tab characters in the string specified by `login-prompt`.
- `no` (the default) 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 For `prompt-format` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration`

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 a `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 (UDP).
- `tcp` specifies Transmission Control Protocol (TCP).

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 File Transfer Protocol (FTP) traffic, and TCP with a `port-number` of 23 represents Telnet traffic.

Location `CONNECTION/"":port-redirect-options`
`FILTER/"":input-filters[`*n*`]:ip-filter`
`FILTER/"":output-filters[`*n*`]:ip-filter`
`FILTER/"":input-filters[`*n*`]:tos-filter`
`FILTER/"":output-filters[`*n*`]:tos-filter`

proxy-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 settings:

- `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/{ { any-shelf any-slot 0 } 0 }`

Q

qos-tag

Description Specifies the priority assigned to a packet depending on the value of the packet's type of service (TOS) byte.

Usage Specify one of the following values:

- `0` (the default) specifies the lowest priority and is nominally defined as best effort.
- `1 to 6` specifies the range of priorities from low to high.

Example `set qos-tag = 3`

Location `QOS:tag-map`

qtp-port

Description Specifies the User Datagram Protocol (UDP) port on which Quick Transaction Protocol (QTP) listens for incoming QTP connections.

Usage Specify a port number from 1 through 65535. The default is 3350.

Example `set qtp-port = 20`

Location TRANSACTION-SERVER

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 through 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

quick-connect-enabled

Description Enables and disables the Quick-Connect feature.

Usage Specify one of the following settings:

- yes enables the Quick-Connect feature.
- no (the default) disables the Quick-Connect feature.

Example `set quick-connect-enabled = yes`

Location CONNECTION/""
TERMINAL-SERVER:modem-configuration

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 through 2000. The default is 350.

Example `set r1-anir-delay = 5000`

Dependencies For r1-anir-delay to apply, you must set signaling-mode to r1-inband.

Location E1/{ any-shelf any-slot 0 }:line-interface
T1/{ any-shelf any-slot 0 }:line-interface

r1-anir-timer

Description Specifies the duration in milliseconds of the Automatic Number ID Request (ANIR) signal.

Usage Specify a number from 180 through 400. The default is 200.

Example `set r1-anir-timer = 300`

Dependencies For `r1-anir-timer` to apply, you must set `signaling-mode` to `r1-inband`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

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 through 1000. The default is 340.

Example `set r1-first-digit-timer = 300`

Dependencies For `r1-first-digit-timer` to apply, you must set `signaling-mode` to `r1-inband`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

r1-modified

Description Enables or disables a modified version R1 signaling required in Taiwan.

Usage Specify one of the following settings:

- `yes` enables a modified version of R1 signaling. For units located in Taiwan, set `r1-modified` to `yes`.
- `no` (the default) disables a modified version of R1 signaling. The unit uses regular R1 signaling (described in the International Telecommunication Union (ITU) recommendation Q.310-332).

Example `set r1-modified = yes`

Dependencies For `r1-modified` to apply, you must set `signaling-mode` to `r1-inband`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

r1-use-anir

Description Enables and disables Automatic Number ID Request (ANIR) processing.

Usage Specify one of the following settings:

- `yes` specifies that the system performs ANIR processing on incoming calls.
- `no` (the default) specifies that the system does not perform ANIR processing on incoming calls.

Example `set r1-use-anir = yes`

Dependencies For `r1-use-anir` to apply, you must set `signaling-mode` to `r1-inband`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

r2-signaling-enabled

Description Indicates whether R2 signaling is enabled.

Usage The `r2-signaling-enabled` value is read-only and can have one of the following settings:

- `yes` indicates that R2 signaling is enabled.
- `no` indicates that R2 signaling is not enabled.

Example `r2-signaling-enabled = no`

Location `BASE`

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 object ID and IP address of the new server.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

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 VSAs to the RADIUS server and does not recognize VSAs if the server sends them. 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.

Example `set radius-server-compat = vendor-specific`

Dependencies At this time, only NavisRadius™ supports 16-bit VSAs.

Location `EXTERNAL-AUTH:rad-auth-server`

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 one of the following settings:

- `yes` specifies that RADIUS clients can send RADIUS commands to the TAOS unit.
- `no` (the default) specifies that RADIUS clients cannot send RADIUS commands to the TAOS unit.

Example `set rad-server-enable = no`

Location `EXTERNAL-AUTH`

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 one of the following settings:

- `yes` enables the TAOS unit to use RARP to obtain its IP address from a RARP server.
- `no` (the default) disables the TAOS unit's ability to use RARP.

Example `set rarp-enabled = yes`

Location `IP-GLOBAL`

rdi-receive

Description Indicates whether the STM link is detecting a Remote Defect Indication (RDI).

Usage The `rdi-receive` value is read-only and can have one of the following settings:

- `true` indicates that the STM link is detecting an RDI.
- `false` indicates that the STM link is not detecting an RDI.

Example `rdi-receive = false`

Location `STM-STAT/{ any-shelf any-slot 0 }`

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`

read-view-name

Description Specifies the name of the view-based access control method (VACM) view for read access.

Usage Specify a string. The default is null.

Example `set read-view-name = readview1`

Location `VACM-ACCESS/{ "" "" v1 no+ }`

read-write-access

Description Specifies whether the TAOS unit grants the Simple Network Management Protocol version 3 user-based security model (SNMPv3 USM) user read and write access to its management information base (MIB) settings.

Usage Specify `yes` or `no`.

- `yes` specifies that the TAOS unit grants the SNMPv3 USM user read and write access to its MIB settings.
- `no` (the default) 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/""`

read-write-community

Description Specifies a read/write Simple Network Management Protocol (SNMP) community name. An SNMP manager must send the correct community name to access the SNMP Get, Get-Next, and Set commands.

Usage Specify the community name. You can enter up to 32 characters. The default is `write`.

Example `set read-write-community = secret`

Location `SNMP`

read-write-enabled

Description Enables or disables read-write access to the unit's management information base (MIB).

Usage Specify one of the following settings:

- `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` (the default) 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`

receive-auth-mode

Description Specifies the authentication protocol to use for incoming Point-to-Point Protocol (PPP), Multilink PPP (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. A message-digest algorithm 5 (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 Data Encryption Standard (DES) encryption.
`token-pap-ppp-auth`	The connection must use PAP with dynamic passwords. When you specify this setting, the system uses one-time DES password encryption and sends a challenge in the token.
`token-chap-ppp-auth`	The connection must use PAP-Token for the first call of a multichannel session, and CHAP for additional channels.
`cache-token-ppp-auth`	The connection must use CHAP with dynamic passwords. The system uses CHAP with challenges, but caches token responses and uses them for authenticating additional channels.
`ms-chap-ppp-auth`	The connection must use MS-CHAP, designed mostly for Windows NT or LAN Manager platforms.
`pap-preferred`	The TAOS unit offers authentication protocols in the following order during Link Control Protocol (LCP) negotiations: 1 PAP 2 CHAP 3 MS-CHAP If a client refuses to accept PAP authentication (for example, a Microsoft Windows client that is configured to accept only encrypted authentication), the TAOS unit then offers CHAP or MS-CHAP authentication.

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`

receive-equalization

Description Specifies whether the REQDIS (Receive Equalization Disable) bit in the LIU control register is set to 0 (zero).

Usage Specify one of the following settings:

- `yes` specifies that the the REQDIS (Receive Equalization Disable) bit in the LIU control register is set to 0 (zero).
- `no` (the default) specifies that the the REQDIS (Receive Equalization Disable) bit in the LIU control register is set to 1.

Example `set receive-equalization = yes`

Dependencies For a DS3-ATM slot card, set `receive-equalization` to `yes` for cable lengths above 450 ft. For an E3-ATM slot card, set `receive-equalization` to `yes` for cable lengths above 300 ft.

Location `DS3-ATM/{ any-shelf any-slot 0 }:line-config`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`

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 Consider the following:

- 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/"":ppp-options`

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/"":port-redirect-options

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 through 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/{ "" "" }

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 through 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/{ "" "" }

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/"":ip-options

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 one of the following settings:

- `yes` enables the TAOS unit to retrieve the login banner and list of Telnet hosts from RADIUS.
- `no` (the default) specifies that you must specify the banner and list of Telnet hosts in a local `terminal-server` profile.

Example `set remote-configuration = no`

Dependencies For `remote-configuration` to apply, you must enable terminal services and use RADIUS authentication.

Location `TERMINAL-SERVER:menu-mode-options`

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 one of the following settings:

- `yes` enables DHCP responses on the interface.
- `no` (the default) disables DHCP responses on the interface.

Example `set reply-enabled = yes`

Location `CONNECTION/"":dhcp-options`

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 Consider the following:

- You can set `reqd-state` by using the `device` or `slot` command.
- In a `slot-state` profile, setting `reqd-state` to `down-reqd-state` does not persist across system restarts.

Location `DEVICE-STATE/{ { any-shelf any-slot 0} 0}`
`SLOT-STATE/{ any-shelf any-slot 0 }`

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/{ { any-shelf any-slot 0 } 0 }:ospf CONNECTION/"":ip-options:ospf-options`

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 through 10. The default is 10.

Example `set retry-count = 10`

Dependencies For `retry-count` to apply, you must set `l2tp-mode` to `lac`.

Location `L2-TUNNEL-GLOBAL:l2tp-config`

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 through 100. The default is 10.

Example `set retry-limit = 25`

Location `ATMP`

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`

retry-timer-mode

Description Specifies the mode in which the Layer 2 Tunneling Protocol (L2TP) Control Channel Transport Layer retry timer operates.

Usage Specify one of the following values:

- `linear` (the default) specifies that the retransmit interval increases in linear mode.
- `exponential` specifies that the retransmit interval increases exponentially.

Example `set retry-timer-mode = exponential`

Location `L2-TUNNEL-GLOBAL:l2tp-config`

rip

Description Specifies Routing Information Protocol (RIP) behavior for a `connection` profile:

- In an `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 Internetwork Packet Exchange (IPX) RIP when the peer is a router.

Note The Internet Engineering Task Force (IETF) has voted to move RIP-v1 into the *historic* category, and its use is no longer recommended. You should upgrade all routers and hosts to RIP-v2. If you must maintain RIP-v1, Lucent Technologies recommends that you create a separate subnet, and place all RIP-v1 routers and hosts on that subnet.

Usage In an `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.

Setting	Description
routing-send-and-recv-v2	The TAOS unit both sends RIP-v2 routing updates and accepts any it receives for the connection.

In an 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/"":ip-options
CONNECTION/"":ipx-options

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 one of the following settings:

- yes (the default) enables RIP-v2 to use the multicast address (224.0.0.9) instead of the broadcast address for its updates.
- no disables the use of the multicast address for RIP updates. 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/{ { any-shelf any-slot 0 } 0 }

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 (the default) indicates type 1 metrics. A type 1 external metric is expressed in the same units as the link-state metric (interface cost).
- 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`

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 Internet Engineering Task Force (IETF) has voted to move RIP-v1 into the *historic* category, and its use is no longer recommended. You should upgrade all routers and hosts to RIP-v2. If you must maintain RIP-v1, Lucent Technologies recommends that you create a separate subnet, and place all RIP-v1 routers and hosts on that subnet.

Usage Specify one of the following settings:

Setting	Description
`routing-off` (the default)	The unit does not send routing updates, and ignores updates it receives for the connection.
`routing-send-only`	The unit sends RIP-v1 routing updates, but ignores updates it receives for the connection.
`routing-recv-only`	The unit does not send RIP-v1 routing updates, but accepts updates it receives for the connection.
`routing-send-and-recv`	The unit both sends RIP-v1 routing updates and accepts updates it receives for the connection.
`routing-send-only-v2`	The unit sends RIP-v2 routing updates, but ignores updates it receives for the connection.
`routing-recv-only-v2`	The unit does not send RIP-v2 routing updates, but accepts updates it receives for the connection.
`routing-send-and-recv-v2`	The unit both sends RIP-v2 routing updates and accepts updates it receives for the connection.

Example `set rip-mode = routing-send-only-v2`

Location `IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }`

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.
- For the `rip-policy` setting to apply, the system must support RIP-v1.

Example `set rip-policy = split-horzn`

Location `IP-GLOBAL`
`VROUTER/""`

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` through `255`. A value of `255` prevents the use of the route. Following are the default preferences for different types of routes:

- `0` (zero)—Connected routes
- `10`—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`

rip-queue-depth

Description Specifies the maximum size of the queue for Routing Information Protocol (RIP) packets.

