Lucent Technologies
Bell Labs Innovations

APX 8000™/MAX TNT®

Administration Guide

Part Number: 7820-0804-004
For software version 9.0
January 2001

Notice

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

Safety, Compliance, and Warranty Information

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

Security Statement

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

Trademarks

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

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

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

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

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

Ordering Information

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

Feedback

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

Lucent Technologies

Customer Service

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

Finding information and software

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

Obtaining technical assistance

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

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

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

Obtaining assistance through email or the Internet

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

Calling the technical assistance center (TAC)

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

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

Contents

Figures

Tables

About This Guide

What is in this guide

This guide describes how to manage and troubleshoot the APX 8000™ and MAX TNT® TAOS units. It assumes that you have set up your unit as described in the *Hardware Installation Guide* that came with your unit and the *APX 8000/MAX TNT Physical Interface Configuration Guide*. You must also have the unit configured for network connectivity as described in the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.

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

Although some of the sections in this manual deal with security issues, the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide* provides a more comprehensive approach to such topics as securing the unit, using firewalls, and understanding the more complex authentication procedures (such as the use of dynamic passwords).

To perform many of the tasks in this manual, you must have administrative permission on the TAOS unit. For instructions on logging into the TAOS unit with administrative permissions, see “Logging into the TAOS unit” on page 2-2.

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

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

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

What you should know

This guide is for the person who installs, configures, and maintains a TAOS unit. To configure a unit, you need to understand the following:

- Internet or telecommuting concepts
- Wide Area Network (WAN) concepts
- Local Area Network (LAN) concepts, if applicable

Documentation conventions

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

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

Documentation set

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

- **Read me first:**
  - *Access Networks Safety and Compliance Guide*
    Contains important safety instructions and country-specific compliance information that you must read before installing a TAOS unit.
  - *TAOS Command-Line Interface Guide*
    Introduces the TAOS command-line environment and shows how to use the command-line interface effectively. This manual describes keyboard shortcuts and introduces commands, security levels, profile structure, and parameter types.
- **Installation and basic configuration:**
  - *APX 8000 Hardware Installation Guide*
    Shows how to install APX 8000 hardware and includes technical specifications for these units.
  - *MAX TNT Hardware Installation Guide*
    Shows how to install MAX TNT hardware and includes technical specifications for these units.
  - *APX 8000/MAX TNT Physical Interface Configuration Guide*
    Shows how to configure the slot cards installed in a TAOS unit and their line attributes for such functions as framing, signaling, and channel usage. It also describes how calls are routed through the system and includes information about configuring the unit in a Signaling System 7 (SS7) environment. This guide explains shelf controller redundancy for an APX 8000 unit.
- **Configuration:**
  - *APX 8000/MAX TNT ATM Configuration Guide*
    Describes how to configure Asynchronous Transfer Mode (ATM) operations on a TAOS unit. This guide explains how to configure physical layer attributes and how to create permanent virtual circuit (PVC) and switched virtual circuit (SVC) ATM interfaces. It includes information about ATM direct and ATM-Frame Relay circuits.
  - *APX 8000/MAX TNT Frame Relay Configuration Guide*
    Describes how to configure Frame Relay operations on a TAOS unit. This guide explains physical layer configuration and restrictions and how to create permanent virtual circuit (PVC) and switched virtual circuit (SVC) interfaces. It includes information about Multilink Frame Relay (MFR) and link management, as well as Frame Relay and Frame Relay direct circuits.
  - *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*
    Shows how to configure LAN and WAN routing for analog and digital dial-in connections on a TAOS unit. This guide includes information about IP routing, Open Shortest Path First (OSPF) routing, Internet Group Management Protocol (IGMP) routing, multiprotocol routers, Virtual Routers (VRouters), and tunneling protocols.
  - *MultiVoice™ for MAX TNT Configuration Guide*
    Shows how to configure the MultiVoice application to run on a MAX TNT unit in both Signaling System 7 (SS7) and H.323 Voice over IP (VoIP) configurations.

- **RADIUS:** *TAOS RADIUS Guide and Reference*
  Describes how to set up a TAOS unit to use the Remote Authentication Dial-In User Service (RADIUS) server and contains a complete reference to RADIUS attributes.
- **Administration and troubleshooting:**
  - *APX 8000/MAX TNT Administration Guide* (this guide),
    Describes how to administer a TAOS unit, including how to monitor the system and cards, troubleshoot the unit, and configure the unit to use the Simple Network Management Protocol (SNMP).
- **Reference:**
  - *APX 8000/MAX TNT Reference*
    An alphabetic reference to all commands, profiles, and parameters supported on TAOS units.
  - *TAOS Glossary*
    Defines terms used in documentation for TAOS units.

Administering Slot Cards

1

Typical system administration tasks for the TAOS unit's slot cards include viewing status information, removing a slot card configuration, and disabling lines. For information about managing your TAOS unit, see Chapter 2, "TAOS System Administration."

Viewing installed slot cards

The Show command displays information about the slot cards installed in the TAOS unit and the status of each card. You can also use the Show command for a particular slot card. For an example, see "Viewing information about slot cards" on page 1-3.

The following example illustrates use of the Show command that displays a list of slot cards installed in the left controller of a unit:

```
super->show

Controller { left-controller } ( PRIMARY ):
    { shelf-1 slot-2 0 }         UP       csmx-card
```

```
{ shelf-1 slot-4 0 }        UP      hdlc2ec-card
{ shelf-1 slot-5 0 }        UP      madd2-card
{ shelf-1 slot-7 0 }        UP      oc3-atm-card
{ shelf-1 slot-8 0 }        UP      hdlc2ec-card
{ shelf-1 slot-9 0 }        UP      ether3-card
{ shelf-1 slot-11 0 }       RESET   8e1-card
{ shelf-1 slot-12 0 }       UP      hdlc2-card
{ shelf-1 slot-13 0 }       UP      csmx-card
{ shelf-1 slot-14 0 }       UP      hdlc2-card
{ shelf-1 slot-15 0 }       UP      hdlc2ec-card
{ shelf-1 slot-16 0 }       UP      hdlc2ec-card
{ shelf-1 slot-17 0 }       UP      hdlc2ec-card
{ shelf-1 slot-19 0 }       UP      ether3-card
{ shelf-1 slot-20 0 }       UP      hdlc2-card
{ shelf-1 slot-21 0 }       UP      hdlc2-card
{ shelf-1 slot-22 0 }       UP      csmx-card
{ shelf-1 slot-23 0 }       UP      t3-card
{ shelf-1 slot-24 0 }       UP      hdlc2-card
{ shelf-1 slot-25 0 }       UP      hdlc2-card
{ shelf-1 slot-26 0 }       UP      csmx-card
{ shelf-1 slot-27 0 }       UP      hdlc2-card
{ shelf-1 slot-29 0 }       UP      ether3-card
{ shelf-1 slot-30 0 }       UP      csmx-card
{ shelf-1 slot-33 0 }       UP      t3-card
{ shelf-1 slot-34 0 }       UP      hdlc2ec-card
{ shelf-1 slot-36 0 }       UP      8t1-card
{ shelf-1 slot-38 0 }       UP      ether3-card
{ shelf-1 slot-39 0 }       UP      ether3-card
```

The output lists the physical address of each slot in which a slot card is installed. The address is in the form {*shelf slot item*}. Each listing also shows the status of the card and the type of card installed.

The status can be reported as follows:

Status	**Signifies**
UP	Normal operational mode.
DOWN	Not in operational mode.
POST	The card is running power-on self tests.
LOAD	The card is loading code as part of booting up.
OCCUPIED	The slot is occupied by a two-slot card (such as the 48 modem card in shelf 1, slots 3 and 4, in the example above).
RESET	The card is being reset.
NONE	The card has been swapped out, but its configuration remains in NVRAM.

The Show command can report the following types of slot cards:

Label	Signifies
`unknown`	Current software does not recognize the card in the slot.
4/1ether-card	Ethernet card with one 100Mbps and four 10Mbps ports.
`4ether-card`	Ethernet card with four 10Mbps ports.
4ether2-card	Ethernet card with one 100Mbps and three 10Mbps ports.
`48modem-card`	48 V.34 modem card.
`48modem-56k-card`	Series56 Digital Modem card.
`8e1-card`	8-line E1 slot card.
`8t1-card`	8-line T1 slot card.
csmx-card	Series56 II Digital Modem card.
`ds3-atm-card`	DS3 card with ATM support.
`shelf-controller`	Shelf-controller card.

Viewing information about slot cards

To use the Show command for information about a particular command, add the shelf and slot-card numbers as arguments. For example:

```
admin>show 1 3
Shelf 1 ( standalone ):

    { shelf-1 slot-3 0 }       UP       4ether2-card:
    { shelf-1 slot-3 1 }       UP         ethernet-1
    { shelf-1 slot-3 2 }       UP         ethernet-2
    { shelf-1 slot-3 3 }       UP         ethernet-3
    { shelf-1 slot-3 4 }       UP         ethernet-4
    { shelf-1 slot-3 5 }                  100-Base-T
```

Opening a session with a slot card

To open a session with a slot card, use the Open command as in the following example:

```
admin> open 1 7
```

where 1 is the shelf number and 7 is the slot number.

After you have established a session with the card, the prompt changes to indicate the type of card, its slot number, and its shelf number. To list the commands available on the card, enter a `?` or `help`, as in the following example:

```
t1-1/7> ?
 ?                              ( user )
 auth                           ( user )
 cbcardif                       ( debug )
 cbsnmptrap                     ( debug )
```

```
 cbStats                          ( debug )
 checkd                           ( debug )
 clear                            ( user )
 clock-source                     ( diagnostic )
 debug                            ( diagnostic )
 debugd                           ( debug )
 display                          ( debug )
 dp-decode                        ( debug )
 dp-ram-display                   ( debug )
 dpram-test                       ( debug )
 dspBypassClients                 ( debug )
 dspDial                          ( debug )
 dspSetDddTimeslot                ( debug )
 fakeCalledId                     ( debug )
 fakeClid                         ( debug )
 fe-loop                          ( diagnostic )
 fill                             ( debug )
 frreset                          ( debug )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

For information about the card-level commands, see the *APX 8000/MAX TNT Reference*.

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

```
t1-1/7> quit
```

Changing a slot state

To force a change in the state of a slot, use the Slot command, as shown in the following examples.

To bring a slot down, use the Slot command with the `-d` option, and specify the shelf and slot number of the card you want to shut down. For example:

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

When you bring a card down with the Slot command, it only remains down until the next reboot. To bring a slot up:

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

Changing a device state

To force a change in the state of a device, use the Device command, as shown in the following examples.

To bring a device down:

```
admin> device -d {{1 3 6} 24}
slot 1/3 state change forced
```

To bring a device back up:

```
admin> device -u {{1 3 6} 24}
slot 1/3 state change forced
```

Removing a slot card and its configuration

TAOS unit slot cards are hot swappable. When you remove a card, the system retains its configuration. This enables you to re-install the card or install another of the same type in the same slot, without reconfiguring the system or uploading a backup configuration. One side-effect of configuration retention is that the NVRAM used to store configuration information is not cleared when a card is removed, until you explicitly clear the configuration.

When a card has been removed, it shows up with a status of NONE in the Show command output. For example:

```
admin> show 1 13
Shelf 1 ( standalone ):
  { shelf-1 slot-13 0 }      NONE      slot-card-8t1:
    { 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 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 the administrator enters the Slot -r command, as in the following example:

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

In either case, all the old profiles associated with the slot are deleted. If a different type of card is inserted, appropriate new profiles are created.

Viewing the clock source for a slot card

The Clock-Source command can be run on the shelf controller or on an individual card, as in the following example on a T1 card:

```
admin> open 1 1

t1-1> clock-source
Master line: 3
Source List:
    Source: line 3 Available*       priority: 1
```

Sources with layer 2 up, which are preferred, are marked with an asterisk. For information about configuring the clock source see the hardware installation guide.

Recovering from a failed slot-card installation

If you installed a new slot card before upgrading the system software, and the slot card does not come up properly, there are two ways to recover:

- Use the Nvram command.
- Remove the slot card.

Using the NVRAM command

Caution: Using the Nvram command resets the entire system. This method cannot be done remotely because the Nvram command clears the TAOS unit's configuration, including its IP address. Before performing this procedure make sure you have access to the TAOS unit's serial port.

To recover from a failed slot-card installation by this method:

1 Save the current system configuration. For example:

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

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

2 Clear the system configuration and restart the TAOS unit by executing the Nvram Clear command:

```
admin>nvram clear
```

3 Restore the saved system configuration.

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

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

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

For a complete description of saving and restoring configurations, see the "Backing up and restoring a configuration" on page 2-19.

Removing the slot card

To recover from a failed slot-card installation by removing the slot card:

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

```
admin>save network bonzo 971001 t1
```

This saves the configuration of all the T1 profiles to a file named 971001 in the TFTP home directory on a host named `bonzo`.

2 Bring down the card, as in the following example:

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

This disables the slot card in shelf 1, slot 1.

3 Remove the card profile:

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

4 Bring the card back up:

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

5 Restore the configuration of any profiles on the card. For the T1 card in this example, you would enter the following command:

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

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

Displaying line status

To display the activity of the TAOS unit's WAN lines, enter the Line command:

```
admin> line [all|enabled] [top|bottom]
```

where

- `all` displays all lines.
- `enabled` displays enabled lines.
- `top` displays the status window at the top of the screen.
- `bottom` displays the status window at the bottom of the screen.

Figure 1-1 shows an example of a line-status window for the T3 card.

Figure 1-1. Example of a T3 card line-status window

```
 1 Connections, 1 Sessions       |"my T3"  1/15/00 LA la  la  la  la  la  la  la
 0065 FRM2-SLC MPP 09/02/1  56000|         1/15/01 LA T-------- -------- --------
                                 |         1/15/02 LA T-------- -------- --------
                                 |         1/15/03 LA T-------- -------- --------
                                 |         1/15/04 LA T-------- -------- --------
                                 |         1/15/05 LA T-------- -------- --------
                                 |         1/15/06 LA T-------- -------- --------
                                 |         1/15/07 LA T-------- -------- --------
                                 |-----------------------------------------------
                                 |M: 520  L: notice  Src: shelf-1/slot-15
                                 |
                                 | Line 28 up
                                 |
                                 |
                                 |
                                 |
 ------------------------------------------------------------------------------
 [ Next/Last Line: <up/dn arw>, Next/Last Page: <pg up/dn>, Exit: <esc> ]
```

The first entry in the right-hand area of the screen shows the overall status of the DS3 line and each of its seven component DS2 channels. One DS2 includes 4 DS1s. The other entries represent each of the component DS1s.

The Line commands put the window in line-status mode, in which the following message appears below the status window:

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

The message indicates the key sequences you can use for displaying additional information in the line status area. The Down Arrow and Up Arrow keys display the next and previous T1 line in the list, respectively. The Page Down and Page Up keys display the list a screen at a time.

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

Line status information includes the following identifiers and codes:

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

Following are the link-status codes:

Code	Description
`LA` (link active)	The line is active and physically connected
`LS` (UDS3 lines)	Loss of Signal. No signal has been detected.
`LF` (UDS3 lines)	Loss of Frame. A signal is present but is not valid for framing.
`NT`	The E1 line is active and configured as network-side equipment.
`TE`	The E1 line is active and configured as user-side equipment.
`RA` (red alarm)	The line is unconnected, improperly configured, experiencing a very high error rate, experiencing a loss-of-receive-signal, or is not supplying adequate synchronization.
`YA` (yellow alarm)	The TAOS unit is receiving a Yellow Alarm pattern, an indication that the other end of the line cannot recognize the signals the TAOS unit is transmitting.
`DF` (d-channel fail)	The D channel for a PRI line is not currently communicating.
`1S` (all ones)	A keep-alive (also known as a Blue Alarm) signal is being sent from the PRI network to the TAOS unit to indicate that the line is currently inoperative.
`ID` (idle—DS3 only)	The DS3 interface has detected an Idle Signal transmitted from the other side. This generally indicates that the line is provisioned but is not in use.
`WF` (wrong framing—DS3 only)	The DS3 interface has detected that the other side is using a framing format that differs from the one the local DS3 interface is configured for (C-bit-parity or M13).

Following are the channel-status codes:

Code	Description
. (period)	The channel is not available because of one of the following reasons: • Line is disabled • Channel has no physical link • Channel does not exist • Channel configuration specifies that it is unused • Channel is reserved for framing (first E1 channel only)
* (asterisk)	The channel is connected in a current call.
- (hyphen)	The channel is currently idle (but in service).
b	The channel is a backup NFAS D channel (T1 PRI only).
c	The channel is currently not available because it is in the process of clearing the most recent call, or because it is in the process of sending echo cancellation tones to receive a call (inband signaling on T1 only).
d	The TAOS unit is dialing from this channel for an outgoing call.
r	The channel is ringing for an incoming call.
m	The channel is in maintenance/backup mode (ISDN and SS7 only).
n	The channel is nailed.
o	The channel is out of service (ISDN and SS7 only).
s	The channel is an active D channel (ISDN only).

Following are the channel-type codes:

Code	Description
E	E1 line
I	T1 PRI signaling
N	All other NFAS types
P	NFAS Primary
S	NFAS Secondary
T	T1 inband signaling

Additional option for displaying line status

The Line command can display line status on screen with paged output (the output is passed to a `more` function before display) and supports the grep-like capability of searching for particular strings.

If you use the Line command without options, or with the `all`, `enabled`, `top`, or `bottom` arguments, it opens the Line status window. With the `-p` option, the command displays the status information at the command line.

To use the Line command, you must have system permissions. The Line command supports the following syntax:

```
admin> help line
line usage: line [ [all | enabled ] [ top | bottom] ] | [ -p ]
```

Option	Description
-p	Print line status information 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 DS0 Channel Status          Signaling Type
1/01/01 ACTIVE      --  LOOP ........ ........ ........  inband
1/01/02 RED ALARM  LOC   --  ........ ........ ........  r1-inband
1/01/03 ACTIVE      --   --  -------- -------- --------  inband
1/01/04 RED ALARM   --   --  ........ ........ ........  isdn-nfas
1/01/05 RED ALARM  LOC   --  ........ ........ ........  inband
1/01/06 DISABLED    --   --  @@@@@@@@ @@@@@@@@ @@@@@@@@  inband
1/01/07 DISABLED    --   --  @@@@@@@@ @@@@@@@@ @@@@@@@@  inband
1/01/08 DISABLED    --   --  @@@@@@@@ @@@@@@@@ @@@@@@@@  inband
```

Following is sample output for E1 lines:

```
admin> line -p

Address Line State CARR LOOP DS0 Channel Status        Signaling Type
1/14/01 ACTIVE      --   --  .------- -------- s------- e1-indian-signa
1/14/02 RED ALARM  LOC   --  ........ ........ ........ e1-dpnss-signal
1/14/03 ACTIVE      --   --  .------- -------- s-------e1-indian-signa
1/14/04 DISABLED    --   --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
1/14/05 DISABLED    --   --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
1/14/06 DISABLED    --   --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
1/14/07 DISABLED    --   --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
1/14/08 DISABLED    --   --  @@@@@@@@ @@@@@@@@ @@@@@@@@ @@@@@@@@
```

The command displays the following line status information:

Output field	Description
Address	Shelf/Slot/Line number of the line. This information was displayed in the Line window in previous releases, and is documented in the *APX 8000/MAX TNT Reference*.
Line State	Status of the line. This information was displayed in the Line window in previous releases, and is documented in the *APX 8000/MAX TNT Reference*. In addition, the LB line-state indicator has been added to indicate that an E1 line is looped back via the `fe-loop` command on the E1 card.
CARR	(Carrier). If the system detects a loss of carrier on a line, `LOC` is displayed. If the line sees carrier, it displays dashes (`--`).

Output field	Description
LOOP	(Loopback status). If the line is locally looped, LOOP is displayed. Otherwise, the column contains dashes (--).
DS0 Channel Status	State of the individual DS0 lines. This information was displayed in the Line window in previous releases, and is documented in the *APX 8000/MAX TNT Reference*.
Signaling Type	The type of signaling in use on the line. This information was displayed in the Line window in previous releases, and is documented in the *APX 8000/MAX TNT Reference*.

Administering DS3-ATM cards

The DS3ATM#lines, Framer, and ATMDumpCall commands allow you to perform diagnostics on the DS3-ATM card.

Displaying DS3-ATM line status

This command uses the following syntax:

```
admin> ds3atmlines -option
```

where **-option** may be one of the following:

Option	Effect
-a	Displays all available DS3-ATM lines.
-d	Displays disabled DS3-ATM lines.
-f	Displays free DS3-ATM lines.
-u	Displays in-use DS3-ATM lines.

In the following example, the DS3-ATMlines command displays all DS3-ATM lines:

```
admin> ds3atmlines -a
All DS3-ATM lines:
                                  (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1  4  1 }        (Up      Idle    UP      UP     00000)
```

Regardless of which option you enter, the DS3-ATMlines command displays the following information:

Column Name	Description
dvOp	The operational state of the DS3 line. Values can be: • Down • Up

Column Name	Description
dvUpSt	The up status of the DS3 line. Values can be: • Idle • Reserved • Assigned
dvRq	The required state of the DS3 line. Values can be: • Down • Up
SAdm	The desired state of the device. Values can be: • Down • Up
nailg	The nailed group that this line is assigned to.

Using the Framer command

The Framer command is a low-level management tool for use during diagnostic sessions with the DS3-ATM card. For example, to use the Framer command on a DS3 card on shelf 1 in slot 3, first enter the Open command as follows:

```
admin> open 1 3
```

Then, enter the Framer command:

```
ds3-atm-1/3> framer -option
```

where ***-option*** is one of the following:

Option	Effect
-t	Toggles debug output.
-d	Dump ATM framer chip status information. The information this command displays is also available from the status lights on the card and in the DS3-ATM-Stat profile.
-l	Toggle a local loopback.
-r	Toggle a remote loopback.
-s	Synchronize to the DS3-ATM profile. The TAOS unit automatically re-reads the line configuration whenever it comes up.
-c	Clear the error counters.
-?	Displays this summary.

For example, to view overall status information about the DS3-ATM line, enter the Framer command with the -d option:

```
ds3-atm-1/4> framer -d
Framer is Enabled

RED_ALARM_LED   : Off
YELLOW_ALARM_LED: Off
```

```
AIS_LED         : Off
OOF_LED         : Off
ACTIVE_LED      : On

F-Bit  Error Counter: 35
P-Bit  Error Counter: 20
C-PBit Error Counter: 10
FEB    Error Counter: 51
BPV    Error Counter: 12
EZD    Error Counter: 39
```

Following are the Framer command output fields with descriptions:

State	Description
Red_Alarm_LED	On indicates the line is not connected, or it is improperly configured, experiencing a very high error rate, or supplying inadequate synchronization.
Yellow_Alarm_LED	On indicates the card is receiving yellow-alarm from far end.
AIS_LED	On indicates the card is receiving alarm indication signal
OOF_LED	On indicates the near end is in an out of frame condition.
Active_LED	On indicates multipoint established.

The remaining parameters indicate the errors on the DS3 line. (Refer to RFC 1407 for complete description of these errors.)

Parameter	Description
F Bit Error Counter	Framing bit errors received since the last TAOS unit's reset or the error counters were cleared.
P Bit Error Counter	P-bit errors indicate that TAOS unit received a P-bit code on the DS3 M-frame that differs from the locally calculated code.
CP Bit Error Counter	For C-Bit-Parity lines indicates that number of parity errors since the last TAOS unit's reset.
FEB Error Counter	Far end block errors received since the last TAOS unit's reset.
BPV Error Count	Bipolar Violation (BPV) errors may indicate that the line sent consecutive one bits with the same polarity. It could also mean that three or more consecutive zeroes were sent or an incorrect polarity.
EZD Error Counter	Number of Excessive Zero Detect (EZD) line code violations that have occurred since the error counters were cleared.

Using the ATMDumpCall command

The ATMDumpCall command is a low-level management tool for use during diagnostic sessions with the DS3-ATM card. It allows you to view the ATM call blocks, which contain information about outgoing calls.

For example, to manage a DS3 card on the shelf 1 in slot 3, first enter the Open command as follows:

```
admin> open 1 3
```

Then, enter the ATMDumpCall command:

```
ds3-atm-1/3> atmdumpcall -option
```

where ***-option*** is one of the following:

Option	Effect
`-a`	Display all ATM call blocks, even those that are inactive.
`-l`	Display DS3-ATM line configuration information.
`-u`	Display in-use ATM call blocks.

For example, to view all ATM call blocks, enter the ATMDumpCall command with the `-a` option:

```
ds3-atm-1/3> atmdumpcall -a
atmdumpcall -a
ATM Call Block Table:
Addr.     Index Active  callID  routeID State     Vpi/Vci     Prof_Name  Sess_Up
E00C47F0  0     1       1       1       CONNECTED 1/43        atm-30-sw  Yes
E00C4834  1     1       2       2       CONNECTED 15/1023     Yossi-TNT  Yes
E00C4878  2     1       3       3       CONNECTED 1/56        Yoss-P220  Yes
E00C48BC  3     0       65535   0       INACTIVE  0/0           -        No
E00C4900  4     0       65535   0       INACTIVE  0/0           -        No
.
.
.
E00C5868  62    0       65535   0       INACTIVE  0/0           -        No
E00C58AC  63    0       65535   0       INACTIVE  0/0           -        No


ATM Free Blocks: 360
ATM Used Blocks: 0
```

Using the OAMLoop command

The OAMLoop command sends ATM operation-and-maintenance (OAM) loop-back cells on an ATM interface, to obtain information about the results of the looped cells. It uses the following syntax:

```
admin> oamloop -option
```

where option is one of the following:

Option	Description
`-e`	(End-to-End). Transmit an end-to-end OAM loop cell, to be looped by the user connection point. This option and the `-s` option are mutually exclusive, and one of them must be specified on the command line.
`-s`	(Segment). Transmit a segment OAM loop cell, to be looped by the first network connection point. This option and the `-e` option are mutually exclusive, and one of them must be specified on the command line.
`–c` *`count`*	Transmit the specified number of cells. If this argument is not specified, the count defaults to 0, which means that the cells are transmitted continuously until the administrator sends an interrupt by pressing Ctrl-C.
`–i sec`	Transmit the cells at the specified interval in seconds. If this argument is not specified, the interval defaults to one second.
`shelf`	Specifies the shelf in which the DS3-ATM card is located.
`slot`	Specifies the slot in which the DS3-ATM card is located.
`vpi`	Specifies the Virtual Path Identifier on which to transmit the looped-back cells.
`vci`	Specifies the Virtual Channel Identifier on which to send the looped-back cells.

Following is an example OAMloop command line and output:

```
admin> oamloop -c 10 -e 1 2 1 32
Received our End2End OAM loopback cell, Id=9
Received our End2End OAM loopback cell, Id=10
Received our End2End OAM loopback cell, Id=11
Received our End2End OAM loopback cell, Id=12
Received our End2End OAM loopback cell, Id=13
Received our End2End OAM loopback cell, Id=14
Received our End2End OAM loopback cell, Id=15
Received our End2End OAM loopback cell, Id=16
Received our End2End OAM loopback cell, Id=17
Received our End2End OAM loopback cell, Id=18
--- OAM loop statistics ---
10 cells transmitted, 10 cells received, 0% cell loss
```

Using the Loopback parameter

For diagnostics, you might want to loopback the DS3 interface by using the Loopback parameter in the DS3-ATM profile. While the interface is looped back, normal data traffic is interrupted. The Loopback parameter in the DS3-ATM profile supports the following settings:

Loopback settings	Effects
`No-Loopback`	This default specifies that the DS3 line is operating normally.
`Facility-Loopback`	During a facility loopback, the DS3 card returns the signal it receives on the DS3 line.
`Local-Loopback`	During a local loopback, the DS3 receive path is connected to the DS3 transmit path at the DS3 multiplexer. The transmitted DS3 signal is still sent to the network as well.

Line statistics are displayed in the DS3-ATM-Stat profile. For information about this profile, see "Using DS3-ATM-Stat profiles" on page 7-9.

To configure a loopback, proceed as follows:

1 Read the DS3-ATM profile:

```
admin> read ds3-atm {1 3 1}
DS3-ATM/{ shelf-1 slot-3 1 } read
```

2 Activate the loopback:

```
admin> set line loopback= facility-loopback
```

3 To end the loopback, set the Loopback parameter to No-Loopback:

```
admin> set line loopback = no-loopback
```

Administering Ethernet cards

For all Ethernet interfaces except the shelf controller, the TAOS unit detects and flags changes in the interface link-state. You can enable a feature in the Ethernet profile that causes automatic routing table updates based on physical link-state changes. Routes to a disabled (down) interface are deleted from the IP routing table, so alternative configured routes can be used instead, and the routes are added again when the interface comes back up. You can also choose to administratively shut down a LAN interface by disabling its Ethernet profile.

The following parameters, shown with their default settings, are related to LAN-interface link-state changes:

```
ETHERNET {shelf-N slot-N item-N}
   enabled = yes
   link-state = up
   link-state-enabled = no
```

For information about configuring a management-only Ethernet interface, see the hardware installation guide for your unit.

Enabling or disabling an Ethernet interface

The Enabled parameter in an Ethernet profile specifies whether a LAN interface is enabled (the default) or disabled. If Enabled is set to No, packets routed to and received on the interface are discarded. Note that the user-specified state is preserved across system resets.

An interface may also be disabled by using the Ifmgr command, or it may be marked as down by the Ethernet driver when Link-State-Enabled is Yes and Link-State is Down.

To enable an interface, set the Enabled parameter to Yes (the default), or use the Ifmgr Up option. Note, however, that if there are physical problems with the interface, specifying the interface as up might not enable it.

To disable an interface with the Ifmgr command, proceed as in the following example:

1 Open a session with an Ethernet card:

```
admin> open 1 4
ether-1/4> ifmgr
```

2 View the interface table:

```
ether-1/4> ifmgr -d
if  slot:if  u p ifname   mac addr      local-addr
-------------------------------------------------------------
000 0:00:000 *   pb0      000000000000 0.0.0.0/32
001 1:17:011 *   ie1-4-1  00c07b6d23f0 11.1.1.1/32
002 1:17:013 *   ie1-4-2  00c07b6d23f1 11.1.2.1/32
003 1:17:015 *   ie1-4-3  00c07b6d23f2 11.1.3.1/32
004 1:17:017 *   ie1-4-4  00c07b6d23f3 11.1.4.1/32
005 1:17:019 *   ie1-4-5  00c07b6d23f4 11.1.5.1/32
<end>
```

3 Mark the interface as down by specifying its name:

```
ether-1/4> ifmgr down ie1-4-1
```

The Ifmgr display indicates that the interface is disabled by displaying a dash instead of an asterisk in the Up column (u):

```
ether-1/4> ifmgr -d
if  slot:if  u p ifname   mac addr      local-add
-------------------------------------------------------------
000 0:00:000 *   pb0      000000000000 0.0.0.0/32
001 1:17:011 -   ie1-4-1  00c07b6d23f0 0.0.0.0/32
002 1:17:013 *   ie1-4-2  00c07b6d23f1 11.1.2.1/32
003 1:17:015 *   ie1-4-3  00c07b6d23f2 11.1.3.1/32
004 1:17:017 *   ie1-4-4  00c07b6d23f3 11.1.4.1/32
005 1:17:019 *   ie1-4-5  00c07b6d23f4 11.1.5.1/32
<end>
```

Note: A disabled Ethernet interface is also shown with a dash in Netstat command output.

To mark an interface as up, enter a command similar to the following:

```
ether-1/4> ifmgr up ie1-4-1
```

For more information about the Ifmgr command, see “IFMgr” on page 4-16.

Specifying IP routing-table link states

The Link-State-Enabled parameter signifies whether the value of the Link-State parameter affects the IP routing tables. If it is set to Yes, routes to an interface are deleted when the link state is down, and added back when the interface comes back up again. If the parameter is set to No (the default), packets are routed to the interface regardless of its link-state. If the interface is down, packets are discarded rather than transmitted over using an alternative route.

Displaying physical link-state

The Link-State parameter shows the physical state of the LAN interface: up or down. The parameter can only be set by the Ethernet driver. A LAN interface is down if it cannot transmit or receive network traffic (for example, if the Ethernet cable is unplugged or the Ethernet hub on that interface is down). For the shelf-controller Ethernet interface, the value of the Link-State parameter is set to Unknown.

Checking multiple IP interfaces on an Ethernet port

In the following Ifmgr command output, the physical interface 1-12-1 has two IP-Interface profiles associated with it. The first is named `ie1-12-1` (the default profile), and the second is named `ie1-12-1-1`:

```
admin> ifmgr -d
bif slot sif u m p ifname     host-name  remote-addr       local-addr
-------------------------------------------------------------------------
000 1:17 000 *     ie0        -          0.0.0.0/32        200.168.6.188/32
001 1:17 001 *     lo0        -          0.0.0.0/32        128.0.0.1/32
002 0:00 000 *     rj0        -          0.0.0.0/32        128.0.0.2/32
003 0:00 000 *     bh0        -          0.0.0.0/32        128.0.0.3/32
004 0:00 000 *     local      -          0.0.0.0/32        128.0.0.1/32
005 0:00 000 *     mcast      -          0.0.0.0/32        225.0.0.0/32
006 1:12 001 *     ie1-12-1   -          0.0.0.0/32        10.5.6.7/32
007 1:12 002 *     ie1-12-2   -          0.0.0.0/32        0.0.0.0/32
008 1:12 003 *     ie1-12-3   -          0.0.0.0/32        0.0.0.0/32
009 1:12 004 *     ie1-12-4   -          0.0.0.0/32        0.0.0.0/32
010 1:12 005 *     ie1-12-1-1 -          0.0.0.0/32        10.9.1.212./24
```

Administering T1 and T3 cards

TAOS unit T1and T3 cards are all administered in much the same way. In most cases, administration of the individual T1 lines on the three cards is identical. Table 1-1 briefly describes the different methods you can use to manage the T1 and T3 cards and show where each method is discussed in this manual.

Table 1-1. T1-line maintenance tasks

Task/section of this manual	Description	Associated parameter or command
“Deactivating PRI lines or T1 channels” on page 1-19.	Deactivating a PRI line allows you to gradually take a line or channels out of service.	Maintenance-State parameter Quiesce command
“Specifying FDL” on page 1-20.	Your T1 service provider can use Facilities Data Link (FDL) to monitor the status of your line.	FDL parameter

Table 1-1. T1-line maintenance tasks (continued)

Task/section of this manual	Description	Associated parameter or command
"Checking the status of T1 channels" on page 1-20.	Display the administrative state and nailed-group assignment of the T1 channels.	T1channel command
"Displaying DS1-level diagnostics for T1 cards" on page 1-21.	Display T1 channel errors.	T1-Stats command
"Verifying proper hardware functionality" on page 1-23.	Loopback the T1 line.	FE-Loop

Deactivating PRI lines or T1 channels

Deactivating (quiescing) a PRI line takes the line out of service by removing channels from service as active calls disconnect. The switch used by the carrier affects whether the line is taken out of service or busied out. For details, see the Quiesce command description in the *APX 8000/MAX TNT Reference*.

You can deacativate a line by using either of the following methods:

- Maintenance-State parameter in the T1 profile
- Quiesce command

Restoring a line or channel that has been quiesced can take up to 10 minutes.

Using the Maintenance-State parameter

To quiesce a line with the Maintenance-State parameter, proceed as in the following example:

```
admin> set line maintenance-state=yes
admin> write
T1/{ shelf-1 slot-2 1 } written
```

Using the Quiesce command

You can enter the Quiesce command to deactivate a PRI line, port, or channel. The command uses the following syntax:

```
admin>quiesce -d|e|r|q|t line
```

where

- `-d` quiesces a single DS0 channel.
- `-e` restores a quiesced DS0 channel.
- `-r` *line* restores the quiesced line.
- `-q` *line* quiesces a PRI line.
- `-t` toggles the diagnostic display.

For example, to deactivate a T1 PRI line at port 4 of a card installed in slot 2:

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

Restoring a line or channel that has been deactivated can take up to 3.5 minutes, because only one service message per channel is sent to the switch, at a rate of one per second.

To restore the line deactivated in the preceding example:

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

Following is an example of deactivating a single channel:

```
admin> quiesce -d {{1 2 4} 1}
```

Specifying FDL

The facilities data link (FDL) is used by the telephone company to monitor the quality and performance of T1 lines. If your carrier's maintenance devices require regular data-link reports, and if the line is not configured for D4 framing, you can specify the type of protocol to use (AT&T, ANSI, or Sprint).

You cannot use FDL reporting on a line configured for D4 framing. However, you can obtain D4 and ESF performance statistics in the FDL Stats windows or the DSX MIB, even if you do not choose an FDL protocol. (For further information, see the Frame-Type parameter description in the *APX 8000/MAX TNT Reference*).

Note: DS3-level FDL capabilities such as the Far-End Alarm and Control Channel (FEAC) and Path Maintenance Data Link are currently unsupported.

To specify the type of FDL, proceed as in the following example:

```
admin> read t1 {1 2 1}
T1/{ shelf-1 slot-2 1 } read
admin> set fdl = [none|at&t|ansi|sprint]
admin> write
```

Checking the status of T1 channels

To show T1-channel information, enter the T1Channels command. Use the following syntax:

```
admin> t1channels - a|d|c|i
```

where

- **-a** displays all available channels.
- **-d** displays the disabled channels.
- **-c** displays all possible channels.
- **-i** displays in-use channels.

For example, to display all T1 channels available, use the `-a` option:

```
admin> t1channels -a
T1 channels available for use:
                                    (dvOp  dvUpSt  dvRq  sAdm
```

```
nailg)
  Channel { {  1  1  3 }  1 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 }  2 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 }  3 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 }  4 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 }  5 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 }  6 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 }  7 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 }  8 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 }  9 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 } 10 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 } 11 }   (Up    Idle    UP    UP
00000)
  Channel { {  1  1  3 } 12 }   (Up    Idle    UP    UP
00000)
```

To display information about which T1 channels are in use:

```
admin> t1channels -i

T1 channels allocated/in-use:
                                (dvOp  dvUpSt  dvRq  sAdm nailg)
  Channel { {  1  1  1 }  1 }   (Up    Assign  UP    UP   00000) I
  Channel { {  1  1  1 }  9 }   (Up    Assign  UP    UP   00006) I
  Channel { {  1  1  1 } 10 }   (Up    Assign  UP    UP   00006) I
  Channel { {  1  1  1 } 11 }   (Up    Assign  UP    UP   00006) I
  Channel { {  1  1  1 } 12 }   (Up    Assign  UP    UP   00006) I
  Channel { {  1  1  1 } 13 }   (Up    Assign  UP    UP   00006) I
  Channel { {  1  1  1 } 14 }   (Up    Assign  UP    UP   00006) I
  Channel { {  1  1  1 } 15 }   (Up    Assign  UP    UP   00006) I
  Channel { {  1  1  1 } 16 }   (Up    Assign  UP    UP   00006) I
  Channel { {  1 10 10 }  1 }   (Up    Assign  UP    UP   00005) I
```

Displaying DS1-level diagnostics for T1 cards

The T1-Stats command reports DS1-level line errors. Before entering the command, use the Open command to open a session with the installed card. For example, to open a session with a card in shelf 1, slot 13:

```
admin> open 1 13
```

Then enter the T1-Stats command. The following example shows the command's syntax:

```
t1-1/13> t1-stats
t1-stats [ -c ] <line>  get error statistics for the line
    -c: reset statistics to zero
```

To view DS1-level statistics on 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
```

Table 1-2 explains the T1-Stats fields.

Table 1-2. T1-Stats command fields

Field	Event that increments the field
CRC Errors	Indicates that a CRC-6 checksum shows data corruption in the signal.
Frame Slips	The TAOS unit receives T1 data at a frequency higher or lower than 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	Framing bit errors occur when the TAOS unit receives T1 data at a frequency higher or lower 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.
Out of Frame Events	The TAOS unit no longer detects a framing pattern in the receiving signal, or it detects a pattern at a different relative offset than expected.
Line Code Violations	The TAOS unit detected either a Bipolar Violation or Excessive Zeros, which means that one of the low-level T1 rules for encoding data was violated in the received signal.

The following example shows how to view and reset the statistics to zero on line 2:

```
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 `Statistics cleared` message at the end of the display indicates that the statistics have been reset to 0 (zero), because the command included the `-c` option.

Verifying proper hardware functionality

When a T1 line is looped back to the network, either as a result of the FE-Loop diagnostic command issued from the T1 card command line interface or as a result of loopback requests received from the network, the T1 line status display on the shelf controller shows the `LB` (loopback) status for the line.

The following examples demonstrate the use of the FE-Loop command:

To verify that the hardware is functioning properly, perform a local loopback by using the FE-Loop command with the `in` option. For example, to internally loop back the first DS1 in slot 1:

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

You can use this command when the line is in RA state. After looping back the line internally, state should change to LA. Note that the T3 card does not support the FE-Loop `in` option.

To turn the internal loopback off:

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

To cause the unit to transmit the received signal back towards the network, enter the following command:

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

The receive side of the T1 is not bridged to the APX 8000. This command can be useful in testing the path to the TAOS unit by:

- Verifying that the switch can synchronize to its own returned signal.
- Supporting test equipment that sends out a test pattern, such as a Quasi-Random Signal (QRS), and verifying that the pattern is received unmodified.

To turn the remote loopback off:

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

T1 and T3 slot card performance monitoring parameters

The following sections provide information on T1 and T3 slot card performance monitoring parameters. For additional information on loopback parameter values, see the *APX 8000/MAX TNT Reference*.

Loopback parameter values

The following parameter is supported in the T3 profile and controls loopback testing on the interface.

Parameter	Specifies
Loopback	Loopback testing options. • `No-Loopback` (default value)—No loopback. • `Line-Loopback`—Loop the DS3 outwards (downstream). • `Local-Loopback`—Loop the DS3 inwards (internally).

Example: `set Loopback = No-Loopback`

Location: T3 {shelf-***N*** slot-*N* N}

Channelized T3 slot card parameters

The following parameters in the T-Stat profile support diagnostic functions on channelized T3 slot cards.

Parameter	Specifies
Loss-Of-Signal	Whether there is a loss of signal on the line. • `False`—No loss of signal. • `True`—Loss of signal.

Example: `set Loopback = No-Loopback`

Location: T3 {shelf-***N*** slot-*N* N}

Loss-Of-Frame	Whether there is a loss-of-frame signal on the line. • `False`—No loss of frame signal. • `True`—Loss of frame signal.

Example: `loss-of-signal = False`

Location: T3-Stat {shelf-***N*** slot-*N* N}

Yellow-Receive	Whether the TAOS unit is receiving a loss-of-frame signal from the remote end (also known as a Yellow Alarm). • `False`—No loss of frame from the remote end. • `True`—Loss of frame from the remote end.

Example: `yellow-receive = False`

Location: T3 {shelf-***N*** slot-*N* N}

Ais-Receive	Whether the remote end is sending an alarm indication signal. • `False`—No alarm indication signal from the remote end. • `True`—Alarm indication signal from the remote end.

Example: `ais receive = False`

Parameter	Specifies

Location: T3 {shelf-***N*** slot-*N* N}

Using DS3 diagnostics

The DS3Link command is a low-level management tool for use during diagnostic sessions with the T3 card. To open a session with the installed T3 card, use the Open command.

For example, to manage a T3 card on shelf 1 in slot 15:

1 Enter the Open command as follows:

```
admin> open 1 15
```

2 Enter the DS3Link command:

```
t3-1/15> ds3link -option
```

where **-*option*** is one of the following:

Option	Effect
`-a`	Displays current DS3 line alarms.
`-b on`	Transmits a DS3 Alarm Indication Signal (blue alarm).
`-b off`	Stops transmitting a DS3 Alarm Indication Signal (blue alarm).
`-c`	Displays and clears line error statistics.
`-d 1 - 7`	Displays current DS2 line state.
`-i on`	Internally loops back the DS3 payload.
`-i off`	Halt internal loop back.
`-l off`	Externally loops back the DS3 payload.
`-l off`	Halt external loop back.
`-s`	Displays line error statistics without clearing.
`-t`	Toggles debug output.
`-?`	Displays this summary.

3 To display alarms on the line:

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

A display of `true` for C-bit parity framing does not indicate an alarm state, but that the far end is using C-bit parity.

4 To display and clear line error statistics:

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

5 To display the line state of the third DS2:

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

Performing an external loopback

To perform an external loopback test, use the `-l` option as follows:

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

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

Performing an internal loopback

An internal DS3 loopback connects the DS3 receive path to the DS3 transmit path at the DS3 line. The transmitted DS3 signal is still sent to the network.

To perform an internal loopback test, use the `-i` option as follows:

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

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

Note: DS1 external loopbacks can be invoked manually with the FE-Loop command on the DS3 card. In addition, you can display DS1 error statistics with the T1-Stats command. To use

these commands, first use the Open command to open a session with the card, as described in "Opening a session with a slot card" on page 1-3.

Administering E1 cards

The E1-Stats command reports DS1-level line errors on E1 cards. Before entering it, use the Open command to open a session with the installed card. For example, to open a session with a card in shelf 1, slot 13:

```
admin> open 1 13
```

Then enter the E1-stats command. The following example shows the command's syntax:

```
e1-1/13> e1-stats
e1-stats [ -c ] <line>  get error statistics for the line
    -c: reset statistics to zero
```

To view DS1-level statistics on the first line on the card:

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

To view and reset the statistics to 0 (zero) on line 2:

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

The `Statistics cleared` message at the end of the display indicates that the statistics have been reset to 0 (zero) because the command included the `-c` option. Table 1-3 explains the E1-Stats fields.

Table 1-3. E1-Stats command fields

Field	Event that increments the field
CRC Errors	A CRC-6 checksum shows data corruption in the signal.
Frame Slips	The TAOS unit receives E1 data at a frequency higher or lower than the internal line clock. In the process of realigning itself to the transmitter, the TAOS unit can skip or repeat a frame.

Table 1-3. E1-Stats command fields (continued)

Field	Event that increments the field
Framing Bit Errors	Framing bit errors occur when the TAOS unit receives E1 data at a frequency higher or lower 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.
Out of Frame Events	The TAOS unit no longer detects a framing pattern in the receiving signal, or it detects a pattern at a different relative offset than expected.
Line Code Violations	The TAOS unit detected either a Bipolar Violation or Excessive Zeros, which means that one of the low-level E1 rules for encoding data was violated in the received signal.
Far end block errors	The far end reported an error in an E1 frame transmitted by the TAOS unit.

Administering UDS3 cards

The UDS3lines and UDS3dump commands enable you to monitor the UDS3 card.

Using the UDS3lines command

This command uses the following syntax:

```
admin> uds3lines -option
```

where ***-option*** may be one of the following:

Option	Effect
`-a`	Displays all available UDS3 lines.
`-d`	Displays disabled UDS3 lines.
`-f`	Displays free UDS3 lines.
`-u`	Displays in-use UDS3 lines.

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

```
admin> uds3lines -a
 All UDS3 lines:
                                  (dvOp   dvUpSt  dvRq    sAdm
nailg)
  Line    {    1 13  1 }         (Up      Idle    UP      UP
00131)
```

Regardless of which option you enter, the UDS3lines command displays the following information:

Column Name	Description
dvOp	The operational state of the UDS3 line. Values can be: • Down • Up
dvUpSt	The up status of the UDS3 line. Values can be: • Idle • Reserved • Assigned
dvRq	The required state of the UDS3 line. Values can be: • Down • Up
SAdm	The desired state of the device. Values can be: • Down • Up
nailg	The nailed group that this line is assigned to.

Using the UDS3Dump command

The UDS3dump card-level command displays the information about the DS3 interface. To use this command, first open a session to the UDS3 card, then issue the UDS3dump command, using the following syntax:

```
uds3-1/11> uds3dump interval
```

where ***interval*** may be one of the following:

Option	Effect
0	Displays the DS3 MIB (RFC 1407) dsx3CurrentTable.
1-96	Displays the DS3 MIB (RFC 1407) dsx3IntervalTable.
97	Displays the DS3 MIB (RFC 1407) dsx3TotalTable.

In the following example, the UDS3dump command displays the current interval table:

```
uds3-1/13> uds3dump 0
Index PESs  PSESs SEFSs UASs  LCVs  PCVs  LESs  CCVs  CESs CSESs
-------------------------------------------------------------------
0     0     0     0     1     0     0     0     0     0     0
```

The output contains the following fields (refer to RFC 1407 for complete description of these errors):

Field	Description
PESs	A P-bit errored second is a second during which one of the following error conditions occurs: • A P-Bit error • An out of frame error • An incoming A1S signal Note that the count is not incremented by the number of unavailable seconds.
PSESs	A P-bit severely errored second is a second during which one of the following error conditions occurs: • There are 44 or more P-Bit errors • An out of frame error • An incoming A1S signal Note that the count is not incremented by the number of unavailable seconds.
SEFSs	A severely errored framing second is a second during which one of the following error conditions occurs: • An out of frame error • An incoming A1S signal
UASs	The number of seconds the interface is unavailable. Note that only LES and SEFS errors are counted while the interface is unavailable.
LCVs	A line coding violation error is the sum of bipolar (BPV) and excessive zero (EXZ) errors. An excessive zero error increments the count by one no matter how many zeros are transmitted.
PCVs	P-bit errors indicate that TAOS unit received a P-bit code on the DS3 M-frame that differs from the locally calculated code.
LESs	A line errored seconds is a second during which one of the following error conditions occurs: • A C-bit coding violation error • A loss of signal error
CCVs	A C-bit coding violation error indicates a parity error.
CESs	A C-bit errored second is a second during which one of the following error conditions occurs: • A C-bit coding violation error • An out of frame error • An incoming A1S signal This applies only to SYNTRAN and C-bit Parity DS3 lines. Note that the count is not incremented by the number of unavailable seconds.

Field	Description
CSESs	A C-bit severely errored second is a second during which one of the following error conditions occurs: • There are 44 or more C-bit coding violation errors • An out of frame error • An incoming A1S signal This applies only to SYNTRAN and C-bit Parity DS3 lines. Note that the count is not incremented by the number of unavailable seconds.

Administering modems

The TAOS unit provides diagnostic commands to display modem status, bring modems or channels up or down, or quiesce modems.

Displaying modem status

To show modem information, enter the Modem command:

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

where

- `-a` Displays all available modems.
- `-d` Displays the disabled channels.
- `-f` Displays failed or non-existent modems.
- `-g` Displays available good modems.
- `-i` Displays in-use modems.
- `-m` Displays all possible modems.
- `-s` Displays suspect modems.

For example, to see which modems are in use:

```
admin> modem -i
Modems allocated/in-use
                              (dv0p dvUpSt DvRq sAdm)
Modem {1 14 1}                (Up   Assign UP   UP )
```

For more information about the Modem command refer to the *APX 8000/MAX TNT Reference*.

Bringing a modem or channel up or down

To administratively up or down a device, you can use the Device command or a Device-State profile. (For discussion of Device-State profiles, see “Using the Device-State profile” on page 7-6.)

For example, to administratively down modem 24 in slot 3 on shelf 1:

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

To bring the modem back up:

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

Disabling a modem

To disable a modem:

1. Read in the LAN Modem profile. For example:

```
admin> read LAN-Modem
LAN-MODEM/{ shelf-1 slot-2 0 } read
```

2. Disable the modem:

```
admin> set modem-disable-mode 1= disable
```

3. Write the profile to commit your changes:

```
admin> write
LAN-MODEM/{ shelf-1 slot-2 0 } written
```

Deactivating digital modems

The system creates a LAN-Modem profile for each installed modem card. Removing or shutting down a modem card does not delete this profile or change its contents. You can use the LAN-Modem profile to quiesce digital modems. Deactivating (or quiescing) a modem makes it available for maintenance in a graceful way, not by tearing down the current connection, but by taking the channel out of service as soon as the connection is dropped.

To use a LAN-Modem profile, first open it and list its contents. For example:

```
admin> read lan {1 6 0}
LAN-MODEM/{ shelf-1 slot-6 0 } read

admin> list
physical-address* = { shelf-1 slot-6 0 }
modem-disable-mode = [ enable enable enable enable enable +
```

Then, to deactivate a modem, list its Modem-Disable-Mode setting and change it to `disable`. For example:

```
admin> list modem-dis
...(All 48 modem settings are displayed)

admin> list 20
admin> set = disable
admin> write
LAN-MODEM/{ shelf-1 slot-6 0 } written
```

To bring the modem back up:

```
admin> set = enable
```

```
admin> write
LAN-MODEM/{ shelf-1 slot-6 0 } written
```

Note: When you deactivate a modem, you can also deactivate an arbitrary idle T1 channel at the same time by using the Dis-Channel setting. For details, see the *APX 8000/MAX TNT Reference*.

TAOS System Administration

2

This chapter explains how to perform common system administration tasks on your TAOS unit. It focuses on tasks you can perform on the system as a whole, such as resetting the unit, setting the time and date, configuring logging, and backing up and restoring a configuration.

For information about managing the TAOS slot cards, see Chapter 1, “Administering Slot Cards.”

Logging into the TAOS unit

To administer the system, you can log in from a PC connected to the TAOS unit’s serial port, or from a workstation that has Telnet access to the system. When you log in, you are prompted for a user name:

```
User:
```

To log in with administrative (superuser) privileges, enter the default password (`Lucent`) assigned to the TAOS unit Admin login at the factory:

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

The name specified in the Admin User profile appears as your system prompt. For example:

```
admin>
```

If you are already connected to the TAOS unit as a different user, use the Auth command to log in as the administrator:

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

Note: Because the Admin login has superuser privileges, you should change the default password immediately. Be sure to write down the password you assign and store it in a safe place.

Following is an example of changing the password for the Admin login:

```
admin> read user admin
USER/admin read
admin> set password = top-secret
admin> write
USER/admin written
```

All subsequent administrator logins will be required to supply the new password. (For more information about configuring User profiles, see Chapter 5, “Creating User Profiles.”)

Securing the serial port

By default, when users connect to the serial port on the shelf controller, they are logged in with the Admin User profile. To secure the serial port with a username and password, proceed as follows:

1 Read the Serial profile:

```
admin>read serial { 1 17 2}
```

2 Set the User-Profile to null:

```
admin>set user =
```

3 Set Auto-Logout to Yes:

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

This automatically logs out the current User profile if DTR is lost on the serial port.

4 Write the profile:

```
admin>write
```

Now users connecting to the serial port must supply a valid username and password for access to the TAOS unit.

Specifying a management-only Ethernet interface

You can specify that one of the TAOS unit's Ethernet interfaces is for management only. The management-only interface can be the shelf-controller port or a port on an installed Ethernet card. Following is the relevant parameter, which is shown with its default setting:

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

Setting Management-Only-Interface to Yes means that incoming traffic on the interface terminates in the system itself. It 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.

To configure a management interface, proceed as in the following example:

```
admin> read ip-int {{ 1 12 1 } 0}
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } read

admin> set management-only = yes

admin> write
IP-INTERFACE/{ { shelf-1 slot-12 1 } 0 } written
```

The IfMgr –d command displays a Management Only field to reflect the port's status.

Overview of TAOS commands

Each card in the TAOS unit has its own set of commands. The commands on the shelf controller typically affect the operation of the entire system. The commands on particular cards, such as the T1 or Ethernet cards, affect only the cards themselves. This section explains the commands available on the shelf controller.

For information about commands available on the cards, see Chapter 1, "Administering Slot Cards," or the *APX 8000/MAX TNT Reference*. For information on debug commands, see Chapter 4, "Using Debug Commands."

Command permission-levels

Commands are organized by permission levels, as described in Table 2-1. A user gains access to a particular command by logging in to the TAOS unit by means of a user profile that

specifies the required permission level. (To create a User profile, see Chapter 5, "Creating User Profiles.") By default, the Admin profile specifies permission to execute all commands.

Table 2-1. Permission levels

Permission level	Description
Code	Allows you to format and manage the PCMCIA cards that store the system software.
Debug	Specialized commands used to troubleshoot the cards. Under most circumstances, these commands are not required for correct operation of the TAOS unit, and in some circumstances might produce undesirable results. (For information about the debug commands, see Chapter 4, "Using Debug Commands."
Diagnostic	Commands used to monitor the TAOS unit and its cards.
System	Commands that allow you to manage and configure the TAOS unit.
Term-Serv	Accesses the TAOS unit's terminal server.
Update	Commands that allow you to update the system configuration.
User	Simple commands available to all users that allow log in.

Commands overview

Table 2-2 briefly describes the TAOS commands available on the shelf-controller. Many of the commands are used in later sections of this manual to perform certain system administration tasks. For complete details of each command, see the *APX 8000/MAX TNT Reference*.

Table 2-2. TAOS system administration commands

Command Name	Permission Level	Effect
?	User	Displays a list of commands.
Arptable	System	Displays or modifies the TAOS unit's Address Resolution Protocol (ARP) table.
Auth	User	Selects a new User profile.
Callroute	Diagnostic	Displays the call-routing database.
Clear	User	Clears the terminal session screen and places the system prompt at the top row of the VT100 window.
Clock-Source	Diagnostic	Displays clock-source statistics.
Clr-History	System	Clears the fatal-error history log.

Table 2-2. TAOS system administration commands (continued)

Command Name	Permission Level	Effect
Connection	System	Displays the connection-status window.
Date	Update	Sets the system date.
Debug	Diagnostic	Enables or disable diagnostic output.
Delete	Update	Permanently deletes a profile from local storage.
Device	Diagnostic	Brings a device up or down.
Dir	System	Lists profiles and profile types.
Dircode	System	Shows contents of PCMCIA card code.
Dnstab	System	Displays DNS table entries.
DS3ATMlines	System	Displays DS3-ATM line information.
Ether-Display	Diagnostic	Displays contents of received Ethernet packets.
Help	User	Displays help about a particular command.
Fatal-History	System	Lists fatal-error history log.
Format	Code	Prepares a flash card for use.
Fsck	Code	Verifies the filesystem on a PCMCIA flash card. If errors are detected, they are reported. No errors are fixed.
Get	System	Displays fields in a profile.
HDLC	System	Displays HDLC-channel information.
If-Admin	Diagnostic	Administer an interface.
IGMP	System	Displays IGMP multicast statistics.
IP-pools	System	Displays the status of the IP address pools configured in the IP-Global profile.
Ipcache	System	Displays IP route caches.
IProute	System	Enables you to manually add or delete IP routes. Routing table changes made by using this command are not remembered across system resets.
Line	System	Displays the line status window.

Table 2-2. TAOS system administration commands (continued)

Command Name	Permission Level	Effect
List	System	Lists fields in working profile.
Load	Update	Uploads code or saved configuration to flash.
Log	System	Invokes/controls the event log window.
Modem	System	Displays modem information.
Netstat	System	Displays routing or interface tables.
New	System	Creates a new profile.
NSlookup	Diagnostic	Resolves the IP address of a specified host name by performing a DNS lookup.
Nvram	Update	Clears configuration and reboot system
Open	Diagnostic	Starts session with slot card.
OSPF	System	Displays information related to OSPF routing, including Link-State Advertisements (LSAs), border routers' routing tables, and the OSPF areas, interfaces, statistics, and routing table.
Ping	Diagnostic	Sends ICMP echo_request packets to the specified host as a way to verify that the host is up and the transmission path to the host is open.
Power	System	Displays power supply statistics.
Quiesce	System	Temporarily disables a modem or DS0 channel.
Read	System	Makes the specified profile the working profile.
Refresh	System	Refreshes the remote configuration.
Reset	Update	Reboots the system.
Save	Update	Saves profile for future restore.
Screen	System	Changes the status window display size for the current session.
Set	System	Sets a parameter's value.
Show	System	Shows shelves, slots, or items.
Slot	Diagnostic	Administers a slot card.

Table 2-2. TAOS system administration commands (continued)

Command Name	Permission Level	Effect
Status	System	Displays system status or hide status window.
T1channels	System	Displays T1 channel information.
Telnet	Diagnostic	Opens a Telnet session to another host.
Terminal-Server	Termserv	Enters terminal-server mode.
Traceroute	Diagnostic	Traces the route an IP packet follows by launching UDP probe packets.
UDS3lines	System	Displays unchannelized DS3 line information.
Uptime	Diagnostic	Displays how long the TAOS unit has been up since its last reset.
Userstat	System	Displays user-session status.
Version	System	Displays software version information.
View	System	Changes content of a status window.
Whoami	User	Displays current User profile name.
Write	Update	Writes a profile.

Displaying system and slot card uptime

The Uptime command reports how long the system and its individual cards have been up. The `slotLastChange` MIB object in the Lucent Enterprise MIB also enables network management stations to obtain uptime information.

The Uptime command uses the following syntax:

```
super->help uptime
uptime usage: uptime [ [ -a ] | [ [ shelf ] slot ] ]
uptime                  display the TNT system uptime.
uptime slot             display the TNT slot card uptime.
uptime shelf slot       display the TNT slot card uptime.
uptime -a               display the uptime for all TNT slot cards.
uptime -?               display this usage message.
```

Without an argument, the command displays system uptime. But in the following example, the command displays the uptime for all slot cards in the UP state (cards that are not in the UP state are not reported):

```
super->uptime -a
22:03:43
{ shelf-1 slot-2 }         csmx-card    3 days 05:23:08     8.0.2c5
{ shelf-1 slot-4 }      hdlc2ec-card    3 days 05:24:00     8.0.2c5
{ shelf-1 slot-5 }        madd2-card    3 days 05:23:52     8.0.2c5
{ shelf-1 slot-7 }      oc3-atm-card    3 days 05:24:18     8.0.2c5
{ shelf-1 slot-8 }      hdlc2ec-card    3 days 05:24:00     8.0.2c5
{ shelf-1 slot-9 }       ether3-card    3 days 05:24:34     8.0.2c5
{ shelf-1 slot-12 }        hdlc2-card    3 days 05:24:08     8.0.2c5
{ shelf-1 slot-13 }         csmx-card    3 days 05:23:08     8.0.2c5
{ shelf-1 slot-14 }        hdlc2-card    3 days 05:24:08     8.0.2c5
{ shelf-1 slot-15 }     hdlc2ec-card    3 days 05:24:00     8.0.2c5
{ shelf-1 slot-16 }     hdlc2ec-card    3 days 05:24:00     8.0.2c5
{ shelf-1 slot-17 }     hdlc2ec-card    3 days 05:24:00     8.0.2c5
{ shelf-1 slot-19 }      ether3-card    3 days 05:24:34     8.0.2c5
{ shelf-1 slot-20 }        hdlc2-card    3 days 05:24:08     8.0.2c5
{ shelf-1 slot-21 }        hdlc2-card    3 days 05:24:08     8.0.2c5
{ shelf-1 slot-22 }         csmx-card    3 days 05:23:08     8.0.2c5
{ shelf-1 slot-23 }           t3-card    3 days 05:24:26     8.0.2c5
{ shelf-1 slot-24 }        hdlc2-card    3 days 05:24:08     8.0.2c5
{ shelf-1 slot-25 }        hdlc2-card    3 days 05:24:08     8.0.2c5
{ shelf-1 slot-26 }         csmx-card    3 days 05:23:08     8.0.2c5
{ shelf-1 slot-27 }        hdlc2-card    3 days 05:24:08     8.0.2c5
{ shelf-1 slot-29 }      ether3-card    3 days 05:24:34     8.0.2c5
```

```
{ shelf-1 slot-30 }        csmx-card    3 days 05:23:08     8.0.2c5
{ shelf-1 slot-33 }          t3-card    3 days 05:24:26     8.0.2c5
{ shelf-1 slot-34 }     hdlc2ec-card    3 days 05:24:00     8.0.2c5
{ shelf-1 slot-36 }         8t1-card    3 days 05:24:46     8.0.2c5
{ shelf-1 slot-38 }      ether3-card    3 days 05:24:34     8.0.2c5
{ shelf-1 slot-39 }      ether3-card    3 days 05:24:34     8.0.2c5
{ shelf-1 left-controller }  shelf-controller    3 days 05:25:51 (
PRIMARY )
```

Note: The left and right controllers are both reported in the display.

Uptime displays the current time (`20:18:18` in the preceding example), identifies the slot card, the software version running on the card, and displays the length of time the system has been up, in days followed by hours:minutes:seconds. The following example shows that a csmx card in slot 2 has been up for 3 days, 5 hours, 23 minutes and 8 seconds:

```
super->uptime 1 2
20:18:18
{ shelf-1 slot-2 }         csmx-card    3 days 05:23:08     8.0.2c5
```

Displaying the system version

Use the Version command to determine which system software version is installed. For example:

```
admin> version
Software version 8.0.1
```

Viewing the factory configuration

The read-only Base profile displays the software versions, enabled features, network interfaces, and other system information. To view the Base profile, use the Get command. For example:

```
admin>get base
[in BASE]
shelf-number = 1
software-version = 8
software-revision = 0
software-level = b
manufacturer = dba-lucent-mfg
d-channel-enabled = yes
aim-enabled = yes
switched-enabled = yes
multi-rate-enabled = yes
t1-pri-conversion-enabled = yes
frame-relay-enabled = yes
maxlink-client-enabled = enabled
```

```
data-call-enabled = yes
r2-signaling-enabled = no
serial-number = 7050270
hardware-level = 0
countries-enabled = 511
domestic-enabled = yes
modem-dialout-enabled = yes
firewalls-enabled = no
network-management-enabled = no
phs-support = no
selectools-enabled = no
routing-protocols-disabled = no
apx-adsl-restricted = no
apx-sdsl-restricted = no
apx-idsl-restricted = no
xcom-ss7 = disabled
ss7asg = disabled
atmp-enabled = enabled
l2tp-enabled = disabled
pptp-enabled = disabled
ipinip-enabled = disabled
```

The Base profile displays system information that is not modified across resets. These values are read from the system ROM, security PAL, and from the hardware assembly itself. (For information about the parameters, see the *APX 8000/MAX TNT Reference*.)

Note: The shelf-number is always 1 in a single-shelf system.

Adjusting screen width

The TAOS unit allows command-line input and terminal-server banners up to 255 characters, rather than the previous limit of 80 characters. Horizontal scrolling of the command line allows viewing of commands and banners that are wider than the terminal display.

To set the width of the terminal display window for the current session, use the Screen command. To specify the width to use for every login to the command-line interface, use the Screen-Width parameter in a User profile.

Setting screen width for the current session

The Screen command enables you to specify the width of the screen. The command uses the following syntax:

```
screen -w <width>
```

The Width argument is a value from `80` to `256` and default is `80`. For example:

```
admin> screen -w 256
```

The specified screen width is the number of characters that are visible without scrolling, including the system prompt and spaces following it. For example, if the screen width is 80 characters and the prompt is `admin>` (a 6-character prompt followed by a space), the maximum number of visible characters in a command is 72. If the user enters a long command,

for example that has 100 characters, 28 of the characters will not be visible at any one time. The user can scroll to the characters not currently visible by moving the cursor left or right.

The following control sequence allows users to redraw the current line:

Control sequence	Effect
Ctrl-L, Ctrl-R	Redraw line

All existing control sequences continue to work as in previous releases. For details, see the *TAOS Command-Line Interface Guide*.

Customizing a User profile for screen width

To enable you to specify the screen width for all subsequent sessions, the following parameter (shown with its default setting) has been added to User profiles:

```
[in USER/""]
screen-width = 80
```

Parameter	Specifies
Screen-Width	Number of characters allowed on a command line or terminal-server banner. An integer from 80 (the default) to 255.

Following is an example of how to customize a user's profile for a screen width of 120 characters:

```
admin> read user admin
USER/admin read
admin> set screen-width = 120
admin> write -f
USER/admin written
```

Setting the system name

The TAOS unit sends this name to callers whenever it establishes a PPP link. The name is not used in DNS lookups.

You specify the system name in the System profile. For example, to set the TAOS unit's system name to `apx01`, proceed as follows:

```
admin> read system
SYSTEM read
admin> set name = apx01
admin> write
SYSTEM written
```

Setting the system time and date

This section explains how to set the TAOS unit's system clock. The TAOS unit can also use Simple Network Time Protocol (SNTP—described in RFC 1305) to set and maintain its system time by communicating with an SNTP server across an IP interface. For information about configuring the TAOS unit to use SNTP, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.

Use the Date command to set the system time and date if it is incorrect when the system initializes. To view the date and time, enter the Date command with no argument:

```
admin> date
Mon Dec 20 11:11:00 1999
```

To set it, append the current date and time to the Date command, in the following format:

```
yymmddhhmm
```

This format uses a two-digit number for each of the following settings: year, month, day, hour, and minute, in that order. For example:

```
admin> date 9911021743
Mon Dec 20 17:43:00 1999
```

In the year field, 00 - 89 represents years 2000 to 2089, and 90-99 represents years 1990 to 1999. For example, to set a date in the year 1999, proceed as in the following example:

```
admin> date 9910130029
Wed Oct 22 0:29:00 1999
```

To set a date in the year 2001, proceed as in the following example:

```
admin> date 0110130029
Sat Dec 25 0:29:00 2001
```

You can also Get the Timedate profile to view the information:

```
admin> get timedate
[in TIMEDATE]
time = { 17 43 34 }
date = { Monday December 2 1998 }
```

The Time and Date parameters in the Timedate profile cannot be set directly. To change their values, use the Date command as shown above.

Managing onboard NVRAM

The system configuration is stored in the onboard non volatile random access memory (NVRAM). Some error conditions might require that you clear the TAOS unit's configuration and reboot. When you clear NVRAM, the system is reinitialized and comes up unconfigured, just as it was when you first installed it.

You can then restore the configuration from a recent backup (see "Backing up and restoring a configuration" on page 2-19).

Caution: Make sure you have a recent backup before using the NVRAM command.

To see how NVRAM is being used, enter the NVRAM command with the `-u` option:

```
admin> nvram -u
```

To clear NVRAM, restoring the unit to its initial, unconfigured state, enter the NVRAM command without specifying an option:

```
admin> nvram
```

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

```
admin> nvram -t
```

Resetting the unit

When you reset the TAOS unit, it restarts and terminates all active connections. All users are logged out and the default security level, configured in the User-Profile parameter, is reactivated. In addition, a system reset can cause a WAN line to temporarily be shut down due to momentary loss of signaling or framing information.

To reset the unit, enter the Reset command:

```
admin> reset
```

During a reset, the TAOS unit runs its Power-On Self Test (POST), just as it would if the unit were power-cycled.

Viewing clock-source information

If a line is specified as the clock-source, it can be used as the source of timing information for synchronous connections, so both the sending device and the receiving device can determine where one block of data ends and the next begins. If multiple T1 lines specify that they are the clock-source (the default configuration), you can assign clock-source priority among multiple T1 lines.

To view the clock-source statistics, enter the Clock-Source command:

```
admin> clock-source

Master: slot-1/1 line 3
Source List:
    Source: slot-1/1 Available      priority: 1
```

Sources with layer 2 up, which are preferred, are marked with an asterisk. For information about configuring the clock source, see the hardware installation guide.

DOS-compatible FAT-16 flash memory format

Shelf controller PCMCIA flash memory cards use a DOS-compatible general-purpose file system. In the initial release, the file system is supported on the TAOS shelf controller PCMCIA flash cards and Intel-compatible linear flash cards, but it has been designed with a minimum of platform dependencies.

The new flash format allows for hierarchical directories and eliminates the need to revise the file system format between versions. In addition, you can read and write the data on the flash card with a standard laptop or palmtop running OS/2 or a Windows version that supports Flash Translation Layer (FTL) linear flash memory.

File formats

The file allocation table-16 (FAT-16) file system is implemented on top of FTL. For details about the formats, see *PCMCIA Media Storage Formats, Chapter 5: Flash Translation Layer Microsoft FAT12 and FAT16 volume formats.*

Note: Filenames on TAOS flash cards must be compatible with the DOS 8.3 format.

A FAT-16 file system can store a large number of files in a hierarchy of directories. After you format flash under this software version, the flash card contains a top-level directory named `/current`, which contains the currently running version of the TAOS software as well as code image files for all supported slot cards. The slot card images are extracted from the tar file and stored as individual files with a `.ffs` filename extension. For example:

```
apxsr.ffs
tnt8t1.ffs
tnthdlc2.ffs
```

The new flash format also allows you to load a new software version or configuration data to the TAOS from a laptop running Windows or OS/2, rather than from a TFTP server. Because the FAT on FTL format is supported only on linear flash cards in this release, the laptop must have FTL linear flash.

Loading file to the flash file system

The Load command supports an image type of `file` for Trivial File Transfer Protocol (TFTP) transfers to a flash card formatted for the FAT-16 format. Images of type `file` are not checked for an Internet Telnet Protocol (ITP) header, and are stored by name in the `/current` directory of the specified flash card. For example, the following command loads a voice-announcement file named `busy.au` from a TFTP server at 10.10.10.10 to the `/current` directory on flash card 1 (the default):

```
admin> load file network 10.10.10.10 busy.au
```

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 apxrel.tar
file apxrel.tar...
untaring and loading image for...
shelf controller (apxsr/apxsr.ffs)...
8t1-card (tnt8t1/tnt8t1.ffs)...
skipping t3-card (tntt3/tntt3.ffs)...
```

```
ether3-card (tntenet3/tntenet3.ffs)...
hdlc2-card (tnthdlc2/tnthdlc2.ffs)...
skipping 4swan-card (tntswan/tntswan.ffs)...
skipping 48modem-56k-card (tntmdm56k/tntmdm56k.ffs)...
skipping 48modem-card (tntmdm/tntmdm.ffs)...
done.
```

Creating directories in the flash file system

The `mkdir` command creates directories in the flash file system. The slash character (/) separates the elements of a pathname. For example, the following command creates a directory named `oldconf` at the top level of the flash card in slot 1:

```
admin> mkdir 1/oldconf
```

The following command creates a subdirectory named `config1` within the `oldconf` directory:

```
admin> mkdir 1/oldconf/conf1
```

You can move files into a directory by using the `mv` command. For example, the following command moves a file named `0001conf` to the new subdirectory on flash card 1:

```
admin> mv 1/current/0001conf 1/oldconf/conf1/0001conf
```

Checking the flash file system

The Fsck command prints a summary of file structures on the card. For example:

```
admin> fsck 2
Volume Stats:
Block Size: 512 (typical: 512)
Blocks Per Cluster: 3 (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: 96 (typically between 32 and 224)
Total Blocks: 11264
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: 29
Number of Root Dir Blocks: 6
Number of Clusters: 3745
FAT Type: Fat12
Cluster Usage
Usable Clusters: 3743
Free Clusters: 1828
Clusters lost during interrupted writes: 0
Other reserved clusters: 1909
```

Using PCMCIA flash cards

Each TAOS unit's shelf supports up to two PCMCIA flash-memory cards. The system comes with onboard NVRAM, and each flash card provides its own additional memory. At present,

the flash cards contain code for the slot cards, the shelf-controller, and profiles. The system configuration is stored in the onboard NVRAM.

The PCMCIA slots on the shelf-controller are labeled 1 (the slot on top) and 2 (the slot below).

Formatting a flash card

Before using a PCMCIA card in the TAOS unit, you must format it. First insert the card into slot 1 or slot 2 in the shelf-controller, then use the Format command. Following are examples of formatting the card in slot 1:

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

Or:

```
admin> format 1
```

Flash-card-1 is the card inserted in the leftmost of the two PCMCIA slots.

For a list of error messages that might appear when using the Format command, see “Format command messages” on page B-11.

Displaying the contents of flash

The system comes with onboard NVRAM, and each flash card provides its own additional memory. The system configuration is stored in the onboard NVRAM.

To check the slot-card images stored in the flash card code directory, use the Dircode command, as shown in the following example:

```
admin> dircode
Flash card code directory:
Card 1, directory size 16
     shelf-controller reg   good  1237961 Nov  24 12:19      8.0
             8t1-card reg   good   203393 Nov  24 12:19      8.0
              t3-card reg   good   224951 Nov  24 12:19      8.0
          4ether-card reg   good   177007 Nov  24 12:19      8.0
           hdlc2-card reg   good   640052 Nov  24 12:19      8.0
           4swan-card reg   good   425375 Nov  24 12:19      8.0
    10-unchan-t1-card reg   good   510029 Nov  24 12:19      8.0
         ds3-atm-card reg   good   444831 Nov  24 12:19      8.0
            csmx-card reg   good   806361 Nov  24 12:20      8.0
```

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

- Type of card supported
- Subtype of the code, which can be regular or diagnostic
- Status, which can be good (present and complete), write (being copied), or bad (incomplete or corrupt)

- Size of the code
- Date the code was loaded to the flash card
- Code version

For a list of error messages that might appear when using the Dircode command, see “Dircode command messages” on page B-11

Checking the file system

If the Dircode command shows a code status other than Good, or if you suspect inconsistencies in the flash card files, use the Fsck command to check the code directory. The Fsck command checks inconsistent conditions in the code directory as well as file contents on a PCMCIA flash card. For each file found, the command displays the type-name, type-number, decimal and hex byte counts, and date written to flash.

If errors are detected they are reported but not fixed. If the Fsck command reports errors, you should reformat the card and then load the code again. If necessary, download the code file again from the Lucent (Ascend) FTP server.