Usage Specify the maximum number of packets from 0 through 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

rip-tag

Description Specifies a tag to associate with Routing Information Protocol (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

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 one of the following settings:

- yes (the default) 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, Routing Information Protocol (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/""

rlogin

Description Enables or disables the use of the `rlogin` command from the terminal-server interface.

Usage Specify one of the following settings:

- `yes` enables the use of the `rlogin` command.
- `no` (the default) 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 For `rlogin` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration:rlogin-options`

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 200ms 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 200ms wink time.
- `inc-w-400` specifies wink-wink signaling with a 400ms 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:

- For `robbed-bit-mode` to apply, you must set `signaling-mode` 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/{ any-shelf any-slot 0 }:line-interface`

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`

Dependencies For `route-address` to apply, you must set `type` to `route-filter`.

Location `FILTER/"":input-filters[n]:route-filter`
`FILTER/"":output-filters[n]:route-filter`

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/"":ip-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }`

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 For `route-mask` to apply, you must set `type` to `route-filter`.

Location `FILTER/"":input-filters[n]:route-filter`
`FILTER/"":output-filters[n]:route-filter`

route-reflector-client

Description Enables or disables a Border Gateway Protocol (BGP) peer as a route reflector client.

Usage Specify one of the following settings:

- yes enables a BGP peer as a route reflector client.
- no (the default) disables a BGP peer as a route reflector client.

Example `set route-reflector-client = yes`

Location BGP-PEER/""

router-id

Description Specifies the router ID for routed connections.

Usage Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example `set router-id = 10.9.8.7`

Location IP-GLOBAL

routing-metric

Description Assigns a Routing Information Protocol (RIP)-style metric to a route.

Usage Specify an integer from 1 through 15. The default is 7.

Example `set routing-metric = 1`

Location ANSWER-DEFAULTS:ip-answer
CONNECTION/"":ip-options

rt-fax-enable

Description Enables or disables T.38 fax call processing.

Usage Specify one of the following settings:

- 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 IP Device Control (IPDC) message from the signaling gateway.
- no (the default) 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/{ "" "" }:rt-fax-options

rtpqos-polling-enable

Description Specifies whether the unit generates periodic Real-Time Transport Protocol (RTP) quality of service (QoS) statistics.

Usage Specify one of the following values:

- `yes` specifies that the unit generates periodic requests for RTP QoS statistics.
- `no` (the default) specifies that the unit does not generate periodic requests for RTP QoS statistics.

Example `set rtpqos-polling-enable = yes`

Location `VOIP/{ "" "" }`

rule

Description Indicates a rule in a Border Gateway Protocol (BGP) policy on this TAOS unit. A BGP policy rule can be one of the following types:

- Acceptance policy rule—admits an IP prefix learned from a BGP peer into a BGP database on the TAOS unit for further consideration as a route.
- Injection policy rule—injects an IP prefix into the routing table that the TAOS unit uses to forward packets it receives to their ultimate destination.
- Advertisement policy rule—advertises an IP prefix that the TAOS unit learned from another peer to a BGP internal or external peer.

Usage The `rule` value is read-only. The default is null.

Example `rule[1] = "permit if prefix 194.194.194.0/24"`

Dependencies You define a rule by means of the `set rule` command.

Location `BGP-POLICY/""`

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 one of the following settings:

- `yes` disables descrambling of the 48-byte ATM cell payload in received cells.
- `no` (the default) 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/{ any-shelf any-slot 0 }:line-config`

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 through 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 slot cards. If you specify a value for a connection that does not use these slot cards, the system ignores the settings.

Location `CONNECTION/"":session-options`

rx-descramble-disabled

Description Enables or disables descrambling of the entire Asynchronous Transfer Mode (ATM) receive stream.

Usage Specify one of the following settings:

- `yes` disables descrambling of the entire ATM receive stream.
- `no` (the default) enables descrambling of the entire ATM receive stream.

Example `set rx-descramble-disabled = yes`

Dependencies Set `rx-descramble-disabled` to `yes` only if the transmitting switch has disabled the corresponding scramble function.

Location `OC3-ATM/{ any-shelf any-slot 0 }:line-config`

S

sap

Description Specifies Internetwork Packet Exchange (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 For `sap` to apply, the TAOS unit must route IPX for the connection or have IPX routing globally enabled.

Location `CONNECTION/"":ipx-options`

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 For `sap-filter` to apply, the TAOS unit must route Internetwork Packet Exchange (IPX) for the connection or have IPX routing globally enabled.

Location `CONNECTION/"":ipx-options`

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 become inactive 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

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

screen-length

Description Specifies the number of lines displayed in the command-line window. (For the values to take effect, the user must log in again.)

Usage Specify a number from 24 through 999. The default is 24.

Example `set screen-length = 68`

Location USER/""

screen-width

Description Specifies the number of characters allowed on a command line or terminal-server banner.

Usage Specify an integer from 80 through 255. The default is 80.

Example `set screen-width = 100`

Location USER/""

See Also

sdsl

Description *Not supported.*

sdsl70d

Description *Not supported.*

sdsl70v

Description *Not supported.*

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 one of the following settings:

- `yes` specifies that the unit establishes HDLC-NRM or Visa terminal connections.
- `no` (the default) specifies that the unit establishes HDLC-NRM or Visa terminal connections but drops the data.

Example `set sdtn-packets-server = yes`

Location `CONNECTION/""`

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/""`

second

Description Specifies the current second.

Usage The `second` parameter is read-only.

Example `second = 25`

Location `TIMEDATE:time`

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/""`

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:

- For `secondary-ip-address` to apply, `enabled` must be set to `yes` in the `ss7-gateway` profile.
- 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 Transmission Control Protocol (TCP) port values can specify two Ethernet interfaces of the same signaling gateway.

Location `SS7-GATEWAY`

secondary-tcp-port

Description Specifies the 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:

- For `secondary-ip-port` to apply, `enabled` must be set to `yes` in the `ss7-gateway` profile.
- 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 Transmission Control Protocol (TCP) port values can specify two Ethernet interfaces of the same signaling gateway.

Location `SS7-GATEWAY`

secondary-tunnel-server

Description The `secondary-tunnel-server` parameter has different uses, depending on your configuration:

- In an Ascend Tunnel Management Protocol (ATMP) configuration, `secondary-tunnel-server` specifies the IP address or hostname of the secondary Home Agent. The TAOS unit initiates a connection to the host after the Foreign Agent receives an error code in an ATMP Register Reply or Challenge Request message.
- For a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnel, `secondary-tunnel-server` specifies the secondary tunnel server. The TAOS unit initiates a connection to the host after a connection attempt to `primary-tunnel-server` times out.

Usage Specify an IP address in dotted decimal notation, or a symbolic hostname containing up to 253 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 User Datagram Protocol (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 `set secondary-tunnel-server = 10.11.22.33:8877`

Dependencies Consider the following:

- For `secondary-tunnel-server` to apply, you must set `profile-type` to `mobile-client`.
- 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/"":tunnel-options`

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/"":visa2-options`

seconds-history

Description Specifies the number of seconds to use as the basis for calculating average line utilization (ALU). When the ALU exceeds or falls below the `target-utilization percentage` for a specified number of seconds, the TAOS unit adds or subtracts bandwidth.

Usage Specify an integer from `1` through `300`. The default is `15`.

Example `set seconds-history = 60`

Dependencies 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/"":mpp-options`

security-enabled

Description Specifies whether the TAOS unit traps security events and sends a trap 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 one of the following settings:

- yes (the default) 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/""

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 For security-for-direct-access to apply, you must set direct-access to yes.

Location TERMINAL-SERVER:dialout-configuration

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 Simple Network Management Protocol version 3 user-based security model (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 `auth-priv` to apply, you must set the `priv-protocol` and `priv-password` parameters in the `snmpv3-usm-user` profile.

Location `SNMP`
`SNMPV3-TARGET-PARAM/""`
`VACM-ACCESS/{"" "" v1 none }:access-properties`

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`

security-model

Description Specifies the security model to use when generating Simple Network Management Protocol (SNMP) messages.

Usage Specify one of the following values:

- v1 (the default) specifies the SNMP version 1 (SNMPv1) security model.
- V3-usm specifies the SNMP version 3 user-based security model (SNMPv3 USM). For SNMPv3 notification or view-based access control model (VACM) 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/""
VACM-ACCESS/{"" "" v1 none }: access-properties
VACM-SECURITY-GROUP/{ v1 "" }:security-properties

security-name

Description Specifies a security name that identifies the user on whose behalf Simple Network Management Protocol version 3 user-based security model (SNMPv3 USM) messages are generated.

Usage Specify up to 22 characters. The default is null.

Example `set security-name = newuser`

Dependencies For security-name to apply, you must set security-model to v3-usm.

Location SNMPV3-TARGET-PARAM/""
VACM-SECURITY-GROUP/{ v1 "" }: security-properties

sel

Description Specifies the selector field of the domain-specific part (DSP) of an Asynchronous Transfer Mode (ATM) end system address (AESA)—a hexadecimal number that is not used for 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/{ { any-shelf any-slot 0 } 0 }:svc-options:
atm-address:aesa-address:dsp-portion
CONNECTION/"":atm-options:svc-options:incoming-caller-addr:aesa-address:
dsp-portion
CONNECTION/"":atm-options:svc-options:outgoing-called-addr:aesa-address:
dsp-portion

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 through 65000. The default is 10000.

Example `set selection-timeout = 5000`

Location TRANSACTION-SERVER

selectools-enabled

Description Indicates whether Selectools™ software is enabled.

Usage The `selectools-enabled` value is read-only and can have one of the following values:

- `yes` indicates that the Selectools™ software is enabled.
- `no` indicates that Selectools™ software is disabled.

Example `selectools-enabled = yes`

Location BASE

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 PPP (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.
`chap-ppp-auth`	The connection requests Challenge Handshake Authentication Protocol (CHAP). The remote end does not send its password in the clear. A message-digest algorithm 5 (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/"":ppp-options`

senddisc-val

Description Specifies the number of seconds the TAOS unit waits before sending an Integrated Services Digital Network (ISDN) disconnect to the switch.

Usage Specify an integer. The default is `0` (zero).

Example `set sendDisc-val = 10`

Location `T1/{ any-shelf any-slot 0 }:line-interface`

send-icmp-dest-unreachable

Description Specifies whether the unit sends Internet Control Message Protocol (ICMP) destination-unreachable packets.

Usage Specify one of the following settings:

- `yes` (the default) 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 Voice over IP (VoIP) environments. Doing so in a non-VoIP environment can cause IPv4 routers to fail to perform essential activities, such as path maximum transmission unit (PMTU) discovery.
- When operating under heavy call volumes, setting `send-icmp-dest-unreachable` to `yes` reduces the load placed on the shelf controller.
- For VoIP applications, User Datagram Protocol (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`

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/"":ppp-options`

sequential-call-enable

Description Specifies whether callers who must enter a personal identification number (PIN) to authenticate MultiVoice® calls can dial subsequent Voice over IP (VoIP) calls without reentering the PIN.

Usage Specify one of the following settings:

- `yes` (the default) 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-call-enable = no`

Dependencies Consider the following:

- If you set `sequential-call-enable` to `no`, the unit must be configured for two-stage dialing and PIN collection (`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/{ "" "" }`

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/{ any-shelf any-slot 0 }`

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`

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 Consider the following:

- L2F does not support the `server-auth-id` setting in a `tunnel-server` profile.
- `server-auth-id` is currently ignored if specified in a `connection` profile.

Location `CONNECTION/"":tunnel-options`
`TUNNEL-SERVER/""`

server-endpoint

Description Specifies the Domain Name System (DNS) hostname or dotted IP address of the Layer 2 Tunneling Protocol (L2TP) network server (LNS), Point-to-Point Tunneling Protocol (PPTP) network server (PNS) endpoint, or Layer 2 Forwarding (L2F) endpoint.

Usage Specify a symbolic hostname of up to 253 characters or an IP address in dotted decimal notation. The default is null.

Example **`set server-endpoint = 200.40.50.2`**

Dependencies 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/""

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, t`server-type` specifies whether to include or exclude advertisements for the server in SAP response packets. If the server is on the remote Internetwork Packet Exchange (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

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/""

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 one of the following settings:

- `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` (the default) 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

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/""`

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 Consider the following:

- 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/""`
`IPX-SAP-FILTER/"":input-ipx-sap-filters`
`IPX-SAP-FILTER/"":output-ipx-sap-filters`

service

Description In the `immediate-mode-options` subprofile, enables or disables immediate mode and, if immediate mode is enabled, specifies the immediate service type.

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 Transmission Control Protocol (TCP) connection.
- `rlogin` specifies immediate `rlogin` service.

Example `set service = rlogin`

Dependencies For `service to` apply, you must enable terminal services.

Location `TERMINAL-SERVER:immediate-mode-options`

service-1
service-2
service-3
service-4

Description Specifies the type of service to use for the host specified by `host-1`, `host-2`, `host-3`, or `host-4`.

Usage Specify one of the following values:

- `telnet` indicates Telnet service.
- `rawtcp` indicates raw Transmission Control Protocol (TCP) service.
- `rlogin` indicates `rlogin` service.
- `ppp` indicates Point-to-Point Protocol (PPP) service.

Example `set service-1 = rlogin`

Location `TERMINAL-SERVER:menu-mode-options`

ses-adsl-cap-down-rate

Description *Not supported.*

ses-adsl-cap-up-rate

Description *Not supported.*

ses-adsl-dmt-down-rate

Description *Not supported.*

ses-adsl-dmt-up-rate

Description *Not supported.*

ses-sdsl-rate

Description *Not supported.*

sessionid-base

Description Specifies the base number that the TAOS unit uses for generating a unique ID for each session.

Usage Specify an integer from 1 through 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, nonvolatile RAM (NVRAM), session IDs might be duplicated.

Dependencies Consider the following:

- 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 restart. 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.
- You can 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

shared-prof

Description Specifies whether multiple incoming calls can share a connection profile.

Usage Specify one of the following settings:

- yes specifies that the TAOS unit allows more than one caller to share the same profile, provided that no IP address conflicts result.
- no (the default) 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 shared-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

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 Consider the following:

- An L2F tunnel can be authenticated with the same shared secret at both ends.
- 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/""`

share-global-pool

Description Specifies whether the virtual router (Vrouter) can share the address pools defined in an `ip-global` profile.

Usage Specify one of the following values:

- `yes` (the default) specifies that the Vrouter can share the address pools.
- `no` speciifes that the Vrouter cannot share the address pools.

Example `set share-global-pool = no`

Location `VROUTER/""`

shelf

Description Specifies the shelf in which an item resides.

Usage The `shelf` setting is always 1.

Example `shelf = 1`

Location `ADMIN-STATE-PHYS-IF/{ any-shelf any-slot 0 }:device-address`
`DEVICE-STATE/{ { any-shelf any-slot 0 } 0 }:device-address`
`DS3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info`
`DS3-ATM/{ any-shelf any-slot 0 }:physical-address`
`E1/{ any-shelf any-slot 0 }: line-interface: channel-config[`*n*`]:`
`call-route-info`
`E1/{ any-shelf any-slot 0 }:physical-address`
`E3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info`
`E3-ATM/{ any-shelf any-slot 0 }:physical-address`
`E3-ATM-STAT/{ any-shelf any-slot 0 }:physical-address`
`LAN-MODEM/{ any-shelf any-slot 0 }:physical-address`

```
OC3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info
OC3-ATM/{ any-shelf any-slot 0 }:physical-address
SERIAL/{ any-shelf any-slot 0 }:physical-address
SWAN/{ any-shelf any-slot 0 }:line-config:call-route-info
SWAN/{ any-shelf any-slot 0 }:physical-address
T1/{ any-shelf any-slot 0 }: line-interface: channel-config[n]:
call-route-info
T1/{ any-shelf any-slot 0 }:physical-address
T1-STAT/{ any-shelf any-slot 0 }:physical-address
T3/{ any-shelf any-slot 0 }:physical-address
T3-STAT/{ any-shelf any-slot 0 }:physical-address
```

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`

shutdown-metric

Description Specifies a number from 0 through 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 through 255. The default is 14.

Example **`set shutdown-metric = 15`**

Location `TRANSACTION-SERVER`

side-select

Description Indicates which link is chosen for the Peripheral Control Timing Facilities Interface (PCTFI).

Usage The `side-select` setting is read-only and can have one of the following values:

- `side-0` indicates that the switch has selected side 0.
- `side-1` indicates that the switch has selected side 1.

Example `side-select = side-1`

Location `PCTFI-STAT/{ any-shelf any-slot 0 }`

signal-degrade

Description Indicates whether the STM link is detecting more than the degrade threshold number of BIP errors.

Usage The `signal-degrade` value is read-only and can have one of the following settings:

- `true` indicates that the STM link is detecting more than the degrade threshold number of BIP errors.
- `false` indicates that the STM link is not detecting more than the degrade threshold number of BIP errors.

Example `signal-degrade = false`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }`
`STM-STAT/{ any-shelf any-slot 0 }`

signal-fail

Description Indicates whether the STM link is detecting more than the fail threshold number of BIP errors.

Usage The `signal-fail` value is read-only and can have one of the following settings:

- `true` indicates that the STM link is detecting more than the fail threshold number of BIP errors.
- `false` indicates that the STM link is not detecting more than the fail threshold number of BIP errors.

Example `signal-fail = false`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }`
`STM-STAT/{ any-shelf any-slot 0 }`

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 Integrated Services Digital Network (ISDN) signaling on the D channel.
- `isdn-nfas` specifies non-facility associated signaling (NFAS). NFAS enables a group of T1 lines on the same slot 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.
- `tunneled-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, Primary Rate Interface (PRI) tunneling is enabled with the next Voice over IP (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 outbound 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 outbound switched telephone network by sending call signaling data in feature group C (FGC) 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 outbound 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 outbound switched telephone network by sending call-signaling data in FGD format.
- `tunneled-pri-signaling` specifies that all layer 3 Q.931 messages are tunneled to the gateway configured in the `ss7-gateway` profile.

For an E1 line, specify one of the following values:

- `isdn` specifies ISDN signaling on the D channel.
- `dtmf-r2-signaling` specifies dual-tone multifrequency (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 dedicated line.

- `e1-dpnss-signaling` specifies Digital Private Network Signaling System (DPNSS) or Digital Access Signaling System 2 (DASS2) 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.
- `e1-vietnam-signaling` specifies R2 signaling for Viet Nam.

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 IP Device Control (IPDC) signal processing is enabled for the TAOS unit. The `base` profile should contain the setting `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` through `3000`) for the `t1-inter-digit-timeout` setting improves call setup times. Assigning a higher value (`3001` through `6000`) improves DTMF detection.
- DTMF R2 detection is supported only when R2 signal processing is enabled for a TAOS unit.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

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. IP Device Control (IPDC) voice announcements and 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 5.3kbps 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/{ "" "" }`

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/{ "" "" }`

silent-mode

Description Specifies whether the TAOS unit suppresses status messages when an interactive terminal-server connection is established.

Usage Specify one of the following settings:

- `yes` specifies that the TAOS unit suppresses status messages when an interactive terminal-server connection is established.
- `no` (the default) specifies that the TAOS unit sends all status messages when an interactive terminal-server connection is established.

Example `set silent-mode = yes`

Dependencies For `silent-mode` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER: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 one of the following settings:

- `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` (the default) 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 private branch exchange (PBX) can relay dual-tone multifrequency (DTMF) signals to the MultiVoice® gateway.
- You are using T1 Primary Rate Interface (PRI) trunks.
- You have enabled DNIS on the TAOS unit.

Location `VOIP/{ "" "" }`

single-file-incoming

Description Specifies whether the TAOS unit treats incoming calls as a single-file list, or handles them in parallel.

Usage Specify one of the following settings:

- `yes` (the default) 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`

slip

Description Enables or disables the use of the terminal-server `slip` command.

Usage Specify one of the following settings:

- `yes` enables a user to begin Serial Line Internet Protocol (SLIP) sessions from the terminal-server interface.
- `no` (the default) disables a user from beginning SLIP from the terminal-server interface.

Example `set slip = yes`

Dependencies For `slip` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:slip-mode-configuration`

slip-bootp

Description Specifies whether the TAOS unit responds to BOOTP within Serial Line Internet Protocol (SLIP) sessions.

Usage Specify one of the following settings:

- `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` (the default) 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 For `slip-bootp` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:slip-mode-configuration`

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 Specify an integer.

Example `set slot = 10`

Location ADMIN-STATE-PHYS-IF/{ any-shelf any-slot 0 }:device-address
DEVICE-STATE/{ { any-shelf any-slot 0 } 0 }:device-address
DS3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info
DS3-ATM/{ any-shelf any-slot 0 }:physical-address
E1/{ any-shelf any-slot 0 }: line-interface: channel-config[*n*]:
call-route-info
E1/{ any-shelf any-slot 0 }:physical-address
E3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info
E3-ATM/{ any-shelf any-slot 0 }:physical-address
E3-ATM-STAT/{ any-shelf any-slot 0 }:physical-address
LAN-MODEM/{ any-shelf any-slot 0 }:physical-address
OC3-ATM/{ any-shelf any-slot 0 }:line-config:call-route-info
OC3-ATM/{ any-shelf any-slot 0 }:physical-address
SERIAL/{ any-shelf any-slot 0 }:physical-address
SWAN/{ any-shelf any-slot 0 }:line-config:call-route-info
SWAN/{ any-shelf any-slot 0 }:physical-address
T1/{ any-shelf any-slot 0 }: line-interface: channel-config[*n*]:
call-route-info
T1/{ any-shelf any-slot 0 }:physical-address
T1-STAT/{ any-shelf any-slot 0 }:physical-address
T3/{ any-shelf any-slot 0 }:physical-address
T3-STAT/{ any-shelf any-slot 0 }:physical-address

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.

Example `set slot-address slot = slot-8`

Location SLOT-INFO/{ any-shelf any-slot 0 }
SLOT-STATE/{ any-shelf any-slot 0 }
SLOT-TYPE/{ any-shelf any-slot 0 }

slot-enabled

Description Specifies whether the TAOS unit traps slot events and sends a trap to the Simple Network Management Protocol (SNMP) manager when the `SlotProfileChange` event occurs.

Usage Specify one of the following settings:

- `yes` (the default) 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/""`

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 one of the following settings:

- `yes` (the default) 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/""`

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 slot card is installed.
`unknown`	The software does not recognize the slot card.
`shelf-controller`	Shelf controller.
`router-card`	Standalone router card.
`8t1-card`	T1 slot card.
`8e1-card`	E1 slot card.
`4swan-card`	Serial WAN (SWAN) slot card.
`10-unchan-t1-card`	Unchannelized T1 FrameLine slot card.
`10-unchan-e1-card`	Unchannelized E1 FrameLine slot card.

Value	Specifies
analog-modem2-card	Analog Modem slot card.
csmx-card	Series56 II Digital Modem slot card.
uds3-card	Unchannelized DS3 slot card.
ds3-atm-card	DS3-ATM slot card.
4ether2-card	Ethernet-2 slot card.
hdlc2-card	Hybrid Access II slot card.
madd-card	48-port MultiDSP slot card.
oc3-atm-card	OC3-ATM (fiber) slot card.
ether3-card	Ethernet-3 slot card.
hdlc2ec-card	Hybrid Access III slot card.
stm0-card	STM-0 slot card.
ds3-atm2-card	DS3-ATM2 slot card.
madd2-card	96-port MultiDSP slot card.
t3-card	Channelized T3 slot 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-PHYS-IF/{ any-shelf any-slot 0 }`
`SLOT-TYPE/{ any-shelf any-slot 0 }`

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-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 restarted 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 restart.

Location `ADMIN-STATE-PERM-IF/""`
`ADMIN-STATE-PHYS-IF/{ any-shelf any-slot 0 }`

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 Simple Network Management Protocol version 1 (SNMPv1) and SNMP version 3 (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
SNMP-MANAGER/""

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 through 5000. The default is 2000.

Example `set snrm-response-timeout = 1000`

Location CONNECTION/"":hdlc-nrm-options

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 time-out.

Usage Specify a number from 0 through 255. The default is 2.

Example `set snrm-retry-counter = 5`

Location CONNECTION/"":hdlc-nrm-options

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/{ any-shelf any-slot 0 }

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 = 10.0

Location SLOT-INFO/{ any-shelf any-slot 0 }

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/{ any-shelf any-slot 0 }

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/{ any-shelf any-slot 0 }

sonet-far-end-line-coding-violations

Description Indicates the number of bit-interleaved parity errors at the far-end device's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

Usage The sonet-far-end-line-coding-violations setting is read-only.