To check the file-system on the flash card in PCMCIA slot 1, use the Fsck command as shown in the following example:

```
super->fsck 1
Card version info 'SiliconTech                ~64MB FLASH
Card~'
Volume Stats:
  Block Size: 512 (typical: 512)
  Blocks Per Cluster: 16 (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: 512 (typically between 32
and 224)
  Total Blocks: 125952
  Media Descriptor: f0 (ignored)
Volume Info calculated from values above:
  Blocks Per Fat: 31
  Fat Start Block: 1
  Root Dir Start Block: 63
  Data Start Block: 95
  Number of Root Dir Blocks: 32
  Number of Clusters: 7866
  FAT Type: Fat16
Cluster Usage
```

```
Usable Clusters: 7864
Free Clusters: 6048
Clusters lost during interrupted writes: 0
Other reserved clusters: 1798
```

For details of the command-line options for the Fsck command, see the *APX 8000/MAX TNT Reference*.

Updating system software

For information on updating system software, see the TAOS *True Access Operating System Addendum.*

Loading specific slot-card images

The TAOS unit supports a large number of slot cards, so the Tar files containing slot-card code images might be too large to load on an 8MB flash card. The Load-Select administrative profile enables you to specify which slot-card images to load to flash when you use a Load Tar command such as the one shown below:

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

Following a system reset, the TAOS unit creates the Load-Select profile if it is not present. The profile lists the entire set of supported slot-card images and an intended load action for each card type when the image is present in a Tar file. It also contains an Unknown-Cards parameter, which represents new cards that were not supported in the previous system version.

When loading the Tar file, the system uses settings in the Load-Select profile to load only specific slot-card images. To prevent version-related problems, it then deletes code images that were present on the flash card but were not updated.

For examples of upgrade procedures using the Load-Select profile, see the TAOS *True Access Operating System Addendum*.

Following are sample contents of the Load-Select profile:

```
[in LOAD-SELECT]
unknown-cards = auto
8t1 = auto
8e1 = auto
t3 = auto
ut1 = auto
ue1 = auto
uds3 = auto
ds3-atm = auto
enet = auto
enet2 = auto
mdm-v34 = auto
mdm56k = auto
amdm = auto
anmdm = auto
```

```
hdlc = auto
hdlc2 = auto
swan = auto
```

Each parameter in the profile represents a card type, and can be set to Auto, Load, or Skip, to specify the action to take when the code image is present in a Tar file. (The Load-Select profile does not list the Shelf-Controller code, because that image is always loaded from the updated Tar file.)

- The Auto setting (the default) causes the system to load images for cards that are installed in the TAOS unit, and skip images for cards that are not installed. A card is considered present in the system if a Slot-Type profile exists for that card type. The system creates a Slot-Type profile when it first detects the presence of a card, and does not delete the profile unless the administrator uses the Slot –r command to permanently remove a card that is no longer installed in the system, or clears NVRAM. To ensure that the system does not load unnecessary images, use Slot –r to remove Slot-Type profiles for cards that are no longer installed in the system.
- The Load setting causes the system to load the image, even if there is no card of that type installed.
- The Skip setting causes the system to skip the image, even if there is a card of that type installed.

Loading an extracted code image

You can override the settings in the Load-Select profile with options to the Load command. For example, if you extract the contents of a Tar archive and then issue the following Load command:

```
admin> load mdm56k network 10.10.10.10 apxmdm56k.ffs
```

The system loads the 56K-modem image even if the Load-Select profile indicates that it should be skipped. For details on the Load command, see the *APX 8000/MAX TNT Reference*.

Backing up and restoring a configuration

The Save command saves all configured profiles, all profiles of a specified type, or a specific profile to a file on a local disk or to a file on a network host. You can then use that file to restore the TAOS unit's configuration. Note that to save passwords, you must have sufficient permissions to view password fields (for a discussion of permissions, see "Understanding command permissions" on page 5-3).

Saving the configuration to a local file

To save the TAOS unit's configuration to a file on the system you are using to access the TAOS unit, turn on the capture function in your VT100 emulation software, and enter the Save command as follows:

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

The entire configuration is written to the specified file. You might want to print a copy of the configuration for later reference.

The `-a` option saves all parameters, even those that are set to their default values.

Saving the configuration to a network host

To save the configuration on network host, you must specify the hostname and the full path of a filename, as in the following example:

```
admin> save -a network host1 /config/981001
configuration being saved to 10.65.212.19
```

In the sample command line, `host1` is the network host and `/config/981001` is the file name.

Restoring or updating the configuration

You can restore a full configuration that you saved with the Save command, or you can upload more specific configuration information, such as single profile.

To restore configuration information, use the Load command.

Restoring from a local file

Before you start the restore procedure, verify that your terminal emulation program has an autotype (or ASCII file upload) feature. Autotype allows your emulator to transmit a text file over its serial port. You should also verify that the data rate of your terminal emulation program is set to 9600 baud or lower and that the term-rate parameter in the System profile is also set to 9600 or lower, and that the Term-Rate parameter in the System profile is set to the same rate. Speeds higher than 9600 baud might cause transmission errors.

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

```
admin> load config console
```

Restoring from a network host

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

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

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

Updating the configuration

You can use the Load command to upload code for any of the slot cards to a flash card. For example, to upload new code for an eight port T1 card from a file named `8t1.ffs` on a network host named `server1`:

```
admin> load t1-8 network server1/cfg/8t1.ffs
```

Saving and Restoring to a PCMCIA flash card

To save or restore full configuration information, use the Save command, as follows.

```
super-> ? save
```

```
save  save all configuration profiles, all profiles of a
given type,
  or a specific profile by writing it in a form that can be
replayed
  to a unit to restore its configuration
 usage: save [ -a ] [ -m ] < target > [ profile-type [
profile-index ] ]
      or
 specify a list of profiles to be included in or excluded
from the
  network save operation
 usage: save [ -a ] [ -m ] network <host> <filename> [ -p |
-x profile1 profile2 ...]
   < target >: network < host > < filename >, console, flash
< device/filename >
   [ -a ]:     explicitly save all fields, even those with
default values
   [ -m ]:     use mib tags instead of field and value names
   [ -p ]:     save specified list of profiles
   [ -x ]:     save all profiles, except the specified list
```

Using the status window

The status windows provide information about what is currently happening in the TAOS unit. For example, one status window displays up to 31 of the most recent system events that have occurred since the TAOS unit was powered up, and another displays statistics about the currently active session. An 80-column by 24-row VT100 window is required for use of the status screens.

This section describes the default configuration of the Status windows. For information about customizing the status window display for User logins, see “Customizing the environment for a User profile” on page 5-6.

Status window command summary

By default, the status window is not displayed upon login, but only when you explicitly request it with one of the following commands:

- Status—Opens or closes the status window.
- Connection—Opens the status window with the connection information displayed.
- Line—Opens the status window with the line information display.
- Log—Opens the status window with the log information display.
- View—Changes the information displayed in the top or bottom status window.

For details on using these commands, see the *APX 8000/MAX TNT Reference*.

Opening and closing the status window

To open the system status window, enter the Status command:

```
admin> status
```

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

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

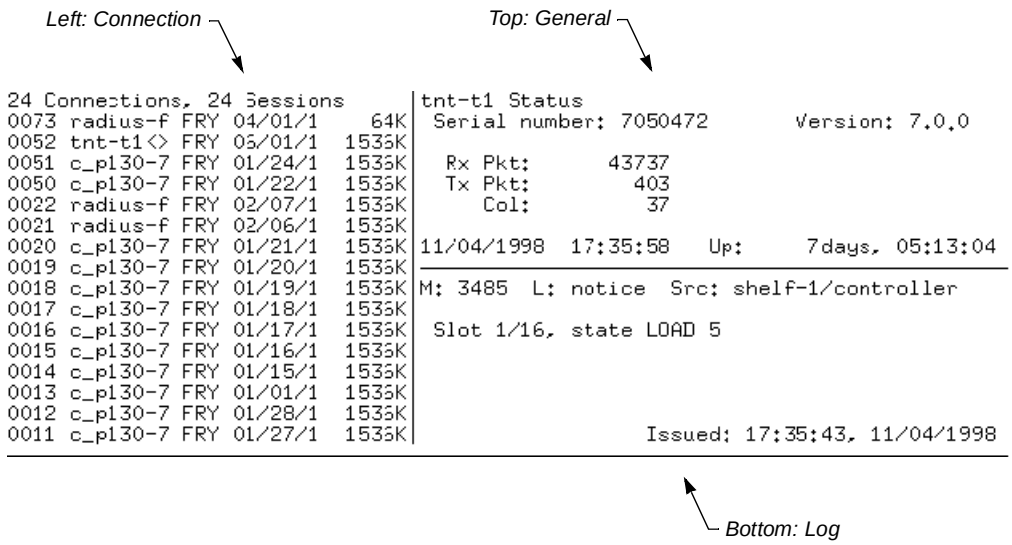
```
admin> status
```

Understanding the status window

The status window (Figure 2-1) has three main areas. In its default configuration, these areas contain the following information:

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

Figure 2-1. System status window



Connection status information

With the default setting in a User profile, the left area of the status window initially displays connection information, as shown in Figure 2-1. One line appears for each active connection, showing the user or station name, type of connection, T1 shelf, line, and channel on which the call was placed or received, and the bandwidth or baud rate of the connection.

If the status window is not already displayed, or if you want to scroll through the list of connections, use the Connection command as in the following example:

```
admin> connection
```

If the Status window is not displayed, the Connection command opens it and displays the connection-status-mode message below the Status window (if the Status window is already open, the Connection command just displays the message):

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

This message indicates the key sequences you can use for displaying additional information in the Connection status area. The Down Arrow and Up Arrow keys display the next and previous connection, respectively, in the list of active connections.

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

General status information

With the default setting in a User profile, the top area of the status window initially displays general status information about the TAOS unit, including its serial number, the version of system software it is running, and the number of packets transmitted and received. This area also shows the current system date and time and how long the system has been up.

If the top of the status window is displaying another kind of information, such as T1 line information, you can redisplay the general status information with the View command:

```
admin> view top general
```

Log messages

With the default setting in a User profile, the bottom area of the status window initially displays the most recent message from the TAOS unit's log buffer. The number of system event messages stored in the log is set by the Save-Number parameter in the Log profile.

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

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

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

```
super> log
```

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

```
[Back: <up arw>, Forward: <dn arw>, Start: <pg up>, End: <pg dn>, Exit:
<esc>]
```

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

- The Down Arrow and Up Arrow keys display the next and previous message in the buffer, respectively.
- The Page Up and Page Down. keys display the first and last message in the buffer, respectively.

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

Displaying WAN line information

The status window can also display information about the WAN lines on the TAOS unit. For details, see “Displaying line status” on page 1-7.

Changing current status window sizes

The Screen command enables you to change the size of the terminal emulator and status windows for the current session. (For information about changing the terminal emulator and status windows for a User profile, see “Customizing the environment for a User profile” on page 5-6.)

The following command changes window display sizes for the current session only:

```
admin> screen screen-length [status-length]
```

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

The *screen-length* option specifies the number of lines displayed in the terminal window. Note that *screen-length* must be at least 6 lines greater than the value of *status-length*.

The optional *status-length* option specifies the number of lines displayed in the status window, including dividing lines. The following example changes the terminal window to 55 lines high and the status windows to 22 lines high.

```
admin> screen 55 22
```

If you only specify the *screen-length* option, and it is not greater than the configured *status-length* by at least 6 lines, the TAOS unit automatically adjusts the length of the status windows. This is shown 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
```

Reviewing the fatal error log

The TAOS unit’s fatal error log contains messages related to the its operations.

To view the log of fatal errors, enter the Fatal-History. For example:

```
admin> fatal-history
OPERATOR RESET:  Index:  99  Revision: 2.0     Shelf 1 (apxsr)
        Date: 01/30/2000.       Time: 16:55:38
        Reset from unknown, user profile admin.
  SYSTEM IS UP:  Index: 100  Revision: 2.0     Shelf 1 (apxsr)
        Date: 01/30/2000.       Time: 16:56:12
```

The command's output information includes the date and time at which the error occurred, the system software version that was running at that time, the slot number on which the error occurred, and a stack trace record of the event. (For a list of fatal error messages, see Appendix B, "Log Messages on the TAOS Unit.")

To clear the fatal error log, enter the Clr-History command:

```
admin> clr-history
```

Configuring message logging

The TAOS unit generates error and event messages related to its operations. You can display these messages with the following commands:

- Log—Invoke or control the event log window.
- Fatal-History—List fatal error history log.

In the Log and User profiles you can configure the way in which the messages are handled .

The Log profile defines system-wide event logging parameters, including the number and level of messages to save and whether to communicate with a Syslog daemon.

Table 2-3 lists the sections describing common tasks you might have to perform to configure message logging on the TAOS unit. The table includes a brief description of each task, and lists the parameters you will use.

(For complete information about the associated parameters, see the *APX 8000/MAX TNT Reference*.)

Table 2-3. Overview of configuring logging on a TAOS unit

Task	Description of task	Related parameters
Configuring system logging on a TAOS unit	You can configure the level and number of messages that are logged to the TAOS unit's log. These messages are displayed in the log status window.	Save-Number Save-Level
Configuring Syslog on the TAOS unit	Syslog is an IP protocol that allows you to track events on the TAOS unit. A host running a Syslog daemon is typically a UNIX host, but it may also be a Windows system.	Sylsog-Enabled Call-Info Host Port Facility

Configuring system logging on a TAOS unit

The TAOS unit records system events in its status window event log. You can use the Save-Level and Save-Number parameters in the Log profile to configure the level and number of messages logged.

The Save-Level parameter specifies the lowest level of message to be saved for status display. The lowest possible level is None (this is the default). The highest level is Debug. For a list of the log message levels, see the *APX 8000/MAX TNT Reference*.

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

To configure the system log on the TAOS unit, proceed as in the following example:

1 Read in the Log profile:

```
admin> read log
LOG read
```

2 Specify the type of message you want logged:

```
admin> set save-level = emergency
```

3 Specify the number of messages to save in the event log:

```
admin> set save-number=200
```

4 Write the profile to save the changes:

```
admin> write
LOG written
```

Specifying a session ID base

The SessionID-Base parameter specifies the base number to use for generating a unique ID for each session. If SessionID-Base is zero, the TAOS unit sets the initial base for session IDs to the absolute clock. For details, see the *APX 8000/MAX TNT Reference*.

Configuring Syslog on the TAOS unit

To maintain a permanent log of a TAOS unit's system events and send Call Detail Reporting (CDR) reports to a host that can record and process them, configure the TAOS unit to report events to a Syslog host on the local IP network.

The host running a Syslog daemon is typically a UNIX host, but it may also be a Windows system. If the log host is not on the same subnet as the TAOS unit, it must have a route to that host, either via RIP or a static route. (For information about Syslog messages, see "Syslog messages" on page B-6.)

Note: Do not configure the TAOS unit to send reports to a Syslog host that can only be reached by a dial-up connection. That would cause the TAOS unit to dial the log host for every logged action, including hang ups.

To configure Syslog, you might need to set some or all of the following parameters:

Parameter	Description
Sylsog-Enabled	Enables Syslog.
Call-Info	Specifies whether the TAOS unit sends a one-line Syslog message to the Syslog host when an authenticated call terminates. This message includes information such as the called and calling number and the encapsulation, data rate, and length of session.
Host	The IP address of the Syslog host.
Port	Specifies the port number on which the remote Syslog daemon is listening. It is set to port 514 by default.
Facility	Identifies the messages as being from a particular TAOS unit.
Syslog-Format	Specifies whether the messages the TAOS unit sends to Syslog are in TAOS format (the default) or in another format as other Lucent products.

To configure Syslog reporting on the TAOS unit, proceed as in the following example:

1 Read in the Log profile:

```
admin> read log
LOG read
```

2 Enable Syslog:

```
admin> set syslog-enabled = yes
```

3 Specify that you want end of call information sent:

```
admin> set call-info=end-of-call
```

4 Specify the IP address of the host running Syslog:

```
admin> set host=10.2.3.4
```

5 Specify the port the Syslog daemon is listening on:

```
admin> set port=588
```

The TAOS unit will send all messages out on this port as soon as you write the Log profile.

6 Specify the Syslog facility:

```
admin> set facility=local0
```

After setting a log facility number, you need to configure the Syslog daemon to write all messages containing that facility number to a particular log file. This file will be the TAOS unit log file.

7 Specify the format of Syslog messages:

```
admin> set syslog-format = max
```

8 Write the profile to save the changes:

```
admin> write
LOG written
```

Note that Call-Info is intended for diagnostic support. It uses UDP, which provides no guaranteed delivery, so it should not be used for billing purposes.

Configuring the Syslog daemon

To configure the Syslog daemon to interact with the TAOS unit, you need to modify the `/etc/syslog.conf` file on the log host. This file specifies which action the daemon will perform when it receives messages from a particular log facility number (which represents the TAOS unit). For example, if you set Log Facility to Local5 in the TAOS unit, and you want to log its messages in `/var/log/tnt01`, add the following line to `/etc/syslog.conf`:

```
local5.info<tab>/var/log/tnt01
```

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

Checking the power supplies

To check the status of the APX 8000 unit's redundant power supplies, enter the Power command. For example:

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

You can also use the Lucent Power Supply MIB to manage and monitor the power supplies.

Using a script to configure the TAOS unit

The TAOS unit's CLI allows you to create configuration scripts with a simple text editor and a Telnet client program with a Text Upload feature. This section briefly describes how you could use a script to make changes to the TAOS unit's configuration.

Following are the basic steps:

1. Create a text file that contains the configuration commands as you would enter them in the TAOS unit's CLI.
2. Log into the TAOS unit with sufficient permissions to change the configuration.
3. To upload the file to the TAOS unit, use the upload file feature of your Telnet or terminal software.

Creating a text file

Following is an example of a text file that configures a T1 line in shelf 1, slot 1.

```
new T1
set name = SF
set physical-address shelf = shelf-1
set physical-address slot = slot-1
set physical-address item-number = 1
set line-interface enabled = yes
set line-interface frame-type = esf
set line-interface encoding = b8zs
set line-interface clock-source = eligible
write -f
;
```

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

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

Logging into the TAOS unit

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

```
% telnet mytnt
User: admin
Password: mypassword
admin>
```

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

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

Uploading the text file

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

Displaying user session information

You can obtain TAOS system user session information with the Userstat and Finger commands.

Using the Userstat command

The Userstat command displays the active users on the TAOS unit. To display the most complete information about active sessions, use the `-l` option, as in the following example:

```
admin> userstat -l
SessionID  Line/Chan  Slot:Item  Tx/Rx Rate  Svc Address      Username
228687860  1.01.02/01 1:03:01/01 56K/56K     PPP 10.100.0.1   barney
228687861  1.02.03/02 1:04:02/00 28800/33600 PPP 10.168.6.24  jake
<end user list> 2 active user(s)
```

Following are the Userstat output fields with descriptions:

Field	Description
`SessionID`	Unique ID assigned to the session.
`Line/Chan`	Physical address (shelf.slot.line/channel) of the network port on which the connection was established, (for example, a T1 line/channel).
`Slot:Item`	*Shelf:slot:item/logical-item* of the host port to which the call was routed (for example, modem, HDLC channel).
`Tx/Rx Rate`	Transmit and receive rate. Note that for modem connections, the transmit rate is set automatically to the receive rate, because modem cards do not support asymmetric data rate connections.

Field	Description
`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) X25 (X.25) FRY (Frame Relay) EUR (EU-RAW) EUI (EU-UI) TLN (Telnet) BTN (Binary Telnet) TCP (raw TCP) TRM (Terminal Server) VCN (Virtual Connect) D25 (D-channel X.25) DTP (DTPT)
`Dialed#` (displays only with `-l` option)	The number dialed to initiate this session.
`ConnTime` (displays only with `-l` option)	The amount of time (in hours:minutes:seconds format) since the session was established.
`IdleTime` (displays only with `-l` option)	The amount of time (in hours:minutes:seconds format) since data was last transmitted across the connection.

To terminate a user, use the `-k` option, as in the following 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
```

The Userstat command can terminate PPP, SLIP, MP+, Telnet, Telnet binary, Raw TCP, or terminal server user sessions. You cannot use the `-k` option to terminate Frame Relay or DTPT service types.

You can configure the Userstat command output with the Userstat-Format parameter. For information, see the *APX 8000/MAX TNT Reference*.

Userstat options to display address and username

The Userstat command supports the following new options:

- `-a`, to take the IP address of a session as input and display the associated session details.
- `-u`, to take a username and display the associated session details.
- `-o`, to restrict the Userstat command output to specified fields.

Following is the new command usage statement:

```
admin> help userstat
userstat usage: userstat -options [ params ] [ -o [format] ]
    command options:
       -s  show users (default)
       -k  <sessionID> kill a user session
       -a  <ipAddress> show the session with matching <ipAddress>
       -u  <username>  show the session with matching <username>
       -l  wide format (> 80 characters)
       -d  dump, do not pass output through more
    format values:
    One or More of the following format characters
       %i  SessionID
       %l  Line/Chan
       %s  Slot:Item
       %r  Tx/Rx Rate
       %d  Type of Service
       %a  Address
       %u  Username
       %c  ConnTime
       %t  IdleTime
       %n  Dialed#
       default : %i %l %s %r %d %a %u %c %t %n
```

Using the -o format specifier option

Use the `-o` option with one or more format specifiers to display only the fields of interest. For example, for an active session, the Userstat command shows the following details:

```
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)
```

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

```
admin> userstat -o %i %l

SessionID  Line/Chan
288532030  1.01.01/012
<end user list>  1 active user(s)
```

Using the -a and -u options

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

```
admin> userstat -a 1.1.1.238

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

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

```
admin> userstat -a 1.1.1.238 -o %u
```

```
Username
net1
<end user list>  1 active user(s)
```

Use the `-u` option to display information related to a known username. It requires a user-name argument on the command line. For example:

```
admin> userstat -u net1

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

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

```
admin> userstat -u net1 -o %a

Address
1.1.1.238
<end user list>  1 active user(s)
```

Using the Finger command

Finger is described in RFC 1288. To enable it in the TAOS unit, set the Finger parameter to Yes, as follows:

1. Read the IP-Global profile:

   ```
   admin> read ip-global
   ```

2. Set Finger to Yes:

   ```
   admin> set finger = yes
   ```

3. Write the profile:

   ```
   admin> write
   ```

The default value for this parameter is No, which causes the TAOS unit to reject queries from Finger clients with the following message:

```
Finger online user list denied.
```

Setting the Finger parameter to 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 a short or wide format. For example, a UNIX client can request the wide (140-character) format by using the `-l` option, as in the following command which displays, in wide format, session information for the system named `apx1`:

```
# finger -l @apx1
```

The following command displays the same information in narrow (80-character) format:

```
# finger @apx1
```

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 Tupshin:

```
# finger tupshin@apx1
```

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.
```

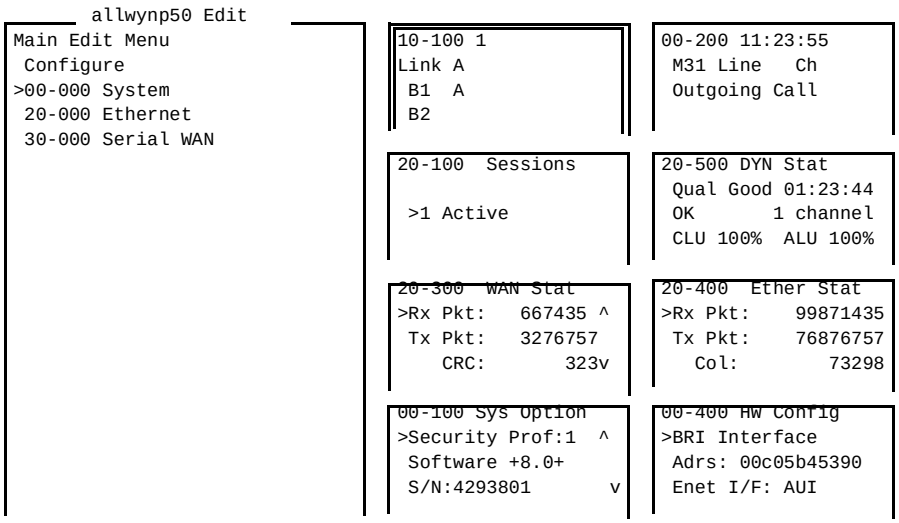
Remote management of other units

The Remote command is available in the terminal-server interface on host cards that accept digital calls, and as a command on the TAOS shelf controller. As on other TAOS platforms, the Remote command is used to remotely manage another unit.

Opening a remote management session

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. The following example shows a remote device that uses the VT100 interface for TAOS. For example:

```
admin> remote allwynp50
```




```
Press Ctrl-n to move cursor to the next menu item. Press return to select it.
Press Tab to move to another window--thick border indicates active window.
```

The Remote command argument is the station name, which must match the value of a Station parameter in a Connection profile, or the user ID at the start of a RADIUS profile. The connection must use the MP+ protocol, and the connection must already be established when you use the Remote command.

When you use the Remote command on the shelf controller, it locates the host card that has an active connection to the remote unit. It then opens a session to that card, invokes the terminal-server interface, 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, which can be used to reconfigure the unit. However, 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.

You can also manually open a session with the host card that has an active connection to the remote unit, invoke the terminal-server, and run the Remote command on the slot card. For example:

```
admin> userstat -s
SessionID  Line/Chan  Slot:Item  Tx/Rx Rate  Svc Address     Username
228687860  1.01.02/01 1:03:01/01 56K/56K     PPP 10.100.0.1  clarap75
228687861  1.02.03/02 1:04:02/00 28800/33600 MPP 10.168.6.24 allwynp50

<end user list>  2 active user(s)

admin> open 1 4

hdlc2-1/4> terminal-server

ascend% remote allwynp50
```

Terminating a remote management session

To exit from the remote management session and return to the command-line interface session on the shelf controller, press Ctrl-C three times in quick succession.

If you opened the session on a slot card, press Ctrl-\ to end the session. You can then quit the terminal server and the slot card session to return to the shelf controller.

Either end of the connection can terminate an MP+ connection by hanging up all channels of the connection.

Note: A remote management session can time out, because the traffic it generates does not reset the idle timer. Therefore, the Idle parameter in the Connection profile at both the calling and answering ends of the connection must be disabled during a remote management session, and restored just before exiting. Remote management works best at higher terminal speeds.

Error messages

The TAOS generates an error message for any condition that causes the session to terminate before sending the full number of packets. The following error messages can appear:

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 specified 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.

Message	Explanation
`<station> did not negotiate MPP`	The remote station did not negotiate an MP+ connection. Possibly the profile for the TAOS dial-in did not specify MP+.
`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. (The Remote Mgmt parameter was set to `no` in the remote station's System profile.)

Reloading profiles from RADIUS

Use the Refresh command to open a connection to a RADIUS server and retrieve the latest configuration information. (For information about RADIUS, see the *APX 8000/MAX TNT Reference*.)

The Refresh command uses the following syntax:

`refresh -a|-n|-p|-r|-t`

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

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

```
admin> refresh -n
```

You can specify how nailed connections are handled following a Refresh –n by using the Perm-Conn-Upd-Mode parameter in the System profile. If set to All (the default), all existing permanent connections are brought down and then brought up again (along with any new connections) following the update. This causes service interruption every time any nailed profile is updated or added.

If set to Changed, only new connections are created, and only those with modified attribute values are reestablished.

Configuring the dialout timer

The Max-Dialout-Time parameter in the System profile specifies the maximum number of seconds the system waits for a Call Setup Complete from the remote side when dialing out. If the TAOS unit cannot establish the call before the timer expires, the dialout attempt fails. The dialout timer allows increased flexibility for international dialing.

Valid values are from 0 to 255. The default is 20 seconds. If set to zero, the TAOS unit uses its internal default of 20 seconds. In the following example, the dialout timer is set to 60 seconds:

```
admin> read system
SYSTEM read

admin> set max-dialout-time = 60

admin> write
SYSTEM written
```

The Max-Dialout-Time setting does not influence the modem timeout to detect carrier. Modems have an internal timer that counts down from dialout to establishing carrier with the remote modem (including training) which for Rockwell modems has a default of 45 seconds.

Network Administration

3

The TAOS unit supports several network management commands, which are useful for locating the sources of problems on the network and for communicating with other hosts for management purposes.

Some of the network management tools focus on routing and interface information. They enable you to display the routing and interface tables, view real-time routing statistics, display route caches, and make changes to the routing table. The OSPF command supports numerous arguments for viewing information about the OSPF link-state database, adjacencies, and other aspects of the router configuration.

Other tools are geared toward network usage, and enable you to display packets received on LAN interfaces, display the ARP cache, Ping a host, and log into a host by means of Rlogin or Telnet.

For complete information about the commands described in this chapter, see the *APX 8000/MAX TNT Reference*.

Diagnostic tools for TCP/IP networks

The TAOS unit maintains an internal IP routing table. You can configure the system to use RIP or OSPF to propagate the information in that table to other routers, receive information from other routers, or both, on any LAN or WAN interface. For information about configuring the router, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.

Testing connectivity

The Ping command is useful for verifying that the transmission path between the TAOS unit and another station is open. Ping sends an ICMP echo_request packet to the specified station. It

the station receives the packet, it returns an ICMP echo_response packet. For example, to Ping the host `techpubs`:

```
admin> ping techpubs

PING techpubs (10.65.212.19): 56 data bytes
64 bytes from 10.65.212.19: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.65.212.19: icmp_seq=3 ttl=255 time=0 ms
^C
--- techpubs ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

You can terminate the Ping exchange at any time by pressing Ctrl-C. When you press Ctrl-C, the command reports the number of packets sent and received, the percentage of packet loss, the number of duplicate or damaged echo_response packets (if any), and round-trip statistics. In some cases, round-trip times cannot be calculated.