Example sonet-far-end-line-coding-violations = 0

Location STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring
STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring

sonet-far-end-line-errored-seconds

Description Indicates the number of errored seconds at the far-end device's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

Usage The `sonet-far-end-line-errored-seconds` setting is read-only.

Example `sonet-far-end-line-errored-seconds = 0`

Location `STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-far-end-line-severely-errored-seconds

Description Indicates the number of severely errored seconds at the far-end device's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

Usage The `sonet-far-end-line-severely-errored-seconds` setting is read-only.

Example `sonet-far-end-line-severely-errored-seconds = 0`

Location `STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-far-end-line-unavailable-seconds

Description Indicates the number of unavailable seconds at the far-end device's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

Usage The `sonet-far-end-line-unavailable-seconds` setting is read-only.

Example `sonet-far-end-line-unavailable-seconds = 0`

Location `STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-far-end-path-coding-violations

Description Indicates the number of bit-interleaved parity errors at the far-end device's path layer. A Synchronous Optical Network (SONET) path is an end-to-end circuit.

Usage The `sonet-far-end-path-coding-violations` setting is read-only.

Example `sonet-far-end-path-coding-violations = 0`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }:`
`interval-performance-monitoring`
`STM-PATH-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-far-end-path-errored-seconds

Description Indicates the number of errored seconds at the far-end device's path layer. A Synchronous Optical Network (SONET) path is an end-to-end circuit.

Usage The `sonet-far-end-path-errored-seconds` setting is read-only.

Example `sonet-far-end-path-errored-seconds = 0`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-PATH-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-far-end-path-severely-errored-seconds

Description Indicates the number of severely errored seconds at the far-end device's path layer. A Synchronous Optical Network (SONET) path is an end-to-end circuit.

Usage The `sonet-far-end-path-severely-errored-seconds` setting is read-only.

Example `sonet-far-end-path-severely-errored-seconds = 0`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-PATH-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-far-end-path-unavailable-seconds

Description Indicates the number of unavailable seconds at the far-end device's path layer. A Synchronous Optical Network (SONET) path is an end-to-end circuit.

Usage The `sonet-far-end-path-unavailable-seconds` setting is read-only.

Example `sonet-far-end-path-unavailable-seconds = 0`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-PATH-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-line-coding-violations

Description Indicates the number of bit-interleaved parity errors at the unit's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

Usage The `sonet-line-coding-violations` setting is read-only.

Example `sonet-line-coding-violations = 0`

Location `STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-line-errored-seconds

Description Indicates the number of errored seconds at the unit's line layer. A SONET line consists of one or more sections.

Usage The `sonet-line-errored-seconds` setting is read-only.

Example `sonet-line-errored-seconds = 0`

Location `STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-line-severely-errored-seconds

Description Indicates the number of severely errored seconds at the unit's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

Usage The `sonet-line-severely-errored-seconds` setting is read-only.

Example `sonet-line-severely-errored-seconds = 0`

Location `STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-line-unavailable-seconds

Description Indicates the number of unavailable seconds at the unit's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

Usage The `sonet-line-unavailable-seconds` setting is read-only.

Example `sonet-line-unavailable-seconds = 0`

Location `STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-path-coding-violations

Description Indicates the number of bit-interleaved parity errors at the unit's path layer. A Synchronous Optical Network (SONET) path is an end-to-end circuit.

Usage The `sonet-path-coding-violations` setting is read-only.

Example `sonet-path-coding-violations = 0`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }:`
`interval-performance-monitoring`
`STM-PATH-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-path-errored-seconds

Description Indicates the number of errored seconds at the unit's path layer. A Synchronous Optical Network (SONET) path is an end-to-end circuit.

Usage The `sonet-path-errored-seconds` setting is read-only.

Example `sonet-path-errored-seconds = 0`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-PATH-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-path-severely-errored-seconds

Description Indicates the number of severely errored seconds at the unit's path layer. A Synchronous Optical Network (SONET) path is an end-to-end circuit.

Usage The `sonet-path-severely-errored-seconds` setting is read-only.

Example `sonet-path-severely-errored-seconds = 0`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-PATH-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-path-unavailable-seconds

Description Indicates the number of unavailable seconds at the unit's path layer. A Synchronous Optical Network (SONET) path is an end-to-end circuit.

Usage The `sonet-path-unavailable-seconds` setting is read-only.

Example `sonet-path-unavailable-seconds = 0`

Location `STM-PATH-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-PATH-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-section-coding-violations

Description Indicates the number of bit-interleaved parity errors at the unit's section layer. A Synchronous Optical Network (SONET) section is a single run of cable.

Usage The `sonet-section-coding-violations` setting is read-only.

Example `sonet-section-coding-violations = 0`

Location `STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring`
`STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring`

sonet-section-errored-seconds

Description Indicates the number of errored seconds at the unit's section layer. A Synchronous Optical Network (SONET) section is a single run of cable.

Usage The sonet-section-errored-seconds setting is read-only.

Example sonet-section-errored-seconds = 0

Location STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring
STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring

sonet-section-severely-errored-framing-seconds

Description Indicates the number of severely errored framing seconds at the unit's section layer. A Synchronous Optical Network (SONET) section is a single run of cable.

Usage The sonet-section-severely-errored-framing-seconds setting is read-only.

Example sonet-section-severely-errored-framing-seconds = 0

Location STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring
STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring

sonet-section-severely-errored-seconds

Description Indicates the number of severely errored seconds at the unit's section layer. A Synchronous Optical Network (SONET) section is a single run of cable.

Usage The sonet-section-severely-errored-seconds setting is read-only.

Example sonet-section-severely-errored-seconds = 0

Location STM-STAT/{ any-shelf any-slot 0 }:interval-performance-monitoring
STM-STAT/{ any-shelf any-slot 0 }:performance-monitoring

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).

Usage Specify an IP address in dotted decimal notation. 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 For source-address to apply in a filter profile, type must be set to ip-filter or tos-filter.

Location FILTER/"":input-filters[*n*]:ip-filter
FILTER/"":output-filters[*n*]:ip-filter
FILTER/"":input-filters[*n*]:tos-filter
FILTER/"":output-filters[*n*]:tos-filter

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.

Usage Specify a value in dotted decimal notation. The default is `0.0.0.0`.

Example `set source-address-mask = 255.255.255.224`

Dependencies Consider the following:

- 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.
- For `source-address-mask` to apply in a `filter` profile, `type` must be set to `ip-filter` or `tos-filter`.

Location `FILTER/"":input-filters[`*n*`]:ip-filter`
`FILTER/"":output-filters[`*n*`]:ip-filter`
`FILTER/"":input-filters[`*n*`]:tos-filter`
`FILTER/"":output-filters[`*n*`]:tos-filter`

source-ip-check

Description Enables or disables antispoofing for the session.

Usage Specify one of the following settings:

- `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` (the default) disables antispoofing for the session.

Example `set source-ip-check = yes`

Location `CONNECTION/"":ip-options`

source-port

Description Specifies a value to compare with the source-port field in a packet.

Usage Specify a number from 0 through 65535. The default is 0 (zero), which matches any port.

Example `set source-port = 25`

Dependencies Consider the following:

- For source-port to apply, you must set type to ip-filter or tos-filter.
- Only Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets have source-port fields.
- The src-port-cmp setting specifies the type of comparison the TAOS unit makes.

Location FILTER/"":input-filters[*n*]:ip-filter
FILTER/"":output-filters[*n*]:ip-filter
FILTER/"":input-filters[*n*]:tos-filter
FILTER/"":output-filters[*n*]:tos-filter

split-code-dot-user-enabled

Description Specifies whether the system can split usernames longer than 5 characters under cache-token authentication.

Usage Specify one of the following settings:

- 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 personal identification number (PIN) and 6-digit ACE token code.
- no (the default) specifies that the system cannot split usernames.

Example `set split-code-dot-user-enabled = yes`

Location CONNECTION/"":ppp-options

src-net-address

Description Specifies an Internetwork Packet Exchange (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 For src-net-address to apply, you must set type to ipx-filter.

Location FILTER/"":input-filters[*n*]:ipx-filter
FILTER/"":output-filters[*n*]:ipx-filter

src-node-address

Description Specifies an Internetwork Packet Exchange (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 For src-node-address to apply, you must set type to ipx-filter.

Location FILTER/"":input-filters[*n*]:ipx-filter
FILTER/"":output-filters[*n*]:ipx-filter

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 Consider the following:

- For src-port-cmp to apply, you must set type to ip-filter or tos-filter.
- You can filter only Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets with the src-port-cmp setting because only TCP and UDP packets contain source ports.

Location FILTER/"":input-filters[*n*]:ip-filter
FILTER/"":output-filters[*n*]:ip-filter
FILTER/"":input-filters[*n*]:tos-filter
FILTER/"":output-filters[*n*]:tos-filter

src-socket

Description Specifies an Internetwork Packet Exchange (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 For `src-socket` to apply, you must set `type` to `ipx-filter`.

Location `FILTER/"":input-filters[n]:ipx-filter`
`FILTER/"":output-filters[n]:ipx-filter`

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/"":input-filters[n]:ipx-filter`
`FILTER/"":output-filters[n]:ipx-filter`

ss7voip-call-persistence

Description Specifies whether a Voice over IP (VoIP) call route persists across IP Device Control (IPDC) requests for a given call, until the call is released.

Usage Specify one of the following values:

- `yes` specifies that a VoIP call route persists across IPDC requests for a given call.
- `no` (the default) specifies that VoIP call persistence is disabled.

Example `set ss7voip-call-persistence = yes`

Location `VOIP/{ "" "" }`

start-with-menus

Description Determines whether the terminal server presents a menu interface for an interactive user initiating a connection.

Usage Specify one of the following settings:

- `yes` specifies that the terminal server starts user logins in menu mode.
- `no` (the default) specifies that the terminal server starts user logins in command mode.

Example `set start-with-menus = yes`

Dependencies For `start-with-menus` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:menu-mode-options`

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` through `255`. A value of `255` prevents the use of the route. Following are the default preferences for different types of routes:

- `0` (zero)—Connected routes
- `10`—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`

static-route-redist-policy

Description Specifies the policy containing the static routes for which the TAOS unit automatically creates Border Gateway Protocol (BGP) summarizations.

Usage Specify a single policy name or the keyword `all`. The `all` value specifies that the unit automatically creates BGP summarizations for all static routes. The default is null.

Example `set static-route-redist-policy = all`

Location `BGP-GLOBAL`

station

Description The station parameter has different uses, depending on the profile:

- In a connection profile, station specifies the name of the remote device that communicates with the TAOS unit.
- In the admin-state-perm-if profile, station indicates the name of a dedicated 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/""

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.

Location CONNECTION/"":hdlc-nrm-options

status-change-trap-enable

Description Specifies whether the unit generates a Simple Network Management Protocol (SNMP) trap when a T1 line changes state.

Usage Specify one of the following values:

- yes specifies that the unit generates the trap.
- no (the default) specifies that the unit does not generate the trap.

Example `set status-change-trap-enable = yes`

Location DS3-ATM/{ any-shelf any-slot 0 }:line-config
E1/{ any-shelf any-slot 0 }:line-interface
T1/{ any-shelf any-slot 0 }:line-interface
UDS3/{ any-shelf any-slot 0 }:line-config

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 through 993. The default is 18.

Example **set status-length = 60**

Dependencies status-length must be less than screen-length by at least six lines.

Location USER/""

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/""

sub-as

Description Specifies the autonomous system number within a confederation.

Usage Specify a number from 0 through 65535. The default is 0 (zero), which specifies no autonomous system.

Example **set sub-as = 5**

Location BGP-GLOBAL

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 through 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/"":mpp-options

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 64 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

substitute-send-name

Description Specifies the name of the Point-to-Point Protocol (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 Consider the following:

- Because bidirectional Challenge Handshake Authentication Protocol (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

summarization-policy

Description Specifies the Border Gateway Protocol (BGP) policy to be used for summarization.

Usage Specify a text string. The default is `all`, which specifies that the local preferences, multiexit discriminators, and community names associated with the policy are set to their default values of 0 (zero).

Example `set summarization-policy = policy1`

Dependencies Consider the following:

- You configure a BGP policy by using the `set rule` command. If you specify an invalid policy for `summarization-policy` or specify the null value, no local preferences, multiexit discriminators, or community names are set and the following error message is displayed:

  ```
  Not redistributed! Improper summarization policy.
  ```

- Using the `set rule` command, you can specify local preferences, multiexit discriminators, and community names. Any other options you specify using the `set rule` command are ignored for purposes of BGP summarization.
- If you make changes to the policy specified by `summarization-policy` after writing the `bgp-summarization` profile, your changes do not take effect until you use the `bgp restart` command, restart the unit, or write the `bgp-summarization` profile again.
- The `bgp-summarization` profile is indexed by a prefix derived from its IP address and subnet mask. Therefore, if `two bgp-summarization` profiles have different IP addresses, the effective prefix that results from applying the subnet mask to the IP address might be the same. If so, the following error message is displayed:

  ```
  Another summarization profile has the same effective prefix.
  ```

- The `bgp-summarization` profile does not support multiple communities. If you specify multiple communities in a policy rule and attempt to use them for the summarization policy, only the first community specified by the rule is used. The rest are ignored.

Location `BGP-SUMMARIZATION/{ 0.0.0.0/0 }`

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 one of the following settings:

- `yes` (the default) 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 parameter does not apply if RIP-v2 is in use or if RIP is turned off.

Location IP-GLOBAL
VROUTER/""

suppress-endpoint-discriminator

Description Enable/disable suppression, by a TAOS unit operating as a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC), of the end point discriminator in the L2TP Incoming Call Connected (ICCN) message sent to the L2TP network server (LNS), in the absence of the ICCN Link Control Protocol (LCP) option.

Usage Specify one of the following values:

- yes specifies that, in the absence of a maximum reconstructed receive unit (MRRU) LCP option, the TAOS unit suppresses the end point discriminator from the LCP attribute-value pairs (AVPs) sent to the LNS.
- no (the default) specifies that the TAOS unit does not suppress the end point discriminator from the LCP AVPs sent to the LNS.

Example `set suppress-endpoint-discriminator = yes`

Location L2-TUNNEL-GLOBAL:l2tp-config

suppress-host-routes

Description Specifies whether the TAOS unit advertises host routes in each update, which can cause excessive routing overhead:

Usage Specify one of the following settings:

- yes specifies that host routes are suppressed.
- no (the default) specifies that host routes are advertised.

Example `set suppress-host-routes = yes`

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

suspect-access-resource-enabled

Description Specifies that whenever a terminating modem, installed MultiDSP slot card, or installed Hybrid Access slot 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 one of the following settings:

- `yes` directs the TAOS unit to send a trap when a terminating modem, installed MultiDSP slot card, or installed Hybrid Access slot card has received four or more calls for which it could not establish a connection.
- `no` (the default) 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/""`

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/{ { any-shelf any-slot 0 } 0 }:svc-options:atm-address`
`CONNECTION/"":atm-options:svc-options:incoming-caller-addr`
`CONNECTION/"":atm-options:svc-options:outgoing-called-addr`

svc-enabled

Description Specifies whether the system accepts incoming Asynchronous Transfer Mode (ATM) switched virtual circuit (SVC) calls.

Usage Specify one of the following settings:

- `yes` specifies that the system accepts ATM SVC calls.
- `no` (the default) specifies that the system does not accept ATM SVC calls.

Example `set svc-enabled = yes`

Location `ANSWER-DEFAULTS:atm-answer`

swan

Description Specifies the action to take when the code image for a Serial WAN (SWAN) slot card is present in a `tar` file.

Usage Specify one of the following settings:

- `auto` (the default) causes the system to load images for slot cards that are installed in the TAOS unit, and to skip images for slot cards that are not installed.
- `load` causes the system to load the image, even if no slot card of that type is installed.
- `skip` causes the system to skip the image, even if a slot card of that type is installed.

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

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 56Kbps is available.
`56k-restricted`	The TAOS unit sets up a data call with an explicit request for 56Kbps 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 56Kbps of the data channel. `56k-clear` is a common setting for T1 Primary Rate Interface (PRI) lines.
`64k-restricted`	The TAOS unit sets up a data call with an explicit request for 64Kbps restricted data transfer. The call must be set up as a data call at a rate of 64Kbps on an AMI-encoded line. With each transmission, a binary 1 is inserted in the least significant bit position.
`64k-clear`	The TAOS unit sets up a data call that uses the full 64Kbps bandwidth of the data channel.

Value	Specifies
`384k-restricted`	The TAOS unit sets up a data call that connects to Multi-Rate or GlobanD data services at 384Kbps.
`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 384Kbps 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 1536Kbps. 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 dedicated connection is in use, `switched-call-type` does not apply.
- If a T1 line is set for extended superframe format/bipolar 8-zero substitution (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 slot card, the call automatically connects at 14,400bps or 28,800bps, regardless of the setting of `switched-call-type`.

Location `FRAME-RELAY/""`

switched-enabled

Description Indicates whether the unit can make switched calls.

Usage The `switched-enabled` value is read-only and can have one of the following settings:

- `yes` indicates that the unit can make switched calls.
- `no` indicates that the unit can use only dedicated links.

Example `switched-enabled = yes`

Location `BASE`

switch-type

Description Specifies the type of network switch that provides Integrated Services Digital Network (ISDN) service.

Usage For a T1 Primary Rate Interface (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 1TR6
`net5-pri`	Euro ISDN services in Belgium, the Netherlands, Switzerland, Sweden, and Singapore

Setting	Specifies
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.

For an E1 line, you can specify the same settings as for a T1 PRI line. E1 lines support the following additional Digital Private Network Signaling System (DPNSS) and Digital Access Signaling System 2 (DASS2) switch types:

- ISDX-DPNSS
- ISLX-DPNSS
- Mercury-DPNSS
- DASS2 (U.K. only)
- Switch-CAS (for E1 R1 and R2 signaling)

Example `set switch-type = nt1-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 calling line ID (CLID) or Dialed Number Information Service (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 `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

syslog-enabled

Description Enables or disables forwarding of log messages to the UNIX syslog server.

Usage Specify one of the following settings:

- yes enables syslog updating.
- no (the default) 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`

syslog-format

Description Specifies the system log message format to use.

Usage Specify one of the following values:

- `tnt` (the default) specifies that `syslog` messages are in MAX TNT format.
- `max` specifies that `syslog` messages are in MAX™ format.

Example `set syslog-format = max`

Location `LOG`

syslog-level

Description Specifies 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 failed to operate 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).

Setting	Lowest-level message indicates
`info` (the default)	State and status changes that are not commonly 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:

- In the `log` profile, the `syslog-level` value applies to the first data stream.
- In the `auxiliary-syslog [1]` subprofile, the `syslog-level` value applies to the second data stream.
- In the `auxiliary-syslog [2]` subprofile, the `syslog-level` 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`

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 Transmission Control Protocol (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, Trivial File Transfer Protocol (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 IP 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`

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 Consider the following:

- For `system-password` to apply, terminal services must be enabled.
- If `security-mode` is set to `none`, the terminal server does not require a password.

Location `TERMINAL-SERVER:terminal-mode-configuration`

system-rmt-mgmt

Description Enables or disables remote management across multichannel calls.

Usage Specify one of the following settings:

- `yes` (the default) allows remote management of the TAOS unit.
- `no` prevents remote management of the TAOS unit.

Example `set system-rmt-mgmt = yes`

Location `SYSTEM`

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`

T

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 is received.

Usage Specify a number from 0 through 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`

t1-inter-digit-timeout

Description Specifies the number of milliseconds the T1 Digital Signal Processor (DSP) waits between digits before considering collection of Dialed Number Information Service/automatic number identification (DNIS/ANI) to be complete.

Usage Specify a number from 100 through 6000 milliseconds. For backward compatibility, the default is 3000 milliseconds (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 For `t1-inter-digit-timeout` to apply, you must set `collect-incoming-digits` to `yes`.

Location `T1/{ any-shelf any-slot 0 }:line-interface`

t2-duration

Description Specifies the value of the transmission time-out 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` through `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`

t3

Description Specifies the action to take when the code image for a T3 slot card is present in a `tar` file.

Usage Specify one of the following settings:

- `auto` (the default) causes the system to load images for slot cards that are installed in the TAOS unit, and to skip images for slot cards that are not installed.
- `load` causes the system to load the image, even if no slot card of that type is installed.
- `skip` causes the system to skip the image, even if a slot card of that type is installed.

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

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 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 through 30000 (0.10 second through 30 seconds). The default is 10000 (10 seconds).

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

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 through 5000. The default is 4000.

Example `set t303-ms = 1000`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:q93b-options`

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 through 50000. The default is 30000.

Example `set t308-ms = 40000`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:q93b-options`

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 through 200000. The default is 0 (zero), which specifies that a default value based on an Asynchronous Transfer Mode (ATM) signaling protocol is used.

Example `set t309-ms = 200000`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:q93b-options`

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 through 50000. The default is 10000.

Example `set t310-ms = 5000`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: q93b-options`

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 through 10000. The default is 4000.

Example `set t313-ms = 2000`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: q93b-options`

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 through 300000. The default is 120000.

Example `set t316-ms = 10000`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: q93b-options`

t322-ms

Description Specifies the timer (in milliseconds) for a response after a `status enq` message is sent.

Usage Specify an integer from 1000 through 10000. The default is 4000.

Example `set t322-ms = 2000`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: q93b-options`

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 through 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 User-to-Network Interface for data terminal equipment (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/""

t392-val

Description Specifies the interval (in seconds) in which status enquiry messages must be received.

Usage Specify an integer from 5 through 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/""

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 through 2147483647. The default is 30000 milliseconds (30 seconds).

Example **set t3-duration = 40000**

Location SS7-GATEWAY:transport-options

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/""

target-params-name

Description Specifies the snmpv3-target-param profile for which to generate traps.

Usage Specify up to 22 characters. The default is null.

Example `set target-params-name = profile1`

Location TRAP/""

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 through 100. The default is 70.

Example `set target-utilization = 70`

Location ANSWER-DEFAULTS:mpp-answer
CONNECTION/"":mpp-options

tcc-ms

Description Specifies the retry time (in milliseconds) for control protocol data units (PDUs).

Usage Specify a value from 0 through 3000. The default is 1000.

Example `set tcc-ms = 500`

Location ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:
qsaal-options

tcp

Description Enables or disables the tcp command from the terminal-server interface.

Usage Specify one of the following settings:

- yes enables a user to initiate a Transmission Control Protocol (TCP) session from the terminal server.
- no (the default) prevents a user from initiating a TCP session from the terminal server.

Example `set tcp = yes`

Dependencies For tcp to apply, terminal services must be enabled.

Location TERMINAL-SERVER:terminal-mode-configuration

tcp-estab

Description Specifies whether a filter must match only established Transmission Control Protocol (TCP) connections.

Usage Specify one of the following settings:

- yes specifies that the filter matches only packets that are part of established TCP connections.
- no (the default) specifies that the filter can match packets that are not part of an established TCP connection.

Example `set tcp-estab = yes`

Dependencies For tcp-estab to apply, protocol must be set to 6 (tcp).

Location FILTER/"":input-filters[*n*]:ip-filter
FILTER/"":output-filters[*n*]:ip-filter

tcp-syn-flood-protect

Description Specifies whether TCP-SYN flood protection is enabled.

Usage Specify one of the following values:

- yes specifies that TCP-SYN flood protection is enabled.
- no (the default) specifies that TCP-SYN flood protection is disabled.

Example `set tcp-syn-flood-protect = yes`

Location IP-GLOBAL

tcp-timeout

Description Specifies a time-out period for Transmission Control Protocol (TCP) connection attempts that use the Domain Name System (DNS) list attempt feature.

Usage Specify an integer indicating the number of seconds for a TCP time-out. Valid values range from 0 through 200 . 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

telnet

Description Enables or disables the `telnet` command from the terminal-server interface.

Usage Specify one of the following settings:

- `yes` specifies that operators can invoke Telnet sessions from the terminal-server interface.
- `no` (the default) disables the use of Telnet in the terminal server.

Example `set telnet = yes`

Dependencies For `telnet` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:terminal-mode-configuration:telnet-options`

telnet-host-auth

Description Determines whether immediate Telnet sessions require local authentication or authentication only by the Telnet host.

Usage Specify one of the following settings:

- `yes` specifies that the session requires authentication only by the Telnet host.
- `no` (the default) specifies that the session must be locally authenticated before undergoing authentication by the Telnet host.

Example `set telnet-host-auth = yes`

Dependencies For `telnet-host-auth` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:immediate-mode-options`

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.
- For `telnet-mode` to apply, terminal services must be enabled.
- 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`

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`

temporary-route

Description Specifies that the TAOS unit adds the route to the routing table only when the link is up.