During the Ping exchange, the TAOS unit displays information about the packet exchange, including the Time-To-Live (TTL) of each ICMP echo_response packet.

The maximum TTL for ICMP Ping is 255, while and the maximum TTL for TCP is often 60 or lower, so you might be able to Ping a host but not be able to run a TCP application (such as Telnet or FTP) to that station. If you Ping a host running a version of Berkeley UNIX before 4.3BSD-Tahoe, the TTL report is 255 minus the number of routers in the round-trip path. If you Ping a host running the current version of Berkeley UNIX, the TTL report is 255 minus the number of routers in the path from the remote system to the station performing the Ping.

Displaying the interface table

At system startup, the TAOS unit creates an IP interface, in the active state, for each Ethernet interface that has a configured IP-Interface profile, and for the built-in loopback, reject, and blackhole interfaces. It also creates IP interfaces in the inactive state for remote connections. For each IP interface that is not configured as a private route, the TAOS unit also adds a route to the routing table.

```
admin>netstat -i
Name    MTU   Net/Dest        Address        Ipkts  Ierr  Opkts   Oerr
ie0     1500  192.168.7.0/24  192.168.7.135  71186  2     53131   96
lo0     1500  127.0.0.1/32    127.0.0.1      53195  0     53195   0
rj0     1500  127.0.0.2/32    127.0.0.2          0  0         0   0
bh0     1500  127.0.0.3/32    127.0.0.3          0  0         0   0
wanabe  1500  127.0.0.3/32    127.0.0.3          0  0         0   0
local   65535 127.0.0.1/32    127.0.0.1      59753  0     59753   0
mcast   65535 224.0.0.0/4      224.0.0.0          0  0         0   0
tunnel7 1500  192.168.7.0/24  192.168.7.135      0  0         0   0
```

```
Name    MTU   Net/Dest         Address         Ipkts  Ierr  Opkts   Oerr
vr0main 1500  192.168.7.135/32 192.168.7.135   0       0     0      0
sip0    65535 -                -               0       0     0      0
wan10   1528  200.4.2.2        192.168.7.135   0       0     0      0
wan11   1528  200.5.2.2        192.168.7.135   0       0     0      0
wan12   1528  200.6.1.2        192.168.7.135   0       0     0      0
wan13   1528  200.6.2.2        192.168.7.135   0       0     0      0
wan14   1528  200.100.2.2      192.168.7.135   0       0     0      0
wan15   1528  200.100.3.2      192.168.7.135   0       0     0      0
wan16   1528  200.4.4.2        192.168.7.135   0       0     0      0
wan17   1500  200.6.100.2      200.1.100.2     0       0     0      0
wan18   1528  200.4.4.3        192.168.7.135   0       0     0      0
wan19   1528  200.4.2.3        192.168.7.135   0       0     0      0
wan20   1528  200.3.2.2        192.168.7.135   0       0     0      0
wan21   1528  200.3.1.2        192.168.7.135   0       0     0      0
wan22   1528  200.4.103.2      192.168.7.135   0       0     0      0
wan23   1500  200.4.101.3      200.2.101.2     0       0     0      0
..
..
..
ie1-5-1 1500  200.1.1.0/24     200.1.1.2       0       0     1      0
ie1-5-2 1500  200.1.2.0/24     200.1.2.2       0       0     1      0
ie1-5-3 1500  200.2.1.0/24     200.2.1.2   75837       0 75838      0
ie1-5-4 1500  200.2.2.0/24     200.2.2.2       0       0     1      0
ie1-5-5 1500  -                -               0       0     0      0
```

The interface table contains the following information:

Column name	Description
`Name`	Name of the interface: • `ie0-`*`n`* —The shelf-controller Ethernet interfaces. • `ie[shelf]-[slot]-[item]`—The Ethernet interfaces for Ethernet cards. • `lo0`—The loopback interface. • `rj0`—The reject interface, used in network summarization. • `bh0`—The blackhole interface, used in network summarization. • `wanN` —A WAN connection, entered as it becomes active. • `wanabe`—An inactive RADIUS dialout profile. • `local`—The local machine. • `mcast`—The multicast interface, which represents the multicast forwarder for the entire class-D address space. • `tunnel`*`N`*—A pseudo-interface that is used only when the TAOS unit is configured as an ATMP Router Home Agent. In that configuration, the TAOS unit creates a route for each registered Mobile Client. Regardless of how many tunnels the Home Agent may terminate, there is always a single tunnel interface. (The number appended to the tunnel interface name is an internal number used by the system.)
`MTU`	(Maximum Transmission Unit) The maximum packet size allowed on the interface.
`Net/Dest`	Network or the target host this interface can reach.
`Address`	Address of this interface.
`Ipkts`	Number of packets received.
`Ierr`	Number of packets that contain errors.
`Opkts`	Number of packets transmitted.
`Oerr`	Number of transmitted packets that contain errors.

Displaying and modifying IP routes

This section explains how to display the TAOS unit's IP routing table. It also explains how to use the Netstat command to display the IP routing table and the IProute command to add or delete static routes. For complete information about configuring IP routing on the TAOS unit, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.

Displaying the routing table

To display the routing table, enter the Netstat command with the `-r` argument, as in the following example:

```
admin> netstat -r
Destination      Gateway      IF     Flg    Pref   Met    Use    Age
127.0.0.0/8      -            bh0    CP     0      0      0      154417
127.0.0.1/32     -            local  CP     0      0      0      154417
127.0.0.2/32     -            rj0    CP     0      0      0      154417
182.21.33.0/24   192.168.7.1  ie0    SG     60     8      0      150873
192.168.7.0/24   -            ie0    C      0      0      50041  154417
192.168.7.135/32 -            local  CP     0      0      2522   154417
..
..
..
216.64.222.0/24   192.168.7.1 ie0    SG     60     8      1456   150873
224.0.0.0/4        -          mcast  CP     0      0      0      154417
224.0.0.1/32       -          local  CP     0      0      0      154417
224.0.0.2/32       -          local  CP     0      0      0      154417
224.0.0.5/32       -          local  CP     0      0      0      154417
224.0.0.6/32       -          local  CP     0      0      0      154417
224.0.0.9/32       -          local  CP     0      0      0      154417
255.255.255.255/32 -          ie0    CP     0      0      0      154417
```

The columns in the routing table contain the following information:

Column	Description
`Destination`	The route's target address. To send a packet to this address, the TAOS unit uses this route. If the target address appears more than once in the routing table, the TAOS unit uses the most specific route (having the largest subnet mask) that matches that address.
`Gateway`	The next hop router that can forward packets to the given destination. Direct routes (without a gateway) show a hyphen in this column.

Column	Description
IF	The name of the interface through which to send packets over this route: • ie0 or ie[shelf]-[slot]-[item] is an Ethernet interface. • 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 dialout profile. • local indicates a single route targeted at the local machine. • mcast indicates a route to a virtual device. The route encapsulates the multicast forwarder for the entire class D address space.
Flg	One or more of the following flags: • C—a directly connected route, such as Ethernet • I—an ICMP redirect dynamic route • N—placed in the table via SNMP MIB II • O—A route learned from OSPF • R—a route learned from RIP • r—a transient RADIUS-like route • S —a static route • ?—a route of unknown origin, which indicates an error • G—an indirect route via a gateway • P—a private route • T—a temporary route • M—a multipath route • *—a backup static route for a transient RADIUS-like route
Pref	The preference value. See the description of the Preference parameter for information about defaults for route preferences.
Metric	A RIP-style metric for the route, with a range of 0-16. Routes learned from OSPF show a RIP metric of 10. OSPF cost-infinity routes show a RIP metric of 16.
Use	A count of the number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent over this route.)
Age	The age of the route in seconds. RIP and ICMP entries are aged once every 10 seconds.

Modifying the routing table

The IProute command enables you to manually add routes to the routing table, delete them, or change their preference or metric values. The command is useful for temporary routing changes. Changes you make to the routing table with the IProute command do not persist

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

The IProute command uses the following syntax:

iproute option

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

Adding a static IP route to the routing table

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

iproute add *dest_IPaddr* [**/*subnet_mask***] ***gateway_IPaddr*** [**/*subnet_mask***] [**pref**] [**metric**]

Syntax element	Description
dest_IPaddr [**/subnet_mask**]	Destination network address. The optional subnet mask specifies the number of bits in the mask. The default is 0.0.0.0/0. Note that the router uses the most specific route (having the largest mask) that matches a given destination.
gateway_IPaddr [**/subnet_mask**]	IP address of the router that can forward packets to the destination network, and optional subnet mask (in bits). The default is 0.0.0.0.
pref	Route preference. The default is 100.
metric	Virtual hop count of the route. You can enter a value between 1 and 15. The default is 1. Note that RIP and OSPF updates can change the metric for any route, including one you have modified manually by using the IProute command.

For example, consider the following command:

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

It adds a route to the 10.1.2.0 network and all of its subnets, through the IP router located at 10.0.0.3/24. The metric to the route is 1 (one hop away).

If you try to add a route to a destination that is already in the routing table, the TAOS unit does not replace the existing route unless it has a higher metric than the route you attempt to add. If you get the message `Warning: a better route appears to exist`, the TAOS unit has rejected your attempt to add a route.

Deleting a static IP route from the routing table

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

`iproute delete`
`dest_IPaddr``[/`***`subnet_mask`***`][`***`gateway_IPaddr`***`[/`***`subnet_mask`***`]]`

The arguments are the same as for IP Route Add. For example, the following command removes the route to the 10.1.2.0 network:

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

You can also change the metric or preference value of an existing route by using the IProute command. For example, if the routing table contains the following route:

```
Destination        Gateway        IF       Flg   Pref Met     Use       Age
10.122.99.0/24     10.122.99.1    wan4     SG     100   7       0     48630
```

You could change the metric as follows:

```
admin> iproute add 10.122.99.0/24 10.122.99.1 50 3
```

Tracing routes

The TraceRoute command is useful for locating slow routers or diagnosing IP routing problems. It 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. For example, to trace the route to the host `techpubs`:

```
admin> traceroute techpubs

traceroute to techpubs (10.65.212.19), 30 hops max, 0 byte packets
1  techpubs.eng.ascend.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Probes start with a TTL of one and increase by one until of the following conditions occur:

- The TAOS unit receives an ICMP `port unreachable` message. (The UDP port in the probe packets is set to an unlikely value, such as 33434, because the target host is not intended to process the packets. A `port unreachable` message indicates that the packets reached the target host and were rejected.)
- The TTL value reaches the maximum value. (By default, the maximum TTL is set to 30.) You can use the `-m` option to specify a different TTL. For example:

```
admin> traceroute -m 60 techpubs

traceroute to techpubs (10.65.212.19), 60 hops max, 0 byte packets
1  techpubs.eng.abc.com (10.65.212.19)  0 ms  0 ms  0 ms
```

TraceRoute sends three probes at each TTL setting. The second line of output shows the address of the router and the round trip time of each probe. If the probe answers come from different gateways, the address of each responding system is shown. If there is no response within a three-second timeout interval, the second line of output lists an asterisk.

For the details of the TraceRoute command, see the *APX 8000/MAX TNT Reference*.

Verifying name service setup

You can retrieve a host address by using the NSlookup command, provided that the TAOS unit has been configured with the address of a name server. (For information about configuring name servers, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*). If a host has several IP interfaces, the command returns several addresses.

To retrieve the IP address of the host `techpubs`, proceed as in the following example:

```
admin> nslookup techpubs

Resolving host techpubs.
IP address for host techpubs is 10.65.212.19.
```

Displaying the ARP cache

The Address Resolution Protocol (ARP) translates between IP addresses and media access control (MAC) addresses as defined in RFC 826. Hosts broadcast an ARP request that is received by all hosts on the local network, and the one host that recognizes its own IP address sends an ARP response with its MAC address.

The TAOS unit maintains a cache of known IP addresses and host MAC, addresses which enables it to act as a proxy for ARP requests for target hosts across the WAN, provided that proxy mode is turned on. (For configuring proxy ARP, see *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.)

With the ARPtable command, you can display the ARP table, add or delete ARP table entries, or clear the ARP cache entirely. To display the ARP cache, enter the ARPtable command without any arguments, as in the following example:

```
admin> arptable
IP Address       MAC Address        Type  IF   Retries/Pkts/RefCnt  Time Stamp

10.103.0.141    00:B0:24:BE:D4:84   DYN   0        0/0/1            23323
10.103.0.2      00:C0:7B:7A:AC:54   DYN   0        0/0/599          23351
10.103.0.220    00:C0:7B:71:83:02   DYN   0        0/0/2843         23301
10.103.0.1      08:00:30:7B:24:27   DYN   0        0/0/4406         23352
10.103.0.8      00:00:0C:06:B3:A2   DYN   0        0/0/6640         23599
10.103.0.7      00:00:0C:56:57:4C   DYN   0        0/0/6690         23676
10.103.0.49     00:B0:80:89:19:95   DYN   0        0/0/398          23674
```

The ARP table displays the following information:

Column	Description
`IP Address`	The address contained in ARP requests.
`MAC Address`	The MAC address of the host.
`Type`	How the address was learned, that is, dynamically (DYN) or by specification of a static route (STAT).
`IF`	The interface on which the TAOS unit received the ARP request.

Column	Description
`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.

To add an ARP table entry, use the `-a` option, as in the following example:

```
admin> arptable -a 10.65.212.3 00:00:81:3D:F0:48
```

To delete an ARP table entry, use the `-d` option, as in the following example:

```
admin> arptable -a 10.9.8.20
```

To clear the entire ARP table, use the `-f` option:

```
admin> arptable -f
```

Displaying protocol statistics

The Netstat command displays the TAOS unit's IP interface and routing tables, protocol statistics, and active sockets. By default (without an argument), the Netstat command reports information about both UDP and TCP. Following is an example that shows the use of Netstat without any arguments to display UDP and TCP socket information:

```
admin> netstat
udp:
-Socket-  Local Port  InQLen  InQMax    InQDrops    Total Rx
1/c    0        1023       0       1           0           0
1/c    1         520       0       0           0       15510
1/c    2           7       0      32           0           0
1/c    3         123       0      32           0           0
1/c    4        5150       0     256           0           0
1/c    5        1022       0     128           0           0
1/c    6         161       0      32           0           0
1/c    7        1797       0     128           0          22
1/8    0        1018       0     128           0           0
1/8    1       20108       0      32           0           0
1/8    2        1008       0     128           0           0
1/8    3        1798       0     128           0           0
1/9    0        1021       0     128           0           0
1/9    1       20109       0      32           0           0
1/9    2        1009       0     128           0           0
1/9    3        1799       0     128           0           0
1/10   0        1020       0     128           0           0
1/10   1       20110       0      32           0           0
1/10   2        1010       0     128           0           0
1/10   3        1800       0     128           0           0
1/11   0        1017       0     128           0           0
1/11   1       20111       0      32           0           0
1/11   2        1011       0     128           0           0
1/11   3        1801       0     128           0           0
1/12   0        1019       0     128           0           0
```

```
1/12   1       20112       0      32           0           0
1/12   2        1012       0     128           0           0
1/12   3        1802       0     128           0           0

tcp:
-Socket- Local                     Remote                    State
1/c    0 192.168.7.135.79          *.*                       LISTEN
1/c    1 192.168.7.135.1723        *.*                       LISTEN
1/c    2 192.168.7.135.23          *.*                       LISTEN
1/c    4 192.168.7.135.23          172.20.32.137.42863       ESTABLISHED
1/c    9 192.168.7.135.23          206.65.212.10.1991        ESTABLISHED
```

The output shows the queue depth of various UDP ports, as well as the total packets received and total packets dropped on each port. The total-packets-received count includes the total packets dropped. For this sample output, the SNMP queue depth was set to 32. For information about queue depths, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.

The Netstat command supports the `-s` option, which displays protocol statistics. The `-s` option uses the following syntax:

`netstat -s identifiers`

If no identifiers follow the `-s` option, all protocol statistics are shown. If specified, the identifiers determine the type of protocol statistics to display. Valid identifiers include `udp`, `tcp`, `icmp`, `ip`, `igmp`, or `mcast`. Following is an example that displays all statistics:

```
admin>netstat -s

udp:
        15636 packets received
        0 packets received with no ports
        0 packets received with errors
        0 packets dropped
        68 packets transmitted

tcp:

        0 active opens
        7 passive opens
        0 connect attempts failed
        0 connections were reset
        2 connections currently established
        1457 segments received
        0 segments received out of order
        1728 segments transmitted
        18 segments retransmitted
        5 active closes
        0 passive closes
        0 disconnects while awaiting retransmission

icmp:

        216 packets received
        0 packets received with errors
        Input histogram:
                216 echo requests
```

```
        271 packets transmitted
        0 packets not transmitted due to lack of resources
        Output histogram:
                216 echo replies
                24 destination unreachable
                31 time exceeded


ip:

        28860 packets received
        0 packets received with header errors
        0 packets received with address errors
        0 packets received forwarded
        0 packets received with unknown protocols
        0 inbound packets discarded
        17310 packets delivered to upper layers
        2084 transmit requests
        0 discarded transmit packets
        49 outbound packets with no route
        0 reassemblies timeout
        268 reassemblies required
        12 reassemblies succeeded
        244 reassemblies failed
        12 fragmentation succeeded
        0 fragmentation failed
        24 fragmented packets created
        0 route discards due to lack of memory
        64 default ttl

igmp:

        0 packets received
        0 bad checksum packets received
        0 bad version packets received
        0 query packets received
        0 leave packets received
        0 packets transmitted
        0 query packets sent
        0 response packets sent
        0 leave packets sent

mcast:

        0 packets received
        0 packets forwarded
        0 packets in error
        0 packets dropped
        0 packets transmitted
```

Logging into a network host

The Rlogin and Telnet commands enable you to log into a network host from the TAOS unit.

Using the Rlogin command

The Rlogin command initiates a login session from a host card, such as a modem or HDLC card, to a remote host. For example, to log into the host `techpubs`, first open a session with the host card. Then issue the Rlogin command:

```
hdlc-1/16> rlogin techpubs

Password:
Last login: Wed Oct  2 10:31:36 from marcel.marceau
SunOS Release 4.1.4 (TECHPUBS-BQE) #1: Wed Jan 4 08:56:59
PDT 2000
techpubs%
```

You can log out of the remote host by entering the Rlogin escape sequence (tilde-dot):

```
techpubs% ~.
Connection closed.
```

Or, you can log out explicitly:

```
techpubs% logout
Connection closed.
```

If you wish, you can change the default escape character from a tilde to any other character. For details, see the *APX 8000/MAX TNT Reference*.

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

```
admin> rlogin -l marcel techpubs
Password:
```

Using the Telnet command

The Telnet command initiates a login session to a remote host. For example, to Telnet into the host `techpubs`:

```
admin> telnet techpubs

Connecting to techpubs (10.65.212.19) ...
Escape character is '^]'
Connected
SunOS UNIX (techpubs)
```

You can close the Telnet session by logging out of the remote host:

```
techpubs% logout
Connection closed.
```

Detecting and reporting patterns in the TCP-Clear data stream

You can run the Tokencount diagnostic command to detect and report the number of instances of a specified pattern (a *token*) in the TCP-Clear data stream sent by the TAOS. 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 resets, it loses the token information.

Tokencount command syntax

On the shelf controller, the Tokencount command supports the following syntax:

```
usage: tokencount -option [ params ]
    -a           clear counter for (a)ll tokens
    -c n         (c)lear counter for nth token
    -d           (d)isable token counting in the TCP-CLEAR buffer
    -e           (e)nable token counting in the TCP-CLEAR buffer
    -i           display counter (i)nfo
    -u n pattern (u)pdate type nth token pattern
    -?           display this summary
```

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

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

Characters	Meaning	ASCII value
\f	Form feed	12
\n	Newline	10
\r	Return	13
\t	Tab	9
\v	Vertical tab	11
\\	Backslash	92
\"	Quotation mark	34
\’	Apostrophe	44

Examples of using Tokencount

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 modem card in shelf 5, slot 6 and display the token information gathered on that card:

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

Tokencount error messages

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

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

The number specified in the Tokencount -u command is out of the valid range from 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.

Diagnostic tools for IGMP multicast interfaces

The IGMP command displays information about IGMP groups and clients. This can be useful for tracking the IGMP group memberships and active client interfaces.

Displaying IGMP group information

To display active multicast group addresses and clients (interfaces) registered for each group, enter the IGMP command with the `group` option:

```
admin> igmp group
IGMP Group address Routing Table Up Time: 0:0:22:17
 Hash      Group Address    Members    Expire time   Counts
  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).
`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.
`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.
`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.
`Counts`	Number of packets forwarded to the client, number of packets dropped due to lack of resources, and the state of the membership. The state is displayed for debugging purposes.