Usage Specify one of the following settings:

- `yes` excludes a route from the routing table when its connection is down.
- `no` (the default) includes the route in the routing table even if its connection is down.

Example `set temporary-route = no`

Dependencies `temporary-route` is especially useful for dedicated IP-routing connections.

Location `CONNECTION/"":ip-options`

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 For `terminal-type` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER: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 = 57600`

Location `SERIAL/{ any-shelf any-slot 0 }`

text-1
text-2
text-3
text-4

Description Specifies text that the TAOS unit displays in the terminal-server menu for the Telnet host specified by `host-1`, `host-2`, `host-3`, or `host-4`.

Usage Specify a text string describing the corresponding Telnet host. The default is null.

Example `set text-1 = database-server`

Dependencies Consider the following:

- For `text-1`, `text-2`, `text-3`, and `text-4` to apply, terminal services must be enabled.
- `text-1`, `text-2`, `text-3`, and `text-4` do not apply if `remote-configuration` is set to `yes`.

Location `TERMINAL-SERVER:menu-mode-options`

tftp-host-name

Description Specifies the symbolic hostname of a Trivial File Transfer Protocol (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`

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/"":visa2-options`

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`

third-party

Description Enables or disables Open Shortest Path First (OSPF) third-party routing for a static route.

Usage: Specify one of the following settings:

- `yes` enables third-party routing for the OSPF router. When `third-party` is set to `yes`, the `gateway-address` value is the third-party router for the route.
- `no` (the default) disables third-party routing for the OSPF router.

Example `set third-party = yes`

Location `IP-ROUTE/""`

third-prompt-sequence

Description 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`

throttle-no-port-match-udp-traffic-on-slot

Description Enables or disables reception of User Datagram Protocol (UDP) packets for UDP ports currently unknown to the TAOS unit.

Usage Specify one of the following settings:

- `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` (the default) 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`

ticks

Description Specifies the distance to the destination network, in IBM PC clock ticks (one-eighteenth of a second).

Usage Specify an integer. The default is 12.

Example `set ticks = 6`

Dependencies The `ticks` setting is for round-trip timer calculation and for determining the nearest server of a given type.

Location `IPX-ROUTE/""`

tidle-ms

Description Specifies the polling interval (in milliseconds) for when the connection is idle.

Usage Specify a value from 1000 through 20000. The default is 15000.

Example `set tidle-ms = 2000`

Dependencies `tidle-ms` applies only to the Asynchronous Transfer Mode (ATM) User-to-Network Interface (UNI) 3.1 signaling protocol.

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: qsaal-options`

timer1-collect-call

Description When E1 R2 Brazilian signaling is in use, specifies the amount of time (in milliseconds) that an incoming unit waits after sending line signaling for `answer` and before momentarily sending line signaling for `clear back` to test for a collect call.

Usage The recommended value is 500, unless the switch specification is available and another value is required. You must specify a value that is a multiple of 10. The default is 0 (zero), which disables the feature and allows all collect calls to go through, regardless of the setting of `timer2-collect-call`.

Example `set timer1-collect-call = 10`

Dependencies For `timer1-collect-call` to apply, you must set `signaling-mode` to `e1-brazil-signaling`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`

timer2-collect-call

Description When E1 R2 Brazilian signaling is in use, specifies the amount of time (in milliseconds) that an incoming unit waits after momentarily sending line signaling for `clear back` (`AB = 11` while in the `answer` state) to receive a `clear forward` (`AB = 10`) signal from the incoming switch, indicating that the current call is a collect call. If `clear forward` is not received within the number of seconds you specify, the call is not a collect call.

Usage The recommended value is 200, unless the switch specification is available and another value is required. You must specify a value that is a multiple of 10. If you specify a non-zero setting and `clear forward` is received within the interval you specify, the unit rejects the collect call. The default is 0 (zero), which disables the feature and allows all collect calls to go through, regardless of the setting of `timer1-collect-call`.

Example `set timer2-collect-call = 10`

Dependencies For `timer2-collect-call` to apply, you must set `signaling-mode` to `e1-brazil-signaling`.

Location `E1/{ any-shelf any-slot 0 }:line-interface`

tkeepalive-ms

Description Specifies the poll interval (in milliseconds) when the interface is in a transient state.

Usage Specify a value from 0 through 3000. The default is 0 (zero), which specifies that a default value based on an Asynchronous Transfer Mode (ATM) signaling protocol is used.

Example `set tkeepalive-ms = 1000`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: qsaal-options`

tnoresponse-ms

Description Specifies the maximum interval (in milliseconds) between receipt of status protocol data units (PDUs).

Usage Specify a value from 0 through 20000. The default is 0 (zero), which specifies that a default value based on an Asynchronous Transfer Mode (ATM) signaling protocol is used.

Example `set tnoresponse-ms = 500`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: qsaal-options`

tnt-adsl-restricted

Description *Not supported.*

tnt-idsl-restricted

Description *Not supported.*

tnt-sdsl-restricted

Description *Not supported.*

toggle-screen

Description Specifies whether an interactive user can switch between terminal-server menu mode and command mode.

Usage Specify one of the following settings:

- `yes` (the default) 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 For `toggle-screen` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:menu-mode-options`

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.

Usage Specify one of the following settings:

- `yes` specifies that calls are switched from the public network to T-Online on the basis of a user-defined match.
- `no` (the default) specifies that T-Online switching is disabled.

Example `set t-online = yes`

Location `SYSTEM`

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 one of the following settings:

- `yes` specifies that the TAOS unit chooses the link with the most available channels.
- `no` (the default) 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:

- For `t-online-most-avail-chan` to apply, `t-online` must be set to `yes`.
- Trunk group 8 is reserved for DTPT calls when `t-online` is set to `yes`.

Location `SYSTEM`

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.

Usage Specify an integer from 1 through 4.

Example If `t-online-offset` is set to 1 and the TAOS unit receives a call on E1 Primary Rate Interface (PRI) line 5, the NT line is line 6.

Dependencies For `t-online-offset` to apply, `t-online` must be set to `yes`.

Location `SYSTEM`

t-online-type

Note This setting is for a customer-specific application. It is not intended for general use.

Description Specifies the E1 Primary Rate Interface (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:

- For `t-online-type` to apply, `t-online` must be set to `yes`.
- One TE-configured line can switch calls to one or more NT-configured lines.

Location `E1/{ any-shelf any-slot 0 }:line-interface`

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/""`

tos-copying

Description Specifies whether the type of service (TOS) byte is copied.

Usage Specify one of the following settings:

- `yes` specifies that the unit copies the TOS byte from the inner IP header.
- `no` (the default) specifies that the unit does not copy the TOS byte from the inner IP header, but sets the TOS byte in the outer IP header to 000.

Example `set tos-copying = yes`

Dependencies TOS copying might not be possible if the connection uses compression, encryption, Multilink PPP (MP), or Multilink Protocol Plus™ (MP+).

Location `CONNECTION/""`

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/"":ip-options`

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/""`

tpoll-ms

Description Specifies the poll interval (in milliseconds) when the connection is active.

Usage Specify a value from 0 through 3000. The default is 0 (zero), which specifies that a default value based on an Asynchronous Transfer Mode (ATM) signaling protocol is used.

Example `set tpoll-ms = 500`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options: qsaal-options`

trace-id-0

Description Specifies a provisioned identification number from the switch for Peripheral Control Timing Facilities Interface (PCTFI) link 0 (zero).

Usage Specify a number from 1 through 15. The default is 0 (zero). The number you specify must match the setting in the 5ESS RC/V terminal view (v.24).

Example `set trace-id-0 = 4`

Location `PCTFI/{ any-shelf any-slot 0 }`

trace-id-1

Description Specifies a provisioned identification number from the switch for Peripheral Control Timing Facilities Interface (PCTFI) link 1.

Usage Specify a number from 1 through 15. The default is 1. The number you specify must match the setting in the 5ESS RC/V terminal view (v.24).

Example `set trace-id-1 = 3`

Location `PCTFI/{ any-shelf any-slot 0 }`

trace-id-mismatch

Description Indicates whether the STM link is detecting a trace identifier mismatch in the trace-id overhead byte.

Usage The trace-id-mismatch value is read-only and can have one of the following settings:

- true indicates that the STM link is detecting a trace identifier mismatch in the trace-id overhead byte.
- false indicates that the STM link is not detecting a trace identifier mismatch in the trace-id overhead byte.

Example trace-id-mismatch = false

Location STM-PATH-STAT/{ any-shelf any-slot 0 }
STM-STAT/{ any-shelf any-slot 0 }

traceroute

Description Enables or disables the use of the traceroute command in the terminal-server interface.

Usage Specify one of the following settings:

- yes specifies that terminal-server users can use the traceroute command.
- no (the default) disables the traceroute command.

Example **set traceroute = yes**

Dependencies For traceroute to apply, terminal services must be enabled.

Location TERMINAL-SERVER:terminal-mode-configuration

traffic-shaper

Description Specifies the traffic shaper assigned to the virtual circuit.

Usage Specify a number from 1 through 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/"":session-options

trailing-digits

Description Specifies the number of digits required to follow the prefix number for the TAOS unit to consider the called number complete.

Usage Specify a value from 1 through 6. The default is 2.

Example **set trailing-digits = 1**

Dependencies Consider the following:

- If `overlap-receiving` is set to `no`, the `pri-prefix-number`, `trailing-digits`, and `t302-timer` settings do not apply.
- 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 restart the timer when the specified number of digits has been received.

Location `E1/{ any-shelf any-slot 0 }:line-interface`
`T1/{ any-shelf any-slot 0 }:line-interface`

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:

- For `transfer-to-operator` to apply, the MultiVoice® gateway must have `single-dial-enable` set to `no`.
- In one of the incoming 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/{ "" "" }`

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/{ { any-shelf any-slot 0 } 0 }:ospf`
`CONNECTION/"":ip-options:ospf-options`

transit-number

Description Specifies an interexchange carrier (IEC) for long-distance Primary Rate Interface (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 dedicated frame relay data-link connection is in use, `transit-number` does not apply.

Location `CONNECTION/"":telco-options`
`FRAME-RELAY/""`

tree-mask

Description Specifies a mask for comparing subidentifiers in an object identifier (OID) for a view-based access control model (VACM) configuration.

Usage Specify a mask in hexadecimal format. The default is `ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff`. Comparison of a subidentifier can be omitted if you set the corresponding mask bit to `0` (zero).

Example `set tree-mask = ff:ff:ff:ff`

Location `VACM-VIEW-TREE/{ "" "" }`

tree-type

Description Specifies whether the object identifier (OID) is accessible in a view-based access control model (VACM) configuration.

Usage Specify one of the following values:

- `included` (the default) specifies that the OID is accessible.
- `excluded` specifies that the OID is not accessible.

Example `set tree-type = excluded`

Location `VACM-VIEW-TREE/{ "" "" }`

tributary-mapping

Description Specifies the way in which an STM link is mapped down to a DS1 rate.

Usage For T1 links, specify one of the following settings:

- `vc-11-async-mapping` (the default) specifies that the STM signal is mapped down to the asynchronous T1 rate.
- `vc-11-bit-sync-mapping` specifies that the STM signal is mapped down to the bit synchronous T1 rate.
- `vc-3-async-mapping` specifies that the STM signal is mapped down to the asynchronous T3 rate.

For E1 links, specify one of the following settings:

- vc-12-async-mapping (the default) specifies that the STM signal is mapped down to the asynchronous E1 rate.
- vc-12-byte-sync-mapping specifies that the STM signal is mapped down to the byte synchronous E1 rate.
- vc-12-bit-sync-mapping specifies that the STM signal is mapped down to the bit synchronous E1 rate.

Example `set tributary-mapping = vc-11-bit-sync-mapping`

Location `STM-PATH/{ any-shelf any-slot 0 }`

true-connect-enable

Description Enables or disables true-connect signaling for Voice over IP (VoIP) calls.

Usage Specify one of the following settings:

- `yes` enables delay of public switched telephone network (PSTN) alerting and connect messages to match the equivalent H.323 alerting and connect messages. If you specify `yes`, an alerting message is sent to the incoming PSTN switch only when an H.323 alerting message is received on the incoming 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` (the default) disables delay of PSTN alerting and connect messages. If you specify `no`, an alerting message is sent to the incoming PSTN switch as soon as the connection is established with the incoming 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 Integrated Services Digital Network (ISDN) trunks, Lucent recommends that you set the T310 time-out on the telco switch or private branch exchange (PBX) to 30 seconds or greater when using the true-connect feature. The T310 time-out includes the time that the called party's telephone is ringing, so a ten-second time-out 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/{ "" "" }`

trunk-group

Description Specifies a trunk-group number.