Displaying IGMP client information

To display a list of multicast clients, enter the IGMP command with the `client` option:

```
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`	ID of the interface on which the client resides. The value 0 (zero) represents the Ethernet. Other numbers are WAN interfaces, numbered according to when they became active. `Mbone` is the interface on which the multicast router resides.
`Version`	Version of IGMP being used.
`RecvCount`	Number of IGMP messages received on the client's interface.
`CLU` `ALU`	Current Line Utilization and Average Line Utilization. Both indicate the percentage of bandwidth utilized across this interface. If bandwidth utilization is high, some IGMP packet types are not forwarded.

Diagnostic tools for OSPF routers

The OSPF diagnostic-level commands enable the administrator to display information related to OSPF routing, including the link state advertisements (LSAs), border routers' routing table, and the OSPF areas, interfaces, statistics, and routing table. To display the usage statement, enter the OSPF command with the `?` option:

```
admin> ospf

ospf ?                              OSPF help information
ospf size                           OSPF size
ospf areas                          OSPF areas
ospf stats                          OSPF statistics
ospf intf [ip-address]               OSPF summary/detail interface
information
ospf lsa area ls-type ls-id ls-orig  OSPF detail link-state
advertisement
ospf lsdb [area]                    OSPF link-state DB summary for an
ospf nbrs [neighbor-id]              OSPF summary/detail neighbor
information
ospf routers                        OSPF routers
ospf ext                            OSPF external AS advertisements
ospf rtab                           OSPF routing table
ospf database                       OSPF entire database summary
```

```
ospf internal                        OSPF internal routes
```

Displaying general information about OSPF routing

To display general information about OSPF, enter the OSPF command with the `stat` option. For example:

```
admin> ospf stats

OSPF version:   2


OSPF Router ID:          10.103.0.254
AS boundary capability:   Yes
Attached areas:           1       Estimated # ext. (5) routes: 65536
OSPF packets rcvd:        71788   OSPF packets rcvd w/errs:    19
Transit nodes allocated:  812     Transit nodes freed:         788
LS adv. allocated:        2870    LS adv. freed:               2827
Queue headers alloc:      64     Queue headers avail:         64
# Dijkstra runs:           10     Incremental summ. updates:   0
Incremental VL udates:     0      Buffer alloc failures:       0
Multicast pkts sent:       27343  Unicast pkts sent:           1154
LS adv. aged out:          0      LS adv. flushed:             507
Incremental ext.(5) updates: 1014  Incremental ext.(7) updates: 0


External (Type 5) LSA database -
Current state:                    Normal
Number of LSAs:                   43
Number of overflows:              0
```

The following table describes the output:

Field	Specifies
`OSPF version`	Version of the OSPF protocols running.
`OSPF Router ID`	IP address assigned to the TAOS unit, which is typically the address specified for the Ethernet interface.
`AS boundary capability`	Yes if the TAOS unit functions as an ASBR or No if it does not function as an ASBR.
`Attached areas`	Number of areas to which this TAOS unit attaches.
`Estimated # ext.(5) routes`	Number of ASE-5 routes that the TAOS unit can maintain before it goes into an overload state.
`OSPF packets rcvd`	Total number of OSPF packets received by the TAOS unit.

Field	Specifies
`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. 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 TAOS unit frees all queue headers from a specific memory block, the TAOS unit returns the block to the pool of available memory blocks.
`# Dijkstra runs`	Number of times that the TAOS unit has run the Dijkstra algorithm (short path computation).
`Incremental summ. updates`	Number of summary updates that the TAOS unit runs when small changes cause generation of Summary LSAs (Type 3) and Summary Router LSAs (Type 4).
`Incremental VL updates`	Number of incremental virtual link updates that the TAOS unit performs.
`Buffer alloc failures`	Number of buffer allocation problems that the TAOS unit has detected and from which it has recovered.
`Multicast pkts sent`	Number of multicast packets sent by OSPF.
`Unicast pkts sent`	Number of unicast packets sent by OSPF.
`LS adv. aged out`	Number of LSAs that the TAOS unit has aged and removed from its tables.
`LS adv. flushed`	Number of LSAs that the TAOS unit has flushed.
`Incremental ext.(5) updates`	Number of incremental ASE-5 updates.
`Incremental ext.(7) updates`	Number of incremental ASE-7 updates.
`Current state`	State of the External (Type-5) LSA database: Normal or Overload.
`Number of LSAs`	Number of LSAs in the External (Type-5) LSA database.
`Number of overflows`	Number of ASE-5s that exceeded the limit of the database.

Displaying the OSPF database

To display the entire OSPF database, enter the OSPF command with the `database` option. For example:

```
admin> ospf database

                        Router Link States (Area: 0.0.0.0)
Type LS ID              LS originator     Seqno     Age   Xsum
RTR  10.101.0.1         10.101.0.1      0x800002a1  746  0x8bd8
RTR  10.101.0.2         10.101.0.2      0x800002d6  539  0x0ea1
RTR  10.102.0.1         10.102.0.1      0x800002a3 2592  0x9bc1
RTR  10.103.0.204       10.103.0.204    0x800001ba 1173  0x725f
RTR  10.103.0.254       10.103.0.254    0x80000301  534  0x7066
RTR  10.104.0.1         10.104.0.1      0x800002ad  777  0xb98e
RTR  10.104.0.2         10.104.0.2      0x80000193 1258  0x265a
RTR  10.105.0.2         10.105.0.2      0x80000299  865  0x4295
RTR  10.105.0.3         10.105.0.3      0x800002e5 1057  0x4449
RTR  10.105.0.4         10.105.0.4      0x80000310 1585  0x5775
RTR  10.105.0.61        10.105.0.61     0x800002ae 1204  0xcf2e
RTR  10.105.0.200       10.105.0.200    0x80000263  213  0x4b25
RTR  10.123.0.8         10.123.0.8      0x80000401 1071  0xecf2
RTR  10.123.0.254       10.123.0.254    0x80000401 1175  0xad39
RTR  12.151.0.2         12.151.0.2      0x800006ee  825  0x0531
RTR  192.1.1.1          192.1.1.1       0x8000039b   18  0xb04b
RTR  210.210.210.1      210.210.210.1   0x800001aa  201  0x5338

               # advertisements:       17

               Checksum total:         0x7946c

                        Network Link States (Area: 0.0.0.0)
Type LS ID              LS originator     Seqno     Age   Xsum
NET  10.101.0.1         10.101.0.1      0x80000236  746  0x1d45
NET  10.102.0.1         10.102.0.1      0x80000235 2592  0x1f40
NET  10.104.0.2         10.104.0.2      0x80000179  830  0x67a8
NET  10.105.0.8         10.123.0.8      0x80000304 1071  0x0ccd
NET  10.123.0.6         12.151.0.2      0x8000023d  825  0x59ed
NET  100.103.100.204    10.103.0.204    0x80000029  252  0x8b34

               # advertisements:       6

               Checksum total:         0x1961b

                        External ASE5 Link States
Type LS ID              LS originator     Seqno     Age   Xsum
ASE5 10.103.1.0         10.103.0.204    0x8000004f 1726  0xd23f
ASE5 10.103.2.0         10.103.0.204    0x8000004f 1716  0xc749
ASE5 10.103.3.0         10.103.0.204    0x8000004f 1704  0xbc53
ASE5 10.103.4.0         10.103.0.204    0x8000004f 1692  0xb15d
ASE5 10.103.6.0         10.103.0.204    0x8000004f 1672  0x9b71
ASE5 10.103.7.0         10.103.0.204    0x8000004f 1666  0x907b
ASE5 10.103.8.0         10.103.0.204    0x8000004f 1641  0x8585
ASE5 10.107.0.0         10.103.0.254    0x80000104  250  0x1413
ASE5 10.113.0.0         10.103.0.254    0x80000121  250  0x0e76
ASE5 10.200.0.2         10.103.0.254    0x80000001  231  0xa823
ASE5 10.222.0.2         10.103.0.254    0x80000001  202  0x9f16
```

```
ASE5 11.0.0.0           10.103.0.254    0x80000027  250  0x49a6
ASE5 11.103.0.0         10.103.0.254    0x80000121  250  0xfc10
ASE5 14.240.0.0         10.103.0.204    0x800001a4  199  0x0926
ASE5 50.151.0.2         10.103.0.254    0x80000121  250  0xa90a
ASE5 101.103.0.0        10.103.0.254    0x80000121  250  0x664c
..
..
               # advertisements:       44
               Checksum total:         0x191d3a
```

The following table describes the output:

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 AS boundary routers. • Type 5 (ASE) are AS-external-LSAs that describe routes to destinations external to the Autonomous System. A default route for the Autonomous System can also be described by an AS-external-LSA. The `ext` option only displays ASE5 LSAs. • 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.

Displaying OSPF external AS advertisements

To display only OSPF External AS advertisements, include the `ext` option with the OSPF command. For example:

```
admin> ospf ext
```

```
Type LS ID              LS originator     Seqno     Age   Xsum
ASE5 10.103.1.0         10.103.0.204    0x8000004f 1702  0xd23f
ASE5 10.103.2.0         10.103.0.204    0x8000004f 1692  0xc749
ASE5 10.103.3.0         10.103.0.204    0x8000004f 1680  0xbc53
```

```
ASE5 10.103.4.0         10.103.0.204    0x8000004f 1668  0xb15d
ASE5 10.103.6.0         10.103.0.204    0x8000004f 1648  0x9b71
ASE5 10.103.7.0         10.103.0.204    0x8000004f 1642  0x907b
ASE5 10.103.8.0         10.103.0.204    0x8000004f 1617  0x8585
..
..
ASE5 214.240.0.127      10.103.0.204    0x800001a4  175  0xdb0b
ASE5 223.57.40.0        10.103.0.254    0x80000121  226  0x7540
ASE5 223.57.40.244      10.103.0.254    0x80000121  226  0xe3dc
               # advertisements:       46
               Checksum total:         0x1a1d9e
```

The output of this command is the same as for the OSPF database command, with the exception of the Type. The OSPF Ext command only shows ASE5 type LSAs.

Displaying OSPF internal AS advertisements

To display OSPF internal AS advertisements, include the `internal` option with the OSPF command. For example:

```
admin> ospf internal
                Area: 0.0.0.1
Destination     Mask            Cost
33.240.0.0      255.255.255.224  1
103.240.0.0     255.255.255.192  1
113.240.0.0     255.255.255.128  1
183.240.0.0     255.255.255.128  1
193.240.0.0     255.255.255.128  1
203.240.0.0     255.255.255.128  1
```

The following table describes the output:

Field	Specifies
`Area`	Area in which the router resides.
`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.
`Mask`	Subnet mask of the route.
`Cost`	Cost of the router.

Displaying the OSPF link-state database

To display the link-state database for the first configured area (or for the only defined area), include the `lsdb` option with the OSPF command. The TAOS unit does not currently operate as an ABR, so each TAOS unit's OSPF interface belongs to the same area. (That area number does not have to be the default backbone area 0.0.0.0.)

For example:

```
admin> ospf lsdb

                    Area: 0.0.0.0
Type LS ID              LS originator     Seqno     Age   Xsum
RTR  10.101.0.1         10.101.0.1      0x8000029f  720  0x8fd6
RTR  10.101.0.2         10.101.0.2      0x800002d1  126  0x189c
RTR  10.102.0.1         10.102.0.1      0x800002a2  767  0x9dc0
RTR  10.102.0.2         10.102.0.2      0x800002cc  124  0x862c
RTR  10.103.0.204       10.103.0.204    0x800001b8 1147  0x765d
RTR  10.103.0.254       10.103.0.254    0x800002fb  167  0x8cc9
RTR  10.104.0.1         10.104.0.1      0x800002ab  751  0xbd8c
RTR  10.104.0.2         10.104.0.2      0x80000191 1232  0x2a58
RTR  10.105.0.2         10.105.0.2      0x80000297  843  0x4693
RTR  10.105.0.3         10.105.0.3      0x800002e3 1032  0x4847
RTR  10.105.0.4         10.105.0.4      0x8000030e 1560  0x5b73
RTR  10.105.0.61        10.105.0.61     0x800002ac 1178  0xd32c
RTR  10.105.0.200       10.105.0.200    0x80000261  194  0x4f23
RTR  10.123.0.8         10.123.0.8      0x800003ff 1045  0xf1ef
RTR  10.123.0.254       10.123.0.254    0x800003ff 1149  0xb236
RTR  12.151.0.2         12.151.0.2      0x800006ec  799  0x092f
RTR  192.1.1.1          192.1.1.1       0x80000398 1791  0xb648
RTR  210.210.210.1      210.210.210.1   0x800001a8  175  0x5736
NET  10.101.0.1         10.101.0.1      0x80000234  720  0x2143
NET  10.102.0.1         10.102.0.1      0x80000234  767  0x213f
NET  10.104.0.2         10.104.0.2      0x80000177  804  0x6ba6
NET  10.105.0.8         10.123.0.8      0x80000302 1045  0x10cb
NET  10.123.0.6         12.151.0.2      0x8000023b  799  0x5deb
NET  100.103.100.204    10.103.0.204    0x80000027  226  0x8f32
               # advertisements:       24
               Checksum total:         0xa2ae6
```

The fields in the output contain the following information:

Field	Specifies
`Area`	Area ID.
`Type`	Indicates the 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 AS boundary routers. • Type 7 are ASE-7 link advertisements that are only flooded within an NSSA.
`LS ID`	Specifies the target address of the route.
`LS originator`	Specifies the address of the advertising router.
`Seqno`	Indicates a hexadecimal number that begins with 80000000 and increments by one for each LSA received.

Field	Specifies
`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, as explained in the next section.

Displaying OSPF link-state advertisements

To view detailed information about a link-state advertisement, 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 the last entry in the link-state database shown in the previous section:

```
admin> ospf lsa 0.0.0.0 ase 10.5.2.160 10.5.2.162

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

The output differs depending on the type of link. The following is an example of a router LSA:

```
admin> ospf lsa 0.0.0.0 rtr 192.1.1.1 192.1.1.1

        LS age:      66
        LS options:  (0x2) E
        LS type:     1
        LS ID (destination): 192.1.1.1
        LS originator:       192.1.1.1
        LS sequence no:      0x80000399
        LS checksum:         0xb449
        LS length:           48
        Router type:     (0x2) ASBR

        # router ifcs:   2
                Link ID:          10.105.0.8
                Link Data:        10.105.0.7
                Interface type:   (2) TrnsNetwork
                        No. of metrics: 0
                        TOS 0 metric:   10 (0)
                Link ID:          10.123.0.6
                Link Data:        10.123.0.7
                Interface type:   (2) TrnsNetwork
                        No. of metrics: 0
                        TOS 0 metric:   10 (0)
```

The next example is for a network LSA:

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

For information about the fields in the output of these commands, see the *APX 8000/MAX TNT Reference* or RFC 1583.

Displaying the OSPF routing table

To display the OSPF routing table, include the `rtab` option with the OSPF command. For example:

```
admin> ospf rtab

DTyp RType Destination       Area          Cost  Flags  Next hop(s)
IfNum
RTE  FIX   50.151.0.2/32     -             1     0x81   0.0.0.6
6
RTE  FIX   130.57.40.243/32   -             10    0x1    0.0.0.6
6
RTE  FIX   130.57.0.0/16      -             10    0x2    0.0.0.6
6
RTE  FIX   140.57.40.244/32   -             10    0x1    0.0.0.6
6
RTE  FIX   140.57.0.0/16      -             10    0x2    0.0.0.6
6
RTE  FIX   150.57.40.245/32   -             10    0x1    0.0.0.6
6
RTE  FIX   150.57.0.0/16      -             10    0x2    0.0.0.6
6
RTE  FIX   160.57.40.246/32   -             10    0x1    0.0.0.6
6
RTE  FIX   160.57.0.0/16      -             10    0x2    0.0.0.6
6
..
..
..
```

The fields in the output contain the following information:

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

The fields in the output contain the following information:

Field	Specifies
LSA type	Type of Link-State Advertisement.
ls id	Target address of the router.
adv rtr	Address of the advertising router.
age	Age of the route in seconds.
seq #	Number that begins with 80000000 and increments by one for each LSA received.
cksum	Checksum for the LSA.
Net mask	Subnet mask of the LSA.
Tos	Type of Service for the LSA.
metric	Cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.
E type	External type of the LSA indicating either 1 (Type 1) or 2 (Type 2)
Forwarding Address	Forwarding Address of the LSA (described in RFC 1583).
Tag	Tag of the LSA (described in RFC 1583).

Displaying information about OSPF areas

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

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

The fields in the output contain the following information:

Field	Specifies
`Area ID`	Area number in dotted-decimal format.
`Authentication`	Type of authentication: Simple-passwd, MD5, or Null.
`Area Type`	Type of OSPF area: Normal, Stub, or NSSA.
`#ifcs`	Number of TAOS unit interfaces specified in the area.
`#nets`	Number of reachable networks in the area.
`#rtrs`	Number of reachable routers in the area.
`#brdrs`	Number of reachable area border routers in the area.
`#intnr`	Number of reachable internal routers in the area.

Displaying information about OSPF routers

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

```
admin> ospf routers
DType RType Destination   Area         Cost     Next hop(s)      IfNum
ASBR  OSPF  10.101.0.1    0.0.0.0        11    10.101.0.2        20
ASBR  OSPF  10.101.0.2    0.0.0.0        10    10.101.0.2        20
ASBR  OSPF  10.103.0.204  0.0.0.0        1     100.103.100.204   24
ASBR  OSPF  10.104.0.1    0.0.0.0        12    10.105.0.4        21
                                              10.105.0.61       21
ASBR  OSPF  10.104.0.2    0.0.0.0        11    10.105.0.4        21
                                              10.105.0.61       21
  BR  OSPF  10.105.0.2    0.0.0.0        1     10.105.0.2        21
ASBR  OSPF  10.105.0.2    0.0.0.0        1     10.105.0.2        21
ASBR  OSPF  10.105.0.3    0.0.0.0        1     10.105.0.3        21
ASBR  OSPF  10.105.0.4    0.0.0.0        1     10.105.0.4        21
ASBR  OSPF  10.105.0.61   0.0.0.0        1     10.105.0.61       21
ASBR  OSPF  10.105.0.200  0.0.0.0        1     10.105.0.200      21
ASBR  OSPF  10.123.0.8    0.0.0.0        1     10.105.0.8        21
ASBR  OSPF  10.123.0.254  0.0.0.0        1     100.103.100.123   24
  BR  OSPF  12.151.0.2    0.0.0.0        1     10.105.0.6        21
ASBR  OSPF  192.1.1.1     0.0.0.0        1     10.105.0.7        21
```

The fields in the output contain the following information:

Field	Specifies
DType	Internal route type. DType displays one of the following values: RTE (generic route), ASBR (AS border route), or BR (area border route).
RType	Internal router type.
Destination	Router's IP address.
Area	Area in which the router resides.
Cost	Cost of the router.
Next hop(s)	Next hop in the route to the destination.
IfNum	Number of the interface used to reach the destination.

Displaying OSPF interfaces

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

Displaying summarized information

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

```
admin> ospf intf
```

```
Ifc Address     Phys     Assoc. Area     Type   State    #nbrs #adjs DInt
10.103.0.254    ie0      0.0.0.0         Brdcst DR        0     0    40
10.105.0.254    ie1-7-1  0.0.0.0         Brdcst Other     9     1    40
100.103.100.254 ie1-7-4  0.0.0.0         Brdcst Other     2     2    40
50.151.0.2      apx1     0.0.0.0         P-P    P-P       0     0    120
10.103.0.254    m2       0.0.0.0         P-P    P-P       1     1    120
10.103.0.254    m1       0.0.0.0         P-P    P-P       1     1    120
```

The fields in the output contain the following information:

Field	Specifies
Ifc Address	Address assigned to the TAOS unit's Ethernet interface. To identify WAN links, use the Type and Cost fields.
Phys	Name of the interface or the Connection profile for WAN links.
Assoc. Area	Area in which the interface resides.
Type	Point-to-Point (P-P) or Broadcast (Brdcst). WAN links are P-P links.
State	State of the link according to RFC 1583. There are many possible states, and not all states apply to all interfaces.
#nbrs	Number of neighbors of the interface.
#adjs	Number of adjacencies on the interface.

Field	Specifies
DInt	Number of seconds that the TAOS unit waits for a router update before removing the router's entry from its table. The interval is called the Dead Interval.

Displaying specific information about a specific interface

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

```
admin> ospf intf interface-address
```

For example:

```
admin> ospf intf 194.194.194.2
              Interface address:      194.194.194.2
              Attached area:          0.0.0.0
              Physical interface:     phani (wan1)
              Interface mask:         255.255.255.255
              Interface type:         P-P
              State:                  (0x8) P-P
              Designated Router:      0.0.0.0
              Backup DR:              0.0.0.0
              Remote Address:         194.194.194.3
DR Priority:       5  Hello interval:  30   Rxmt interval:  5
Dead interval:   120  TX delay:         1   Poll interval:  0
Max pkt size:   1500  TOS 0 cost:      10
# Neighbors:       1  # Adjacencies:    1   # Full adjs.:   1
# Mcast floods: 1856  # Mcast acks:  1855
```

The fields in the output contain the following information:

Field	Specifies
Interface Address	IP address specified for 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). 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.
Designated Router	IP address of the designated router for the interface.
Backup DR	IP address of the backup designated router for the interface.
Remote Address	IP address of the remote end of a Point to Point (WAN) link.
DR Priority	Priority of the designated router.
Hello interval	Interval in seconds that the TAOS unit sends Hello packets (as defined in RFC 1583).

Field	Specifies
`Rxmt interval`	Retransmission interval (as described in RFC 1583).
`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 Count`	Type of Service normal (*0*) cost.
`# neighbors`	Number of neighbors.
`# adjacencies`	Number of adjacencies.
`# Full adjs.`	Number of fully-formed adjacencies.
`# Mcast floods`	Number of multicast floods on the interface.
`# Mcast acks`	Number of multicast acknowledgments on the interface.

Displaying OSPF neighbors

To display information about OSPF neighbors to the TAOS unit, include the `nbrs` option with the OSPF command. For example:

```
admin> ospf nbrs

Neighbor ID     Neighbor addr   State      LSrxl DBsum LSreq Prio Ifc
10.105.0.4      10.105.0.4      2Way/-       0     0     0     5  ie1-7-1
10.105.0.2      10.105.0.2      2Way/-       0     0     0     5  ie1-7-1
12.151.0.2      10.105.0.6      2Way/-       0     0     0     1  ie1-7-1
10.105.0.3      10.105.0.3      2Way/-       0     0     0     5  ie1-7-1
10.105.0.61     10.105.0.61     2Way/-       0     0     0     5  ie1-7-1
210.210.210.1   10.105.0.49     Exstar/BDR   0     0     0     5  ie1-7-1
192.1.1.1       10.105.0.7      2Way/-       0     0     0     5  ie1-7-1
10.123.0.8      10.105.0.8      Full/DR      0     0     0     5  ie1-7-1
10.105.0.200    10.105.0.200    2Way/-       0     0     0     5  ie1-7-1
10.103.0.204    100.103.100.204 Full/DR      0     0     0     5  ie1-7-4
10.123.0.254    100.103.100.123 Full/BDR     0     0     0     5  ie1-7-4
10.102.0.2      10.102.0.2      Init/-       0     0     0     5  m1
10.101.0.2      10.101.0.2      Full/-       0     0     0     5  m1
```

The fields in the output contain the following information:

Field	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).

Field	Specifies
`State`	State of the link-state database exchange. Full indicates that the databases are fully aligned between the TAOS unit and its neighbor. For a description of possible states, see RFC 1583.
`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 particular OSPF neighbor, append the Neighbor ID to the `nbrs` option. For example:

```
admin> ospf nbrs 10.105.0.4
OSPF Router ID:         10.105.0.4
               Neighbor IP address:    10.105.0.4
               Neighbor State:         (0x8) 2Way
               Physical interface:     ie1-7-1 (ie1-7-1)
               DR choice:              10.105.0.8
               Backup choice:          10.105.0.49
               DR Priority:            5
  DB summ qlen:      0  LS rxmt qlen:      0  LS req qlen:       0
  Last hello:        6
  # LS rxmits:       0  # Direct acks:     0  # Dup LS rcvd:     0
  # Old LS rcvd:     0  # Dup acks rcv:    0  # Nbr losses:      0
  # Adj. resets:     0
```

Diagnostic tools for IPX routers

The TAOS unit provides two diagnostic commands for monitoring IPX networks, Show Netware Servers and Show Netware Networks.

To display the IPX service table, first enter the Terminal-Server command to access the TAOS unit's terminal server interface, then enter the Show command with the `netware servers` option. For example:

```
admin> terminal-server
** Ascend APX Terminal Server **
ascend% show netware servers
IPX address                     type            server name
ee000001:000000000001:0040      0451            server-1
```

The output contains these fields:

- `IPX address`: The IPX address of the server. The address uses this format:
  `network number:node number:socket number`

- `type`: The type of service available (in hexadecimal format). For example, 0451 designates a file server.
- `server name`: The first 35 characters of the server name.

To display the IPX routing table, enter the Show command with the `netware networks` option. For example:

```
ascend% show netware networks
network     next router        hops        ticks   origin
CFFF0001    00000000000        0         1       Ethernet        S
```

The output contains these fields:

Fields	Descriptions
`network`	The IPX network number.
`next router`	The address of the next router, or 0 (zero) for a direct or WAN connection.
`hops`	The hop count from the shelf controller to the network.
`ticks`	The tick count to the network.
`origin`	The name of the profile used to reach the network. If the origin is a network connected to a TAOS unit's Ethernet interface, the Origin field displays `Ethernet`.

Note: An `S` or an `H` flag can appear next to the origin. `S` indicates a static route. `H` indicates a hidden static route. Hidden static routes occur when the router learns of a better route.

Diagnostic tools for displaying filter information

The Filterdisp command enables you to display information about filters in use for active sessions. The command uses the following syntax:

```
filterdisp usage: filterdisp <sessNum>
        without <sessNum> : display all active sessions and
                            their filter names
         with <sessNum>    : display filter details of the session
```

Displaying filter information for all active sessions

With no arguments, the command output lists all active sessions with associated filter information. For example:

```
admin> filterdisp
ID   Username    Src Route-Filter Data-Filter Call-Filter TOS-Filter
-------------------------------------------------------------------
010  dialin-23   ext
016  dialin-4    ext
017  edleung     ext               < filters present >
018  jwebster    ext               < filters present >
019  pyan        loc            datfilt2       callfilt4  tostestfilt
020  guest       ext
021  pvc2        loc    route-pvc                  gen_callfilt
```

```
022  pvc4        loc                                  gen_callfilt
023  pvc5        loc
<end user list>  9 active user(s)
```

The output displays a session ID number, username, and an indication of where the session was authenticated (local or external). Sessions authenticated by local profiles display the filter names specified in the Connection profile. Externally authenticated sessions, such as RADIUS sessions, have no associated filter names so they appear with a `<filters present>` notation. The columns in the command output provide the following information:

Output field	Specifies
ID	Identification number for the session.
Username	Name of the authenticated profile.
Src	Source of the profile: whether it is downloaded through RADIUS (ext) or is a local profile (loc).
Route-Filter	If 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	If 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	If a call filter has been applied to the session. For sessions authenticated locally, the name of the filter is supplied. For externally authenticated sessions, `<filters present>` indicates that a call filter has been applied. If blank, no call filter applies.
TOS-Filter	If a type of service (TOS) filter has been applied to the session. For sessions authenticated locally, the name of the filter is supplied. For externally authenticated sessions, `<filters present>` indicates that a TOS filter has been applied. If blank, no TOS filter applies.