- In a `t1`, `e1`, `e3-atm`, `ds3-atm`, `oc3-atm`, `swan`, or `uds3` 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` through `9`.

- In a `t1`, `e1`, `e3-atm`, `ds3-atm`, or `swan` profile, the default is `9`.
- In a `call-route`, `oc3-atm`, or `uds3` profile, the default is `0` (zero), which matches any trunk-group number.

Example `set trunk-group = 4`

Dependencies For `trunk-group` to apply, you must set `use-trunk-groups` to `yes`.

Location `CALL-ROUTE/{ { { any-shelf any-slot 0 } 0 } 0 }`
`DS3-ATM/{ any-shelf any-slot 0 }:line-config`
`E1/{ any-shelf any-slot 0 }:line-interface:channel-config`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config`
`SWAN/{ any-shelf any-slot 0 }:line-config`
`T1/{ any-shelf any-slot 0 }:line-interface:channel-config`
`UDS3/{ any-shelf any-slot 0 }:line-config`

trunk-group-callback-control

Description Specifies the trunk group number that the unit prepends to the number supplied by the user for Callback Control Protocol (CBCP) callback.

Usage Enter an integer. The default is null.

Example `trunk-group-callback-control = 9`

Location `CONNECTION/"":ppp-options`

trunk-prefix-enable

Description Specifies a trunk group for connecting Voice over IP (VoIP) calls to the called end point on an outbound MultiVoice® gateway.

Usage Specify one of the following settings:

- `yes` causes an outbound MultiVoice® gateway to use a preselected trunk group, assigned by either the incoming MultiVoice® gateway or the MultiVoice® Access Manager (MVAM) device, to route outgoing calls to the public switched telephone network (PSTN).
- `no` (the default) specifies that the outbound 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 outbound MultiVoice® gateway.
- The size of the trunk groups must be defined on all outbound MultiVoice® gateways.
- Trunk group numbers must be assigned for outbound T1 trunks.

Location `VOIP/{ "" "" }`

trunk-quiesce-enable

Description Enables or disables deactivation of a T1 Primary Rate Interface (PRI) line when a gateway is unavailable.

Usage Specify one of the following settings:

- `no` (the default) 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 PRI signaling and have been configured for VoIP can be deactivated systemwide by the `trunk-quiesce-enable` setting.

Location `VOIP/{ "" "" }`

trunk-state

Description Indicates the state of the F2 and F3 bit for the virtual tributary.

Usage The `trunk-state` setting is read-only and can have one of the following values:

- `unused` indicates that the bits are in an invalid state.
- `non-operational` indicates that a signal is present but the trunk is out of service.
- `operational` indicates that a signal is present and the trunk is in service.
- `unequipped` indicates that no signal is present.

Example `trunk-state = operational`

Location `PCTFI-STAT/{ any-shelf any-slot 0 }:virtual-ds1-line-status`

ts-idle-mode

Description Specifies when the TAOS unit is to restart 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 restarts the timer when an input character is received.
- `input-output-idle` specifies that the TAOS unit restarts the timer when either input or output characters are processed.

Example `set ts-idle-mode = input-only-idle`

Location `ANSWER-DEFAULTS:session-info`
`CONNECTION/"":session-options`

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` through `65535`. The default is `120`.

Example `set ts-idle-timer = 360`

Dependencies For `ts-idle-timer` to apply, `ts-idle-mode` must be set to a value other than `no-idle`.

Location `ANSWER-DEFAULTS:session-info`
`CONNECTION/"":session-options`

tunnel-accounting

Description Specifies whether the unit performs accounting for Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP) tunnels.

Usage Specify one of the following settings:

- yes specifies that the unit performs accounting for L2F and L2TP tunnels.
- no (the default) specifies that the unit does not perform accounting for L2F and L2TP tunnels.

Example `set tunnel-accounting = yes`

Location `EXTERNAL-AUTH:rad-acct-client`

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`

Dependencies 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/"":tunnel-options`

tunnel-server-pre-sccrq-lookup

Description When a tunnel password is not available, specifies whether the unit searches for a matching `tunnel-server` profile before sending a Start Control Connection Request (SCCRQ) message.

Usage Specify one of the following values:

- `yes` specifies that the unit searches for a matching `tunnel-server` profile. If a matching `tunnel-server` profile cannot be located and tunnel authentication is enabled, the tunnel establishment attempt fails.
- `no` (the default) specifies that the `tunnel-server` lookup is postponed until after the unit sends an SCCRQ message.

Dependencies The unit performs a lookup for a matching `tunnel-server` profile by one of the following criteria:

- Remote Authenticated Dial-In User Service (RADIUS) `Tunnel-Server-Auth-ID` attribute-value pair (AVP)
- RADIUS `Tunnel-Server-Endpoint` AVP
- Remote hostname

Location `L2-TUNNEL-GLOBAL:l2tp-config`

tx-cell-payload-scramble-disabled

Description Enables or disables scrambling of the 48-byte Asynchronous Transfer Mode (ATM) payload in transmitted cells.

Usage Specify one of the following settings:

- `yes` disables scrambling of the 48-byte ATM payload in transmitted cells.
- `no` (the default) 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/{ any-shelf any-slot 0 }:line-config`

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` through `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 slot cards. If you specify a value for a connection that does not use these slot cards, the system ignores the settings.

Location `CONNECTION/"":session-options`

tx-scramble-disabled

Description Enables or disables scrambling of the entire Asynchronous Transfer Mode (ATM) transmit stream.

Usage Specify one of the following settings:

- `yes` disables scrambling of the entire ATM transmit stream.
- `no` (the default) 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/{ any-shelf any-slot 0 }:line-config`

type

Description The `type` parameter has different uses, depending on the profile:

- In a `filter` profile, the `type` setting specifies the type of the current filter.
- In the `transport-options` subprofile, the `type` setting specifies the type of transport layer.
- In the `resilience-options` subprofile, the `type` setting specifies the type of behavior that a unit follows when a T1 or E1 line is lost.

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 Internetwork Packet Exchange (IPX) filter.
- `route-filter` specifies a route filter.
- `tos-filter` specifies a type of service (TOS) filter.

In the `transport-options` subprofile, specify one of the following values:

- `ascend` (the default) specifies the transport layer used by the Access SS7 Gateway Control Protocol (ASGCP) and IP Device Control (IPDC) protocol: 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 the `resilience-options` subprofile, specify one of the following values:

- `release-all` (the default) specifies that a Signaling System 7 (SS7) Notify Line Status (NLS) message is sent to the signaling gateway, indicating that the line is down; all calls on that line are dropped; and an SS7 Release Channel Completed (ACR) message for each call is sent to the signaling gateway, acknowledging release of the call.
- `maintain-active` specifies that an SS7 NLS message is sent to the signaling gateway, indicating that the line is down and that the TAOS unit maintains all call connections until it receives a Release Channel Request (RCR) message from the signaling gateway. Upon request to restart, the TAOS unit drops the call and returns an ACR message to the signaling gateway.

- `timed-release` specifies that an SS7 NLS message is sent to the signaling gateway, indicating that the line is down and that the TAOS unit waits for the amount of time specified by the `duration` value. If the T1 or E1 line reestablishes synchronization within the specified time, call connections are maintained. If the T1 or E1 line does not reestablish synchronization, the TAOS unit initiates release of the call connections.

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 `FILTER/"":input-filters`
`FILTER/"":output-filters`
`SS7-GATEWAY:resilience-options`
`SS7-GATEWAY:transport-options`

type-filter

Description Specifies whether the Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP) filter explicitly includes the service in the SAP table or excludes 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`

type-of-service

Description The `type-of-service` parameter has different uses, depending on the subprofile in which it is set:

- In a `signaling-tos` subprofile, the `type-of-service` parameter specifies the type of service (TOS) for User Datagram Protocol (UDP) packets.
- In a `tos` subprofile, the `type-of-service` parameter specifies the TOS for Signaling System 7 (SS7) signaling traffic.
- In a `tos-options` or `tos-filter` subprofile, the `type-of-service` parameter specifies the TOS 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 `signaling-tos`, `tos`, or `tos-options` subprofile, or `type` to `tos-filter` in the `input-filters` or `output-filters` subprofile.

Location `CONNECTION/"":ip-options:tos-options`
`FILTER/"":input-filters[`*n*`]:tos-filter`
`FILTER/"":output-filters[`*n*`]:tos-filter`
`SS7-GATEWAY:transport-options:tos`
`VOIP/{ "" "" }:signaling-tos`
`VOIP/{ "" "" }:tos-options`

U

udp-cksum

Description Enables or disables the use of User Datagram Protocol (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:

- Ascend Tunnel Management Protocol (ATMP)
- Domain Name System (DNS)
- ECHOSERV
- Remote Authenticated Dial-In User Service (RADIUS)
- Routing Information Protocol (RIP)
- Simple Network Time Protocol (SNTP)
- SYSLOG
- Terminal Access Controller Access Control System (TACACS)
- Trivial File Transfer Protocol (TFTP)

Usage Specify one of the following settings:

- `yes` (the default) 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`

udp-port

Description Specifies a User Datagram Protocol (UDP) port as follows:

- In an `atmp` profile, specifies the 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 Consider the following:

- 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 restart the system.

Location `ATMP`
`CONNECTION/"":tunnel-options`
`STACKING`

uds3

Description Specifies the action to take when the code image for an unchannelized DS3 slot card is present in a `tar` file.

Usage Specify one of the following settings:

- `auto` (the default) causes the system to load images for slot cards that are installed in the TAOS unit, and to skip images for slot cards that are not installed.
- `load` causes the system to load the image, even if no slot card of that type is installed.
- `skip` causes the system to skip the image, even if a slot card of that type is installed.

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

ue1

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

Usage Specify one of the following settings:

- `auto` (the default) causes the system to load images for slot cards that are installed in the TAOS unit, and to skip images for slot cards that are not installed.
- `load` causes the system to load the image, even if no slot card of that type is installed.
- `skip` causes the system to skip the image, even if a slot card of that type is installed.

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

unknown-cards

Description Specifies the action to take when the code image for newly supported slot cards is present in a `tar` file.

Usage Specify one of the following settings:

- `auto` (the default) causes the system to load images for slot cards that are installed in the TAOS unit, and to skip images for slot cards that are not installed.
- `load` causes the system to load the image, even if no slot card of that type is installed.
- `skip` causes the system to skip the image, even if a slot card of that type is installed.

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

update-interval

Description Defines the Simple Network Time Protocol (SNTP) update interval, in seconds, for up to 31 days.

Usage Specify the update interval in seconds from 1 to 2678400. The default is 600.

Example `set update-interval = 750`

Location `IP-GLOBAL:sntp-info`

update-threshold

Description Specifies the maximum time offset (in seconds) allowed between the Simple Network Time Protocol (SNTP) server and system before an update occurs.

Usage Specify an integer from 0 through 2147483647. The default is 10.

Example `set update-threshold = 5`

Dependencies For `update-threshold` to apply, `enabled` must be set to `passive`.

Location `IP-GLOBAL:sntp-info`

up-status

Description Indicates the status of a device.

Usage The `up-status` value is read-only and can have one of the following settings:

- `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/{ { any-shelf any-slot 0} 0}`

up-trans-delay

Description Specifies the transition delay time, in tenths (0.1) of a second, during which the unit keeps a T1 line disconnected after detecting a carrier signal on the line.

Usage Specify a number from 100 (the default) through 1000.

Example `set up-trans-delay = 200`

Location `T1/{ any-shelf any-slot 0 }:line-interface`

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 one of the following settings:

- `yes` (the default) 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`

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 one of the following settings:

- `yes` (the default) specifies that the system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it, or 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/""`

user-1

user-2

user-3

user-4

Description Specifies the username for `rlogin` sessions with `host-1`, `host-2`, `host-3`, or `host-4`.

Usage Specify a text string of up to 31 characters. The default is null.

Example `set user-1 = robin`

Dependencies For `user-1`, `user-2`, `user-3`, or `user-4` to apply, you must set the corresponding `service-1`, `service-2`, `service-3`, or `service-4` parameter to `rlogin`.