Displaying filter details for a single active 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, first use the Filterdisp command without an argument, as described in the preceding section.) 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
dummyForPadding = 0
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
dummyForPadding = 0

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
```

Displaying software version log messages

To facilitate troubleshooting procedures, you can configure the TAOS unit to log the current software version every hour, rather than at system startup only. Following is a sample log message:

```
LOG debug, Shelf 1, Controller, Time: 13:00:46--
Software version 8.0.0
```

Following is the relevant parameter, shown with its default value:

```
[in LOG]
log-software-version = no
```

Parameter	Specifies
Log-Software-Version	Enable/disable hourly log messages reporting the current software version. The message is sent to the Syslog host. If Debug permission is enabled, the message is also displayed on the screen.

Displaying Ethernet packet contents

The Ether-Display command displays the hexadecimal contents of Ethernet packets being received and transmitted on the specified Ethernet port. You must specify how many octets of each packet you want to display.

The Ether-Display command requires that you enable debug output as follows:

```
admin> debug on
Diagnostic output enabled
```

The following example displays 12 octets of each packet on a ports:

```
admin> ether-display 0 12

ETHER XMIT: 12 of 60 octets

107E1350: 00 c0 80 89 03 d7 00 c0  7b 6b 9f d6                ........
{k..

ETHER XMIT: 12 of 64 octets

107E1350: 00 c0 80 89 03 d7 00 c0  7b 6b 9f d6                ........
{k..

ETHER RECV: 12 of 60 octets

107B8FD4: 00 c0 7b 6b 9f d6 00 c0  80 89 03 d7                 ........

{k..
```

```
ETHER XMIT: 12 of 407 octets
107E1350: 00 c0 80 89 03 d7 00 c0  7b 6b 9f d6                ........
{k..
ETHER XMIT: 12 of 161 octets
107E1350: 00 c0 80 89 03 d7 00 c0  7b 6b 9f d6                ........
{k..
ETHER RECV: 12 of 60 octets
..
..
..
```

To stop displaying the Ethernet statistics, specify 0 (zero) octets:

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

Alternatively, you can stop the display by disabling debug output:

```
admin> debug off
Diagnostic output disabled
```

For complete information about the Ether-Display command, see the *APX 8000/MAX TNT Reference*.

Using Debug Commands

4

Note: Every attempt has been made to confirm that this chapter correctly describes the functionality and output of the TAOS unit's debug commands. However, while debug mode can be a very valuable troubleshooting tool for anyone, its primary focus is on the requirements of Lucent's development engineers. For this reason, Lucent does not guarantee the completeness of the list of commands published for a given release nor the exhaustive cataloging of their functionality.

Caution: Under most circumstances, debug commands are not required for correct operation of the TAOS unit. And in some circumstances they might produce undesirable results. Please use the following information with caution. Contact Lucent Technical Support with any questions or concerns.

Enabling debug permissions

Before you can access the debug commands, you must log into the TAOS unit with a User profile that specifies debug privileges.

To enable debugging privileges:

1 Open a user profile:

```
admin> open user admin
```

2 Enable debug permissions:

```
admin> set allow-debug=yes
```

This is a hidden parameter. It does not appear in the interface.

3 Write the profile to save the changes:

```
admin> write
```

Note that when you are logged into the TAOS unit with debug privileges, the interface might display normally unavailable parameters and commands, some of which are not configurable in certain situations. For this reason, you should create a special profile for debugging purposes, and only use that profile when you are debugging the TAOS unit.

Centralizing debug output

The Diag command, introduced in TAOS 9.0, enables centralized control of all debug output in the system. In previous releases, many debug commands existed, and each enabled you to turn debug output on or off for a particular system component. Now the functions of many of these commands have been consolidated in a single Diag command. The sections that follow describe its basic uses.

Note: Which Diag command options are available depends on whether you type the command at the console or from a slot card. For those options specific to a particular slot card, you must open a session with the slot card before executing the command.

Determining which system components have debug output

To generate a list of all the system components for which you can generate debug output, enter the following command:

```
admin> diag ?
```

Following is a partial list of the components that the system displays:

```
arp                          ( Address Resolution Protocol )
networki                     ( Call Control )
vrouter <0xffff>             ( Virtual Router )
vroutercb                    ( Control Bus )
xdb <0xff>                   ( Radius )
zip                          ( AppleTalk )
```

Enabling or disabling debug output

To enable debug output for all system components, enter the following:

```
admin> diag ALL
```

To enable or disable debug output for a particular system component, enter the following command:

```
admin> diag component
```

The command works as a toggle. For example, to enable debug output for ARP, enter the following:

```
admin> diag arp
arp debug is ON
```

To disable ARP output, enter the following:

```
admin> diag arp
arp debug is OFF
```

To list all system components with debug output enabled, enter the following:

```
admin> diag -l
```

Enabling debug output for components with output disabled

To enable debug output for all components for which output is currently disabled, enter the following:

```
admin> diag ON
```

For example, suppose that the `networki` and `zip` components are currently disabled. To enable them, enter the following:

```
admin> diag ON
networki debug is ON
zip debug is ON
```

Enabling debug output

To enable debug output for all commands on the system or on a card, use the Debug command as in the following examples.

To enable debug:

```
hdlc-2/1> debug on
Diagnostic output enabled
```

To disable debug:

```
hdlc-2/1> debug off
Diagnostic output disabled
```

When you enable debug output, the TAOS unit displays the debug messages on the terminal screen.

Debug levels

Debug levels determine the number and type of messages displayed. But generally, the lower you set the debug level, the fewer messages the TAOS unit displays. Setting the debug level to 0 (zero) disables the debug output for the command.

Set the debug level with the specific debug command followed by the `-t` option, as in the following examples:

```
admin> ifmgr -t 0
ifmgr debug level is now 0 (disabled)


admin> ifmgr -t 4
ifmgr debug level is now 4 (enabled)
```

Getting online help for debug commands

To see a list of all commands, including the debug commands, enter ? at the command prompt, as in the following example:

```
admin> ?
 ?                              ( user )
 @fatalTest                     ( debug )
 acctevnt                       ( debug )
 addrpool                       ( debug )
 ARA                            ( debug )
 aracbmgr                       ( debug )
 arptable                       ( system )
 atmpdebug                      ( debug )
 auth                           ( user )
 briChannels                    ( system )
 brouterDebug                   ( debug )
 brouterLoad                    ( debug )
 brouterMessage                 ( debug )
 brouterSave                    ( debug )
 brouterstats                   ( debug )
 cadslLines                     ( system )
 callback                       ( debug )
 callblocks                     ( debug )
 callroute                      ( diagnostic )
 cbacctevnt                     ( debug )
 cbcardif                       ( debug )
 cbcifping                      ( debug )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

To get basic help for a debug command, enter the Help command, followed by the name of the debug command, as in the following example:

```
admin> help ifmgr
ifmgr usage: ifmgr -option
             -d  (d)isplay interface table entries.
             -d  <ifNum> (d)etails of given i/f table entry.
             -t  (t)oggle debug display.
       ifmgr [up|down] [ifNum|ifName]
```

Using combinations of commands

Since most debug commands are designed to give a developer information about specific portions of TAOS unit's functionality, you might find it helpful to use commands in combination to troubleshoot different problems.

For example, if you see problems with the initial connection of remote users, you might want to use a combination of `Networki`, `Routmgr` and `Wantoggle` to obtain a complete view of three functions involved in establishing a call.

When troubleshooting modem-related issues, you might want to use `Modemdrvstate`, `Modemdiag` and `Mdialout` (if modem outdial is supported on your TAOS unit) to get all modem-related information for your calls.

Using several commands simultaneously not only gives you a clearer picture of a given situation, it also shows you a chronological timeline of the events that are happening.

Using the debug commands

Debug commands allow you to monitor and diagnose different areas of the TAOS unit's functionality. This section lists some of the more common debug commands and the areas of the TAOS unit's they apply to.

Frame Relay

The following commands display information about Frame Relay interfaces.

- FRDLstate
- FRdump
- FRinARP
- FRLinkState
- FRLMI
- FRMgrDump
- FRPriorityErrors
- FRScert
- FRstate

Calls

The following commands display information about how the TAOS unit handles calls.

- Callback
- Permconn-list
- Tntcall
- Routmgr

Authentication

The following commands display information about how the TAOS unit authenticates calls.

- Authendebug
- Lanval
- Radacct
- Raddbgdump
- Radif
- Radservdump

- Radsessdump
- Radstats

Host-side devices

The following commands display information about the TAOS unit's host devices.

- ModemDrvDump
- ModemDrvState
- Modemd1stats, Modemd2stats, Modemd3stats
- Ether-Stats
- Ifmgr

Network-side devices

The following commands display information about the TAOS unit's network devices.

- NetIF
- Networki
- Pridisplay
- WANdisplay
- WanEventsStats
- WANopening
- Wantoggle

Protocols

The following commands display information about the TAOS unit's protocols.

- Addrpool
- Brouterdebug
- Brouterload
- Ctcheck
- Ctdebug
- Ipxripdebug
- Lcstate
- Leakpool
- Ospfavltree
- Ospfdebug
- Sntp
- Tcpflushtimer

Tunneling

The following commands display TAOS unit tunneling information.

- ATMP
- Dtunnel
- Tunneldebug
- Tunnelslot

System and devices

The following commands display information about the TAOS unit's system and devices.

- Pools
- Portinfo
- Reset
- Revision
- Stacklimit
- Stackusage
- Tsshow
- Update
- Watchdogtoggle

Terminal server

The following commands display information about the TAOS unit's terminal server.

- Telnetdebug
- Tsbadterminfo

Special administrative commands

The following command should only be used when requested by Lucent technical support.

- Coredump

Alphabetical list of debug commands

This section describes the TAOS unit's debug commands in alphabetic order. The information is organized for quick reference, and does not include tutorials.

Acct-Failsafe

Description: The Acct-Failsafe debug command is available on the shelf contoller or the host cards for verifying correct accounting proxying. (Slot host cards do not include the `-d` option.)

```
admin> acct-failsafe
usage: acct-failsafe -option [ params ]
       -d <shelf> <slot>
           (d)isplay AFS info for <shelf> <slot>
       -d (d)isplay AFS info for all relevant slots
```

```
       -t (t)oggle module debug level
       -? display this summary
```

To display information about the calls on any slot which are candidates for proxy accounting.:

```
admin> acct-failsafe -d
Slot 1/8:
HashTable @ 10542160, bucketCount: 192, callCount: 23, hashName
<afs-1:8>
Slot 2/5:
HashTable @ 10585730, bucketCount: 48, callCount: 7, hashName
<afs-2:5>
```

To display the same information for a single slot card in shelf 1, slot 8:

```
admin> acct-failsafe -d 1 8
Slot 1/8:
HashTable @ 10542160, bucketCount: 192, callCount: 23, hashName
<afs-1:8>
```

To specify which level of debug to use for the command, use the –t option. A debug level of zero indicates none (no messages). A level of 7 is fairly verbose.

Addrpool

Description: Displays messages related to dynamic address pooling. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`addrpool`** at the command prompt.

Example: Following are several examples of output produced when Addrpool is active.

With 18 addresses currently allocated from a pool:

```
ADDRPOOL: lanAllocate index 0 inuse 18
```

The address 208.147.145.155 was just allocated:

```
ADDRPOOL: allocate local pool address [208.147.145.155]
```

The address 208.147.145.141 is to be freed because the user of that address has hung up. The TAOS unit must find the pool to which the address belonged, then free the address so it is available for another user:

```
ADDRPOOL: found entry by base [208.147.145.141] entry
[208.147.145.129]
ADDRPOOL: free local pool address [208.147.145.141]
```

In the IP Global profile, the Pool-Base-Address [1] is set to 192.168.8.8, and Assign-Count [1] is set to 4:

```
ADDRPOOL: Deleting addrPool
ADDRPOOL: New Addr pool rc = 0
addrPool index 1 ip [192.168.8.8] count 4
```

The Assign-Address parameter of an existing pool is changed from 4 to 3:

```
ADDRPOOL: Deleting addrPool
ADDRPOOL: New Addr pool rc = 0
addrPool index 1 ip [192.168.8.8] count 3
```

A second pool is created. In the IP Global profile, the Pool-Base-Address [2] is set to 192.168.8.8, and Assign-Count [2] is set to 10:

```
ADDRPOOL: Deleting addrPool
ADDRPOOL: New Addr pool rc = 0
addrPool index 1 ip [192.168.8.8] count 4
ADDRPOOL: New Addr pool rc = 0
addrPool index 1 ip [192.168.8.8] count 4
addrPool index 2 ip [192.168.10.1] count 10
```

The second pool is deleted:

```
ADDRPOOL: Deleting addrPool
ADDRPOOL: New Addr pool rc = 0
addrPool index 1 ip [192.168.8.8] count 4
```

ATMPdebug

Description: Displays messages related to Lucent's Ascend Tunnel Management Protocol (ATMP) sessions. (ATMP is described in RFC 2107.) The command is a toggle that alternately enables and disables the debug display. You would normally use this command with the Tunneldebug command.

Usage: Enter **`atmpdebug`** at the command prompt.

Example:

The mobile node sends a request to foreign agent asking for connection to the home agent:

```
ATMP: sendRegReq: HA=200.67.1.254:5150  RcvUdp=5150
ATMP: Id=162, FA=130.67.40.254
ATMP:MC=141.111.40.82, HomeNetName=[]
```

The home agent sets up a tunnel:

```
ATMP: received cmd <RegisterRequest> from 130.67.40.254:5150
ATMP: procRegReq: from=130.67.40.254:5150
ATMP: FA=130.67.40.254, MC=141.111.40.82, HomeNet=
ATMP: sendChallReq: to 130.67.40.254:5150, Id=162, EC=Good completion
ATMP: received cmd <ChallengeReply> from 130.67.40.254:5150
ATMP: procChallReply: from 130.67.40.254:5150, Id=162
ATMP: sendRegisterReply: to udp=5150, Id=162, Tunnel=156, EC=Good
completion
```

AuthenDebug

Description: Displays messages related to Link Control Protocol (LCP) authentication on the TAOS unit. The command is a toggle that alternately enables and disables the debug display. This command is available on host cards such as the HDLC card and the modem card.

Usage: `authendebug`

Example: The following display indicates a successful PAP authentication.

```
AUTH: lcp_pap_req(remote=0)
AUTH-3: verify_pap(given<len.id=13:140.57.40.135, pwdLen=6>)
AUTH-3: verify_pap No authData - getting one
AUTH-3: verify_pap: authDispatcher() == OK
AUTH-3: verify_pap_callback: AUTHCOMMAND_SUCCESS
```

BrouterDebug

Description: Displays messages related to the router functionality of the TAOS unit. The command is a toggle that alternately enables and disables the debug display.

You can use this command for a general view of the load experienced by the TAOS unit.

Usage: Enter **`brouterdebug`** at the command prompt.

Example: Typically, `brouterdebug` displays very few messages. The following session took place over a period of several minutes on a TAOS unit with 40–45 users active.

```
admin> brouterdebug
BROUTER debug display is ON
BROUTER_LOAD_MSG: time= 0
BROUTER_LOAD_MSG: time= 1
BROUTER_LOAD_MSG: time= 0
admin> brouterdebug
BROUTER debug display is OFF
```

The BROUTER_LOAD_MSG message is an indication of how busy the TAOS unit's router function is. A low number, as is illustrated here, indicates the router is not experiencing any problems.

BrouterLoad

Description: Reports router backlog time, which indicates whether the TAOS unit is experiencing any delay. The time is shown in ticks. Multiply the number of ticks by ten to get the time in milliseconds.

You can use this command for a general view of the load experienced by the TAOS unit.

Usage: Enter **`brouterload`** at the command prompt.

Example: The following display indicates no delays in the router.

```
admin> brouterload
BROUTER load time is 0 ticks (x10msec)
```

Ctdebug

Description: Displays messages related to CIDR routing. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`ctdebug`** at the command prompt.

Example:

```
admin> ctdebug
CIDR tree debug is 0
```

DTunnel

Description: Displays the status of enabled tunnels on the TAOS unit.

Usage: Enter **dtunnel** at the command prompt.

Example:

```
admin> dtunnel
MajDev  Proto  Agent Mode      HA Type  IPX sap   UDP   password
------  -----  ----------      -------  -------  -----  --------
   7     ATMP  Home-Agent      Router   disabled  5150  lucent
   Idle-Limit 120 mins

Tunnels:
-------------------------------------------------
Tunnel 36734  IfNum 65535  Majdev 7  Agent Address 130.67.40.254:5150
 Ident=0x56  TN=0x47BF  DnsSN=0
 ATMP Home-Agent
 State 5 (UP)  Router Mode  Home Network Name
 Remote client   Idle-Limit 120 mins
 Client IP Address 141.111.40.86/32
-------------------------------------------------
Tunnel 36732  IfNum 65535  Majdev 7  Agent Address 130.67.40.254:5150
 Ident=0x55  TN=0x47BE  DnsSN=0
 ATMP Home-Agent
 State 5 (UP)  Router Mode  Home Network Name
 Remote client   Idle-Limit 120 mins
 Client IP Address 141.111.40.85/32
```

Ether-Stats

Description: Displays all statistics and error counters maintained by the 10Base-T Ethernet driver.

Usage: `ether-stats 0 n`

Where `0` is the first Ethernet port for which to display statistics and `n` is the last.

Example:

```
admin> ether-stats 0
Tx unicast:     48382
   non-unicast: 23736
   octets:      10746332
   collisions:  443
   dma under:   0
   cts loss:    0
   no carrier:  0
```

```
   late coll:   0
Rx unicast:     45952
   non-unicast: 31307
   octets:      13491043
   collisions:  0
   short frame: 0
   dma over:    0
   no resource: 0
   Alignment:   0
   Unaligns:    0
   Length Errs: 0
   Restarts:    0


   admin> ether-stats 0-10
   Tx unicast:     48559
      non-unicast: 23784
      octets:      10805138
      collisions:  443
      dma under:   0
      cts loss:    0
      no carrier:  0
      late coll:   0
   Rx unicast:     46165
      non-unicast: 31500
      octets:      13576590
      collisions:  0
      short frame: 0
      dma over:    0
      no resource: 0
      Alignment:   0
      Unaligns:    0
      Length Errs: 0
      Restarts:    0
```

FRDLstate

Description: Displays information regarding the state of the Frame Relay connections, focusing mostly on Data Link information. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`frdlstate`** at the command prompt.

Example:

```
admin> frdlstate
FRDLCALL state display is now ON
```

In this example, an outgoing call is to be placed. A route to the destination is available over a Frame Relay link. The following message appears:

```
FRDLCALL: Clear Call for route: 136
```

The following message indicates that an outgoing call is connected:

```
FRDLCALL-136: call complete, status 1, 0 channels
```

The next message indicates that either the TAOS unit or the far end device has destroyed a route. The TAOS unit updates its table to reflect this routing change.

```
FRDLCALL-136: dead call
FRDLCALL-136: route destroyed
```

FRdump

Description: Displays a snapshot of the Frame Relay Interface table. The display shows data for each DLCI assigned to a Frame Relay link.

Usage: Enter **`frdump`** at the command prompt.

Example:

```
admin> frdump
* Frname  State  DLinkAddr  routeID.id frmgrLink dlIfNum dlIfSpeed
  frt14    CONNECTED  1012c920  15  0 738 512000
   *dlci Addr  ifNum routeID   dataLink   state
304    100cada0    23   136       1012c920     INACTIVE
   frt18    CONNECTED  1012ffa0  14  0 742 1536000
   *dlci Addr  ifNum routeID   dataLink   state
306    101719a0    33   36       1012ffa0     ACTIVE
 604    10193c60    27   32       1012ffa0     ACTIVE
 603    10191fe0    26   31       1012ffa0     ACTIVE
   frt17    CONNECTED  10149b60  13  0 741 1536000
   *dlci Addr  ifNum routeID   dataLink   state
305    101975e0    32   35       10149b60     ACTIVE
 600    101910a0    24   30       10149b60     ACTIVE
 303    1018cea0    22   28       10149b60     ACTIVE
 301    10186360    20   26       10149b60     ACTIVE
frt16    CONNECTED  1017ad20  7  0 740 1536000
   *dlci Addr  ifNum routeID   dataLink   state
605    101961e0    29   34       1017ad20     ACTIVE
 300    1018a820    21   27       1017ad20     ACTIVE
frswan4    CONNECTED  10125ba0  2  0 734 64000
   *dlci Addr  ifNum routeID   dataLink   state
411    101592a0    31   5       10125ba0     ACTIVE
 407    10155ae0    30   4       10125ba0     ACTIVE
 403    10153be0    25   3       10125ba0     ACTIVE
```

FRinARP

Description: Performs an Inverse ARP test over the specified Frame Relay link and DLCI. You can use FRinARP to help troubleshoot connectivity and routing problems over a Frame Relay link.

Usage: **`frinarp Frame_Relay_profile_name DLCI`**

Example:

```
admin> frinarp FR-1 38
frInArp: frinarp  frname  dlci
```

```
Inverse Arp op 2304 hw type 3840 prot type 8 hw len 2 prot len 4
Source Hw address 0401 Target Hw address 0000
Source Protocol address cd933401 Target Protocol address cd930005
```

FRLinkState

Description: Displays Frame Relay control messages. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`frlinkstate`** at the command prompt.

Example:

```
admin> frlinkstate
FR control msg display is ON
```

The following message indicates that the TAOS unit sent a Frame Relay Status Enquiry. The Send sequence number is 135. The Receive sequence number is 134.

```
FRMAIN: time 67192300, send status enquiry (135,134)
```

The next message indicates that DLCI 16 is being processed. This is a normal message. You should see one `process` message for each DLCI.

```
process pvc dlci 16
```

FRLMI

Description: Displays Frame Relay Local Management Interface (LMI) information. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter `frlmi` at the command prompt.

Example:

```
admin> frlmi
FRMAIN: Lmi display is ON
FRMAIN: Setting timer DTE
```

The following message validates the consistency of sequence numbers in LMI messages. The 144 after `want` indicates the original sequence number the TAOS unit sent. The two numbers after the second `got` indicate the switch's Send sequence number and the Switch's report of the last sequence number it received from the TAOS unit, respectively. The original sequence number should match the switch's report of the last sequence number it received.

```
FRMAIN: Time 67201400, got link report: want (*,144), got (144,144)
```

FRMgrDump

Description: Displays the Frame Relay link and DLCI information, including states and counters.

Usage: Enter **`frmgrdump`** at the command prompt.

Example:

```
admin> frmgrdump
Data Link Info
Status
B04FBD40 ACTIVE   B04C0480 1532   19759603   19530429
Status
enq sent =      66710              rsp rcvd =      66763
upd rcvd =         53              timeouts =          1
Errors
UI field =          0              PD field =          0
CR field =          0              msg type =          0
stat rsp =          0              lock shf =          0
inv info =          0              rpt type =          0
Last Error
type = 5
time =       6100
Fr Type 0      value: 20 octets @ B04FBE26
[0000]: 04 91 03 CC 45 00 00 3A 4B 0E 00 00 7F 11 54 D7
[0010]: CD 93 08 07
LMI type =  AnnexD
DTE Monitor  n391 = 6, t391 = 10, n392 = 3, n393 = 4
Event: recv seq 155 send Seq 155 Index = 0, cycles left = 4
OK OK OK OK OK OK OK OK OK OK
DCE Monitor  t392 = 15,n392 = 3, n393 = 4
Event:  dce send seq 0  index = 0
OK OK OK OK OK OK OK OK OK OK
DLCI info
--addr-- dlci --state- userHndl n201 --check- -pkt xmit- -pkt recv-
B04C09A0    0 ACTIVE          0 1532 NO CHECK      66710      66763
---DE--- --FECN-- --BECN-- -crTime-  chgTime  pending
0        0        0      100      100 FALSE
```

FRPriorityErrors

Description: Reports statistics about Frame Relay priority errors on a host card. All values in its output should be zero. A non-zero value indicates an extreme shortage of memory.

For example:

```
hdlc-1/5> frPriorityErrs
Output:
_sendStatusEnquiryNoMbuf: 0
_mkStatusReplyNoBuf:      0
_mkStatusReplyMbuf:       0
```

FRScert

Description: Toggles between Sprint and Frame Relay Forum LMI checks. The default is the Sprint certification policy. In most cases, the default setting is correct and should not be changed.

Usage: Enter **frscert** at the command prompt.

Example:

```
admin> frscert
frSCert is FRFCert
admin> frscert
frSCert is SCert
```

FRstate

Description: Displays messages related to Frame Relay state changes. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **frstate** at the command prompt.

Example: An administrator enables the display, data is received from the Frame Relay interface and processed, and the administrator disables the display.

```
admin> frstate
FRrly state display is ON
FRRLYIF: Calling frifRecv routeId 20
FR1490 dataFrom wan entry state 2
FRRLYIF: Send up stack ifnum 1
FRRLYIF: Calling frifRecv routeId 20
FR1490 dataFrom wan entry state 2
FRRLYIF: Send up stack ifnum 7
FRRLYIF: frIfSend ifNum 1
FR1490 data to  wan entry state 2
FRRLYIF: datatoWan datalink B04C0480
admin> frstate
 FRrly state display is OFF
```

GRE

Description: Displays the TAOS unit's Generic Routing Encapsulation (GRE) information. The command has little practical use other than as a tool for developmental engineering.

IFMgr

Description: Displays interface-table entries for the Ethernet interface, toggles the debug display, and marks an interface as enabled or disabled. This command is available on the shelf controller and on host cards such as the Ethernet, modem, and HDLC cards. The output differs slightly depending on where the command is executed.

Usage: **ifmgr** [**-d** [***ifnam/ifnum***] | **-t**] [**up**|**down** ***ifnum***|***ifname***]

Syntax element	Description
-d	Display interface table entries.
-d ***ifname/ifnum***	Display details of the specified interface name or number.
-t	Toggle debug display.
up | **down** ***ifnum*** | ***ifname***	Enable or disable the specified interface. These options have the same effect as setting the Enabled parameter in the Ethernet profile, and are subject to the same limitations.