Location `TERMINAL-SERVER:menu-mode-options`

user-profile

Description The `user-profile` parameter has different uses, depending on the profile:

- 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 restarted 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 `IP-GLOBAL`
`SERIAL/{ any-shelf any-slot 0 }`

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.
`%r`	11	`Tx/Rx Rate`	Transmit and receive rates.
`%d`	3	`Svc`	A three-letter code showing the type of service (TOS).
`%a`	15	`Address`	IP address.
`%u`	14	`Username`	Name of a `connection` profile.
`%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 (CLID), if known.

The default value of `userstat-format` causes the standard session-listing output format for both the `userstat` command and Finger queries.

Example `set userstat-format = %u (%d) @ %c`

Location `SYSTEM`

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 one of the following settings:

- `yes` (the default) 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/""`

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 time-outs in the receipt of acknowledgments 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 one of the following settings:

- `yes` (the default) 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`

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 one of the following settings:

- `yes` specifies that all channels must be assigned a trunk-group number for outgoing calls.
- `no` (the default) 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`

ut1

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

Usage Specify one of the following settings:

- `auto` (the default) causes the system to load images for slot cards that are installed in the TAOS unit, and to skip images for slot cards that are not installed.
- `load` causes the system to load the image, even if no slot card of that type is installed.
- `skip` causes the system to skip the image, even if a slot card of that type is installed.

Dependencies A slot 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 slot card, and does not delete the profile unless the administrator uses the `slot –r` command to permanently remove a card no longer installed in the system, or clears nonvolatile RAM (NVRAM). To ensure that the system does not load unnecessary images, use `slot –r` to remove `slot-type` profiles for slot cards no longer installed in the system.

Location `LOAD-SELECT`

V

v42/mnp

Description Specifies how the digital modems negotiate Link Access Procedure for Modems/Microcom Networking Protocol (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 = must-v42`

Dependencies For `v42-mnp` to apply, terminal services must be enabled.

Location `TERMINAL-SERVER:modem-configuration`

v44-enabled

Description Specifies whether the TAOS unit negotiates V.44 compression with modems having this feature.

Usage Specify one of the following values:

- `yes` enables V.44 compression negotiation.
- `no` (the default) disables V.44 compression negotiation.

Example `set v44-enabled = yes`

Location `TERMINAL-SERVER:modem-configuration`

v110-subaddress

Description Specifies the subaddress for V.110 rate adaption connections.

Usage Specify a valid subaddress. The default is `0` (zero).

Example `set v110-subaddress = 100`

Location `SYSTEM`

valid-entry

Description The `valid-entry` parameter has different uses, depending on the profile:

- In a `filter` profile, `valid-entry` enables or disables the current input or output filter.
- In a `default-call-mapping` subprofile, `valid-entry` specifies whether the unit skips this entry when mapping a call.

Usage Specify one of the following settings:

- `yes` activates the filter or permit list.
- `no` (the default) disables the filter or permit list.

Example `set valid-entry = yes`

Location `FILTER/"":input-filters`
`FILTER/"":output-filters`
`TUNNEL-SERVER/"":dialout-options:default-call-mapping`

valid-filter

Description Enables or disables the Internetwork Packet Exchange (IPX) Service Advertising Protocol (SAP) input or output filter.

Usage Specify one of the following settings:

- `yes` enables the IPX SAP filter.
- `no` (the default) 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`

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. The default is null.

Example `set value = aaaa0300000080f3`

Location `FILTER/"":input-filters[n]:gen-filter`
`FILTER/"":output-filters[n]:gen-filter`

vc-fault-management

Description Specifies the fault management type for the virtual circuit.

Usage Specify one of the following settings:

- `none` (the default) specifies that no fault management is performed on the virtual circuit.
- `segment-loopback` specifies that the system sends an operations, administration, and maintenance (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/"":atm-options`

vci

Description Specifies the virtual circuit identifier (VCI) for the connection.

Usage Specify a number from 32 through 1023. The default is 32.

Location `CONNECTION/"":atm-options`

vc-max-loopback-cell-loss

Description Specifies the number of consecutive loopback cells lost before the system clears the connection. When a permanent virtual circuit (PVC) is cleared, the interface is in an inactive state until the system can reestablish the connection.

Usage Specify an integer. The default is 1.

Example `set vc-max-loopback-cell-loss = 5`

Location `CONNECTION/"":atm-options`

verify-remote-host-name

Description Specifies whether or not the unit verifies the remote peer hostname against the corresponding Remote Authentication Dial-In User Service (RADIUS) attribute, if present.

Usage Specify one of the following values:

- `yes` specifies that the unit verifies the remote peer hostname against the corresponding RADIUS attribute.
- `no` (the default) specifies that the unit does not verify the remote peer hostname against the corresponding RADIUS attribute.

Example `set verify-remote-host = yes`

Location `L2-TUNNEL-GLOBAL:l2tp-config`

version

Description *Not supported.*

view-name

Description Specifies the name of a view for a view-based access control model (VACM) configuration.

Usage Specify a string. The default is null. The system determines whether the view contains a given object identifier (OID) by comparing the `view-name` value with `view-tree-oid`.

Example `set view-name = view1`

Location `VACM-VIEW-TREE/{ "" "" }:tree-properties`

view-tree-oid

Description Specifies the object identifier (OID) for a view defined in a view-based access control model (VACM) configuration.

Usage Specify an OID in dotted decimal format. The default is null.

Example `set view-tree-oid = 1.2.3.4`

Dependencies The system determines whether a view contains a given OID by comparing the `view-name` value with `view-tree-oid`.

Location `VACM-VIEW-TREE/{ "" "" }:tree-properties`

vj-header-prediction

Description Specifies whether Van Jacobson IP header prediction should be negotiated on incoming calls.

Usage Specify one of the following settings:

- `yes` (the default) enables VJ compression for Transmission Control Protocol (TCP) packets.
- `no` disables VJ compression for TCP packets.

Example `set vj-header-prediction = no`

Location `ANSWER-DEFAULTS:ip-answer`
`CONNECTION/"":ip-options`

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/{ "" "" }`

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 Voice over IP (VoIP) call.

Location `VOIP/{ "" "" }`

voip-accounting

Description Enables or disables Remote Authentication Dial-In User Service (RADIUS) accounting for Voice over IP (VoIP) calls.

Usage Specify one of the following values:

- `yes` (the default) enables RADIUS accounting for VoIP calls.
- `no` disables RADIUS accounting for VoIP calls.

Example `set voip-accounting = no`

Location `EXTERNAL-AUTH:rad-acct-client`

voip-call-logging

Description Enables or disables call logging for Voice over IP (VoIP) calls.

Usage Specify one of the following values:

- `yes` (the default) enables call logging for VoIP calls.
- `no` disables call logging for VoIP calls.

Example `set voip-call-logging = no`

Location `CALL-LOGGING`

voip-enabled

Description Indicates whether the unit enables Voice over IP (VoIP).

Usage The `voip-enabled` value is read-only and can have one of the following settings:

- `yes` indicates that VoIP is enabled.
- `no` indicates that VoIP is not enabled.

Example `voip-enabled = yes`

Location `BASE`

voip-gk-change-enabled

Description Enables 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 that the gatekeeper change occurred (`sysAbsoluteCurrentTime`)

Usage Specify one of the following settings:

- `yes` enables trap generation when the registered gatekeeper changes.
- `no` (the default) disables trap generation when the registered gatekeeper changes.

Example `set voip-gk-change-enabled = yes`

Location `TRAP/""`

voip-max-capacity-allowed

Description Indicates whether the unit enforces a maximum Voice over IP (VoIP) call-processing limit.

Usage The `voip-max-capacity-allowed` value is read-only and can have one of the following values:

- `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`

vpi

Description Specifies the virtual path identifier (VPI) for the connection.

Usage Specify a number from 0 through 15. The default is 0 (zero).

Example `set vpi = 5`

Location `CONNECTION/"":atm-options`

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. 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

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.

Example `set vpi-vci-range = 0-31/32-2047`

Location `DS3-ATM/{ any-shelf any-slot 0 }:line-config`
`DS3-ATM-STAT/{ any-shelf any-slot 0 }`
`E3-ATM/{ any-shelf any-slot 0 }:line-config`
`OC3-ATM/{ any-shelf any-slot 0 }:line-config`

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 one of the following settings:

- `yes` specifies that the TAOS unit does not prompt for a PIN from the user.
- `no` (the default) 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/{ "" "" }`

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 Internetwork Packet Exchange (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.
- Specifying the name in an `ss7-gateway` profile defines the VRouter to use as the source for outbound IP Device Control (IPDC) packets.

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, the `vrouter` parameter enables the system to separate traffic for different L2TP network server (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 Ascend Tunnel Management Protocol (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/""`
`CONNECTION/"":tunnel-options`
`IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }`
`IP-ROUTE/""`
`SS7-GATEWAY`

vrouter-ip-addr

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-addr = 200.40.60.5`

Location `VROUTER/""`

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 (`wanLineIfIndex`).
- The line usage (`wanLineUsage`). This usage is reported as `trunk`, `quiesced`, or `disabled`.
- The absolute time to show when the line state changed (`sysAbsoluteCurrentTime`).

Usage Specify one of the following settings:

- `yes` enables trap generation if the state of an E1 or T1 line changes.
- `no` (the default) disables trap generation if the state of an E1 or T1 line changes.

Example `set wan-line-state-change-enabled = yes`

Location `TRAP/""`

warmstart-enabled

Description Specifies whether the 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 one of the following settings:

- `yes` (the default) 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 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.

Example `set warmstart-enabled = no`

Location `TRAP/""`

watchdog-index

Description Indicates the type, location ID and the unit number of the watchdog.

Usage The `watchdog-index` cannot be set directly.

Example `watchdog-index = {fantray fantray 1}`

Location `WATCHDOG-CONFIG`

watchdog-name

Description Specifies an individual watchdog.

Usage Specify up to 80 characters. The default is a system-defined standard name.

Example `set watchdog-name = tempModule1`

Location `WATCHDOG-CONFIG`

watchdog-trap-enable

Description Enables or disables the watchdog warning trap for the specified watchdog.

Usage Specify one of the following settings:

- `Yes` (the default) enables the watchdog warning trap.
- `No` disables the watchdog warning trap.

Example `set watchdog-trap-enable = no`

Location `WATCHDOG-CONFIG`

weekday

Description Specifies the day of the week.

Usage Specify a text string representing a day of the week.

Example `set weekday = Wednesday`

Location `TIMEDATE:date`

window-size

Description Specifies a window size:

- In the `qsaal-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 `qsaal-options` subprofile, specify an integer from `16` through `128`. The default is `64`.
- In the `ss7-gateway` profile, specify an integer from `1` through `63`. The default is `7`.

Example `set window-size = 128`

Location `ATM-INTERFACE/{ { any-shelf any-slot 0 } 0 }:svc-options:qsaal-options`
`SS7-GATEWAY:transport-options`

write-access

Description Specifies whether the Simple Network Management Protocol (SNMP) manager has read and write access.

Usage Specify one of the following settings:

- `yes` specifies that the SNMP manager has read and write access.
- `no` (the default) specifies that the SNMP manager has read-only access.

Example `set write-access = yes`

Dependencies For `write-access` to apply, you must set `active` to `yes` in the `snmp-manager` profile.

Location `SNMP-MANAGER/""`

write-view-name

Description Specifies the name of the view-based access control model (VACM) view for write access.

Usage Specify a string. The default is null.

Example `set write-view-name = writeview1`

Location VACM-ACCESS/{ "" "" v1 no+ }

X

x25chan-target-utilization

Description *Not supported.*

xcom-ss7

Description Enables or disables IP Device Control (IPDC) processing on the unit.

Usage Specify one of the following settings:

- `enabled` (the default) 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

Y

year

Description Specifies the year.

Usage When using a four-digit format, specify a number from 1990 through 2089. When using a two-digit format, specify a number from 00 through 99. The unit interprets a setting from 0 through 89 as the years 2000 through 2089, and a setting from 90 through 99 as the years 1990 through 1999.

Example `set year = 2002`

Location TIMEDATE:date

yellow-receive

Description Specifies whether the local device has received a loss-of-frame indication.

Usage The `yellow-receive` value is read-only and can have one of the following settings:

- `true` specifies that the local device has received a loss-of-frame indication.
- `false` specifies that the local device has not received a loss-of-frame indication.

Example `yellow-receive = false`

Location `DS3-ATM-STAT/{ any-shelf any-slot 0 }`
`E3-ATM-STAT/{ any-shelf any-slot 0 }`
`T1-STAT/{ any-shelf any-slot 0 }`
`T3-STAT/{ any-shelf any-slot 0 }`
`UDS3-STAT/{ any-shelf any-slot 0 }`

Index

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X