Example: To view the IFMgr usage summary for an Ethernet card in slot 4, first open a session to the card:

```
admin> open 1 4
```

Then you can use the `-d` option to view the interface number and name:

```
ether-1/4> ifmgr -d
if  slot:if  u p ifname   mac addr      local-addr
------------------------------------------------
000 0:00:000 *   pb0      000000000000  0.0.0.0/32
001 1:17:011 *   ie1-4-1  00c07b6d23f0  11.1.1.1/32
002 1:17:013 *   ie1-4-2  00c07b6d23f1  11.1.2.1/32
003 1:17:015 *   ie1-4-3  00c07b6d23f2  11.1.3.1/32
004 1:17:017 *   ie1-4-4  00c07b6d23f3  11.1.4.1/32
005 1:17:019 *   ie1-4-5  00c07b6d23f4  11.1.5.1/32
<end>
```

The IFMgr `-d` output for an Ethernet card contains the following fields:

Field	Description
`if`	Ethernet interface number.
`slot:if`	Shelf, slot and system-wide interface number. (This interface number is reported by executing the IFMgr command on the shelf controller.)
`u`	Flag indicating whether the interface is up (*) or down (-).
`p`	Flag indicating whether the interface is permanent. A `P` indicates a permanent interface. A hyphen (-) or a blank indicates that it is not. A permanent interface is an interface configured in the command-line interface and stored in the TAOS unit's NVRAM. All the Ethernet interfaces and the virtual interfaces made for Connection profiles are permanent. Transient interfaces are those the TAOS unit builds from RADIUS, TACACS, or an Answer profile. These interfaces have no interface entry when the connection is down.
`ifname`	Interface name.
`mac addr`	Interface MAC address.
`local-addr`	Interface local address.

Following is an example of disabling an interface:

```
ether-1/4> ifmgr down ie1-4-1
```

The IFMgr `-d` output indicates that the interface is disabled by displaying a hyphen instead of an asterisk in the Up (`u`) column:

```
ether-1/4> ifmgr -d
if  slot:if  u p ifname   mac addr      local-addr
------------------------------------------------
000 0:00:000 *   pb0      000000000000  0.0.0.0/32
001 1:17:011 -   ie1-4-1  00c07b6d23f0  0.0.0.0/32
002 1:17:013 *   ie1-4-2  00c07b6d23f1  11.1.2.1/32
```

```
003 1:17:015 *   ie1-4-3  00c07b6d23f2  11.1.3.1/32
004 1:17:017 *   ie1-4-4  00c07b6d23f3  11.1.4.1/32
005 1:17:019 *   ie1-4-5  00c07b6d23f4  11.1.5.1/32
<end>
```

Note: The Netstat command also displays a hyphen to indicate a disabled Ethernet interface.

To mark an interface as up, use the `up` option:

```
ether-1/4> ifmgr up ie1-4-1
```

An interface can be administratively disabled by using the IFMgr command or by updating the Ethernet profile, or it can be marked as down by the Ethernet driver when Link-State-Enabled is Yes and Link-State is Down. Therefore, using the `Up` option to the IFMgr command does not necessarily enable the interface. However, it does mark the interface as up.

Following is an example of using the IFMgr command on the shelf controller:

```
admin> ifmgr -d
bif slot sif u m p ifname      host-name  remote-addr       local-addr
-------------------------------------------------------------------------------
000 1:17 000 *     ie0         -          0.0.0.0/32        192.168.7.133/32
001 1:17 001 *     lo0         -          0.0.0.0/32        127.0.0.1/32
002 0:00 000 *     rj0         -          0.0.0.0/32        127.0.0.2/32
003 0:00 000 *     bh0         -          0.0.0.0/32        127.0.0.3/32
004 0:00 000 *     wanabe      -          0.0.0.0/32        127.0.0.3/32
005 0:00 000 *     local       -          0.0.0.0/32        127.0.0.1/32
006 0:00 000 *     mcast       -          0.0.0.0/32        224.0.0.0/32
007 0:00 000 -     tunnel7     -          0.0.0.0/32        192.168.7.133/32
008 1:11 001 *   p wan8        apx-t1-t32 200.2.1.2/32      192.168.7.133/32
009 1:11 002 *   p wan9        apx-t1-t32 200.2.2.2/32      192.168.7.133/32
010 1:11 003 *   p wan10       apx-e1-t22 200.3.2.2/32      192.168.7.133/32
011 1:11 004 *   p wan11       apx-e1-t32 200.5.1.2/32      192.168.7.133/32
012 1:11 005 *   p wan12       apx-e1-t32 200.5.2.2/32      192.168.7.133/32
013 1:11 006 *   p wan13       apx-t1-t22 200.1.1.2/32      192.168.7.133/32
014 1:15 001 *   p wan14       apx-t1-s1- 100.1.100.2/32    100.6.100.2/32
015 1:11 007 *   p wan15       apx-e1-t22 200.3.1.2/32      192.168.7.133/32
016 1:11 008 *   p wan16       cisco-t221 200.4.103.2/32    192.168.7.133/32
017 1:11 009 *   p wan17       m-e1-t2211 200.4.4.2/32      192.168.7.133/32
018 1:11 010 *   p wan18       m-e1-t2212 200.4.4.3/32      192.168.7.133/32
019 1:17 000 -   p wan19       m2t81      200.8.1.2/32      192.168.7.133/32
020 1:17 000 -   p wan20       m41        200.4.1.2/32      200.6.1.2/32
021 1:16 001 *   p wan21       p1321n<>p1 0.0.0.0/32        0.0.0.0/32
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

The IFMgr output on cards other than the Ethernet card includes the following fields:

Field	Description
`bin`	Bundle interface number. There is one interface number per bundle, including MPP connections. It is the global interface-table number.
`slot`	Shelf and slot the interface is assigned to.

Field	Description
sif	Slot interface.
u	Flag indicating whether the interface is up (*) or down (-).
m	Indicates that the interface is part of an MP bundle.
p	Flag indicating whether the interface is permanent. A P indicates a permanent interface. A hyphen (-) or a blank indicates that it is not. A permanent interface is an interface that is configured in the command-line interface and stored in the TAOS unit's NVRAM. All the Ethernet interfaces and the interfaces based on Connection profiles are permanent. Transient interfaces are those the TAOS unit builds from RADIUS, TACACS, or an Answer profile. These interfaces have no interface entry when the connection is down.
ifname	Interface name.
host-name	Host name of remote device.
remote-addr	Remote address of device as configured in a Connection profile.
local-addr	Local address of device as configured in a Connection profile.

Following is an example of displaying information about a particular interface:

```
admin> ifmgr -d 009
inUse:          Yes
hostName:       apx-t1-t3212-s4
dialoutName:
ExternalAuth:   No
ExternFilters:  No
ExternRoutes @  0
ExternIpxRoutes @       0
miscInfo @      0
reDirectDest:   0.0.0.0
DLCI routeId:   34
MP(P) id:       0
Logical iff:    2
virtual id: 0, virtual next @ 0, virtual main @ 0
minor device:   9
device status:  0x303
mtu:            1528
ip_addr:        192.168.9.133
dstip_addr:     100.2.1.2
netmask:        255.255.255.0
net:            192.168.9.0
subnet:         192.168.9.133
bcast:          192.168.9.255
nbcast:         192.168.9.133
directed-bcast:         no
macaddr:        000000000000
inp_qcnt:       0
out_qcnt:       0
```

```
nexthop:        0.0.0.0
Num pkts queued for brouter:    0
proxy_arp_mode: 0
proxy_arp_head: 0
No associated connection profile
```

The ICMP-Reply-Directed-Bcast parameter in the IP-Global profile specifies whether the TAOS unit responds to directed-broadcast ICMP echo requests. If set to No, the system does not respond to any directed-broadcast ICMP requests. The setting of this parameter is shown in the Directed-Bcast field in the Ifmgr output.

IPXRIPdebug

Description: Displays incoming and outgoing IPX RIP traffic. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`ipxripdebug`** at the command prompt.

Example:

```
admin> ipxripdebug
IPX-RIP state display is ON
```

The following message appears as the TAOS unit sends an IPX RIP packet announcing its route:

```
IPXRIP: 10000a17 announced 0 routes on interface 1000:
```

Next, a Pipeline 50 has dialed the TAOS unit. The TAOS unit receives a RIP route from the Pipeline.

```
IPXRIP: received response from ac1b0001:00c07b5e04c0 (1 nets).
```

The following message indicates that the TAOS unit is delaying sending a RIP packet to prevent the interpacket arrival time from being shorter than busy/slow boxes can handle. An IPX router should never violate the minimum broadcast delay.

```
IPX-RIP: too soon to send on interface 1000.
IPXRIP: 10000a81 announced 0 routes on interface 1000:
IPXRIP: received response from ac1b0001:00c07b6204c0 (1 nets).
IPXRIP: 10000aa6 announced 0 routes on interface 1000:
IPXRIP: received response from ac1b0001:00c07b5504c0 (1 nets).
IPXRIP: 10000abc announced 0 routes on interface 1000:
```

Lanval

Description: Displays messages related to external validation requests. You can use this command in conjunction with `radif` to troubleshoot authentication issues.

Usage: Enter **`lanval`** at the command prompt.

Example:

```
admin> lanval
LANVAL state display is ON
```

```
LANVAL: radius auth, id B054AD60
LANVAL: radius callback, id B054AD60, auth SUCCESS
LANVAL:_lanvFreeInfo: freeing iprof@B05A9360
```

LifDebug

Description: Displays ISDN layer 2 and layer 3 information. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`lifdebug`** at the command prompt.

Example: Following are several examples of `LifDebug` output:

```
admin> lifdebug
LIF debug is now ON
```

A packet is being sent over the WAN. The packet is constructed:

```
LIF_SendPkt(): DSL 0, source 0x400, destination 0x300,
event 0x340, SAPI 0, CES 1, Call_Id 77, Chan_Id 0
```

The following message displays the contents of the packet:

```
PACKET:
Header (4): a0 50 59 b0  Info (9): 08 02 00 00 84 08 02 80 90 01
L3_Go: source 0x400, event 0x340, DSL 0, call_id 77, ces 1
L3_ProcessUserEvent(): State 0x9, Event 0x84, Index 6,
DSL 0, CallID 77
```

Another packet is sent:

```
LIF_SendPkt(): DSL 0, source 0x300, destination 0x205,
event 0x240, SAPI 0, CES 1, Call_Id 77, Chan_Id 0
PACKET:
Header (4): a0 50 59 b0  Info (9): 08 02 83 fe 45 08 02 80 90 00
L3_Go(): end of L3 task, NLCB State 10
L2_Go(): DSL_Id=0, SAPI=0, CES=1, TEI=0, Event=240
L2_ProcessEvent(): DSL 0, index 13, state 7
L2_ProcessEvent(): DSL 0, index 19, state 7
L2_Go(): DSL_Id=0, SAPI=0, CES=1, TEI=0, Event=1
L2_ProcessEvent(): DSL 0, index 1, state 7
L2_Go() end: DLCB->State 7
```

MdbStr

Description: Modifies the default modem AT command strings used by the modems on the TAOS unit for both incoming and outgoing calls. Previously, you could not modify the AT command for modems on the TAOS unit. You could only affect the string in minor ways by modifying the parameters in the Terminal-Server>Modem-Configuration subprofile. Note that when the modem card or the TAOS unit is reset, the AT command strings revert to their defaults.

The MdbStr command also allows you to return the string to its factory default settings.

The modem chip in the TAOS unit supports AT commands up to 56 characters in length. To fully support all possible functionality, each command is sent as two separate strings. You can modify one or both strings.

Caution: The AT command string initializes the modems it supports. When you change the AT command string, you are changing the functionality of the modems. Use this command with caution.

Here are the two default strings for the TAOS unit:

1 `AT&F0&C1V0W1X4`

2 `AT%C3\N3S2=255S95=44S91=10+MS=11,1,300,33600A`

Usage: `mdbstr [ 0 ] [ 1 ] [ 2 ] [ AT-command-string ]`

Example: The following examples show you how to modify each portion of the AT command string:

To override the existing first string with a new string:

```
mdbstr 1 AT&F0&C1V1W1
```

This will override the second portion of the AT command string:

```
mdbstr 2 AT%C3\N3S2=255S95=44S91=10+MS=11,1,300,14400A
```

This will return both strings to their factory default settings:

```
mdbstr 0
```

MDialout

Description: Displays messages related to modem dial out. This command can be used in conjunction with the ModemDrvState command to get detailed information about outbound modem calls.

The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`mdialout`** at the command prompt.

Example: In the following example, a modem on the TAOS unit prepares to make an outbound modem call, but never receives a dialtone.

```
admin> mdialout
MDIALOUT-2/4: >> CURR state=Await_Off_Hook, NEW
event=Event_Off_Hook
MDIALOUT-2/4: connected to DSP!
MDIALOUT-2/4: rqst tone (14) via channelIndex 0
MDIALOUT-2/4: tone generation started.
MDIALOUT-2/4: >> CURR state=Await_Dial_Tone, NEW
event=Event_Dialtone_On
MDIALOUT-2/4: decode timer started.
MDIALOUT-2/4: << NEW state=Await_1st_Digit
MDIALOUT-2/4: enabling tone search, channel index=0,
timeslot=0
MDIALOUT-2/4: << NEW state=Await_1st_Digit
```

```
MDIALOUT-2/4: >> CURR state=Await_1st_Digit, NEW
event=Event_On_Hook
MDIALOUT-2/4: stopping decode timer.
MDIALOUT-2/4: rqst tone (15) via channelIndex 0
MDIALOUT-2/4: disabling tone search, channel index=0
MDIALOUT-2/4: disconnected from DSP.
MDIALOUT-2/4: << NEW state=Await_Off_Hook
MDIALOUT-2/4: >> CURR state=Await_Off_Hook, NEW
event=Event_Close_Rqst
MDIALOUT-?/?: << NEW state= <DELETED>
```

MDialSess

Description: Displays all the active modem dialout sessions.

Usage: Enter `mdialsess` at the command prompt.

Example:

```
admin> mdialsess
entry slot:mdm route port hookDetect DSP:tone:timr:decode state
1    6:4     145   16 pollForOff  n : n  : n  :  n    Await_Off_Hook
```

ModemD1Stats, ModemD2Stats, ModemD3Stats

Description: Displays modem statistics. ModemD1Stats displays statistics for the first 16 modems, ModemD2Stats displays statistics for the second 16 modems, and ModemD3Stats displays statistics for the last 16 modems.

Usage: `modemd1stats`

To use this command, first open a session with a modem card, then enter the command.

Example:

```
modem-1/2> modemd1stats
modem:  ansFail    ansOK   1-2400 2.4-14.4  14.4-up  21.6+up  28.8+up
 1/ 0:        3      171        0        0     171      171      171
 1/ 1:        3      171        0        0     171      171      171
 1/ 2:        2      172        0        0     172      172      172
 1/ 3:        2      172        0        0     172      172      171
 1/ 4:        4      170        0        0     170      170      170
 1/ 5:        1      173        0        0     173      173      172
 1/ 6:        0      174        0        0     174      174      174
 1/ 7:        1      173        0        0     173      173      173
 1/ 8:        1      173        0        0     173      173      173
 1/ 9:        0      174        0        0     174      174      174
 1/10:        2      172        0        0     172      172      172
 1/11:        1      173        0        0     173      173      173
 1/12:        1      173        0        0     173      173      173
 1/13:        0      174        0        0     174      174      174
 1/14:        1      173        0        0     173      173      173
```

```
 1/15:        3      171        0        0     171      171      170
```

ModemDrvDump

Description: Displays information about the status of each modem.

Usage: Enter **`modemdrvdump`** at the command prompt.

Example: Following is a message about modem 0 (the first modem) in the modem card in slot 3 on the TAOS unit. The numbers in brackets indicate number of calls with unexpected open requests, unexpected Rcode events, unexpected release events, and unexpected timeouts:

```
MODEMDRV-3/0: Unexp Open/Rcode/Rlsd/TimOut=[0,0,0,0]
```

ModemDrvState

Description: Displays communication to and from the modem driver on the TAOS unit. You can see which buffers are allocated and which AT command strings are being used to establish modem connections.

You can also determine whether data is received from the modem in an understandable format. If line quality is poor, the modem driver attempts to parse incoming data from the modem, but it might not be successful. This command can be used in conjunction with the MDialout command to get detailed information about outbound modem calls.

The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`modemdrvstate`** at the command prompt.

Example: Following are examples of a modem call coming into the TAOS unit, and a modem call being cleared from the TAOS unit:

```
admin> modemdrvstate
MODEMDRV debug display is ON
```

Modem 1 on the modem card in slot 3 has been assigned to answer an incoming modem call:

```
MODEMDRV-3/1: modemOpen modemHandle B04E3898, hdlcHandle B026809C,
orig 0
```

The modem is idle, so it is available to answer the call:

```
MODEMDRV-3/1: _processOpen/IDLE
```

The next two lines show the TAOS unit's modem sending the first string:

```
MODEMDRV: Answer String, Part 1 - AT&F0E0+A8E=,,,0
```

A buffer needs to be allocated for sending the command out to the WAN:

```
MODEMDRV-3/1: _hdlcBufSentFnc: buffer = 2E12EAE0, status = SENT
```

Buffers are allocated for data being received from the WAN:

```
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13ADF0, len=8,
parseState[n,v]=[0,0], status= RCVD
```

```
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13BA20, len=5,
parseState[n,v]=[0,0], status= RCVD
```

The TAOS unit's modem receives an OK from the calling modem:

```
MODEMDRV-3/1: data =OK
```

The process is repeated for strings 2 and 3:

```
MODEMDRV-3/1: processTimeout/DIAL_STR2[2D]
MODEMDRV: Answer String, Part 2 - AT&C1V1\V1W1X4S10=60
MODEMDRV-3/1: _hdlcBufSentFnc: buffer = 2E12EAE0, status = SENT
MODEMDRV-3/1: _hdlcBufRcvdFnc: data=2E13C038, len=2,
parseState[n,v]=[0,0], status= RCVD
MODEMDRV-3/1: data = 0
MODEMDRV-3/1: _processTimeout/DIAL_STR3
MODEMDRV: Answer String, Part 3 -
AT%C3\N3S2=255S95=44S91=10+MS=11,1,300,33600,A
```

Now result codes are processed to clarify the characteristics of the connection.

```
MODEMDRV-1/1: _hdlcBufRcvdFnc: data=9880C628, len=48,
parseState[n,v]=[1,0], stD
MODEMDRV-1/1: data =
CONNECT 115200/V34/LAPM/V42BIS/28800:TX/33600:
MODEMDRV-1/1: decodeSLC[15]=<CONNECT 115200/> checking for error
correction
MODEMDRV-1/1: decodeSLC[4]=<V34/> checking for error correction
MODEMDRV-1/1: decodeSLC[5]=<LAPM/> checking for error correction[29]
MODEMDRV-1/1: decodeSLC[7]=<V42BIS/> checking for compression[21]
MODEMDRV-1/1: decodeSLC[9]=<28800:TX/> checking for xmit[1]
MODEMDRV-1/1: _hdlcBufRcvdFnc: data=9880C828, len=4,
parseState[n,v]=[4,0], staD
MODEMDRV-1/1: data = RX
> checking for recv[0]C[9]=<33600:RX
decodeSLC complete
```

At this point the modem call is up, and the modem driver has completed its tasks. The call will be passed to Ethernet resources:

```
MODEMDRV-3/1: _processRcodeEvent/AWAITING RLSD, mType=5, RLSD=0
MODEMDRV-3/1: _processRlsdChange/AWAITING RLSD = 1
```

Following is the normal sequence of steps for a modem call that is cleared (by either modem). Modem 5 on the modem card in slot 7 of the TAOS unit is freed from the previous call, and it is reinitialized (so it is available for the next call).

```
MODEMDRV-7/5: modemClose modemHandle B04E6F38
MODEMDRV-7/5: _closeConnection:ONLINE, event=3
MODEMDRV-7/5: _processTimeout/INIT
```

MPCMtoggle

Description: Displays information about related channel addition with Multilink Point-to-Point connections. This information is not related to MP+ or BACP connections. This

command displays only information from connections established as MP (RFC1717) connections.

The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`mpcmtoggle`** at the command prompt.

Example:

```
admin> mpcmtoggle
MPCM debug is now ON
MPCM-432: adding 1 channels
```

MPentry

Description: Displays information for a specified, active, MP or MP+ connection, including the options negotiated in the connection. This command can be extremely helpful when researching MP or MP+ compatibility issues.

Note: The MpID number that must be entered is an internally generated number. To get a list of all currently assigned MpID numbers on your TAOS unit, enter the `IFmgr -d` command and specify an interface name or number.

Usage: Enter **`mpentry`** at the command prompt.

Example: The following example shows an MP+ call (noted as MPP). The End Point Discriminator (used to bundle the channels together) is shown under `bundle id`. In this case, it is the hardware MAC address of the calling device.

```
admin> mpentry
MpID required
admin> mpentry 28
MP entry 28 @ B055DE60
MpID  28, Flags: delete No, remote No, ncp Yes, mpp Yes bacp No
bundle id: 15 octets @ B0558BE0
[0000]: 03 00 C0 7B 53 97 07 73 65 63 61 2D 68 73 76
vjInfo @ B0562060
startTime 227521989, mrru: local 1524, peer 1524
send: ifIx 1, count 0, seq 77268 / recv: seq 75046
IF 50, send idle 0, recv idle 1, last seq 75045 mode 0 #chans 1
Head:
Tail
Reassembe packet cnt 0 bad lrg pkts 0
```

MPPCM

Description: Displays MP+ call-management information. The command is a toggle that alternately enables and disables the debug display. You can use it in conjunction with the MPtoggle command, since each command logs debug from a different place in code, but both display information based on multichannel connections.

Usage: Enter **`mppcm`** at the command prompt.

Example:

```
admin> mppcm
MPPCM debug is now ON
```

The following 8 messages indicate that a second channel is added to a 1-channel MP+ connection:

```
MPP-5: Event = Utilization, CurrentState = Idle/A
MPP-5: check dynamic says: current = 1, recommended = 2
MPP-5: requesting 1 additional channel(s)
MPP-5: 1 call(s) posssible.
MPP-5: new state is: Add/C
MPP-5: Event = RxAddComplete, CurrentState = Add/C
MPP-5: enterIdleA, AddLock = Yes, RemoveLock = No
MPP-5: new state is: Idle/A
```

The following 12 messages indicate that a remote management session is brought up for the MP+ user with MpID 28. You can open a remote session to an MP+ user from the terminal server.

```
MPP-28: Event = StartRM, CurrentState = Idle/A
MPP-28: start remote management
MPP-28: new state is: Idle/A
MPP-28: Event = RxRmRsp, CurrentState = Idle/A
MPP-28: remote management response (0)
MPP-28: new state is: Idle/A
MPP-28: Event = RxRmTxReq, CurrentState = Idle/A
MPP-28: new state is: Idle/A
MPP-28: Event = RecvRMM, CurrentState = Idle/A
MPP-28: new state is: Idle/A
MPP-28: Event = StopRM, CurrentState = Idle/A
MPP-28: stop remote management

admin> mppcm
MPPCM debug is now OFF
```

MPtoggle

Description: Displays information about MP and MP+ connections. You can use this command in conjunction with the MPPCM command, since each command logs debug from a different place in code, but both display information based on multichannel connections. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`mptoggle`** at the command prompt.

Example:

```
admin> mptoggle
MP debug is now ON
MP-26: sending control message 191
MP-5: sending control message 76

admin> mptoggle
MP debug is now OFF
```

NetIF

Description: Displays the TAOS unit's network interface mappings.

Usage: **`netif -m -q -t -v -?`**

Syntax element	Description
`-m`	Display mappings for the specified map type.
`-q`	Display the queue for a map.
`-t`	Toggle debug display.
`-v`	Display valid mapping tables.
`-?`	Display this summary.

Example:

```
admin> netif -v
map 0x1042C0E0: type 0 (call-id), id 0x1042B5A0


admin> netif -m 0
SHELF  SLOT  SysID      SlotID
   1         1      52      2
   1         6      90     58
   1         6      89     57
   1         6      86     56
   1         6      78     51
   1         6      72     50
   1         6      71     49
   1         6      70     48
   1         6      69     47
   1         6      68     46
   1         6      62     45
   1         6      61     44
   .
   .
```

PermConn-List

Description: Displays a list of all permanent connection profiles in the TAOS unit.

Usage: Enter **`permconn-list`** at the command prompt.

Pools

Description: Displays a snapshot of a large selection of memory pools, the size of each pool, and the status of each pool. At the end of the list is a summary of the total memory allocation in the TAOS unit.

Memory is dynamically allocated to support various tasks, and should be freed when a particular task has been completed. Taking pools snapshots over an extended period of time can help troubleshoot a problem with a memory leak, in which memory is allocated for a task but never freed.

Snapshots should never show the entire quantity of allocated memory (or even any single pool) increasing over an extended period of time.

Usage: Enter **pools** at the command prompt.

Example: The number of pools displayed is usually very large. The following example displays just a portion of the typical output.

```
admin> pools
Pool Name                          size  limit  inUse  hiWat  heapAdrs
Accounting Session Change Registrants      8     0       1      1
103CCAE0
AcctEvnt                            14     0     127    127   103CCAE0
AfsHashEntry                       191     0       0      0   103CCBE0
AfsTaskMsg                         219     0       0      0   103CCBE0
AssignedChannelPool                 32     0     127    139   103CCAE0
AuthData                           116     0       0      0   103CCBE0
BrouterPool                         80     0       2     14   103CCB60
.
.
.
volatile profile instance           16     0     171    184   103CCAE0
volatile profile type info          12     0       7      7   103CCAE0
```

The first portion of the Pools command output includes the following fields:

Field	Description
Pool name	Pool name.
Size	Size of the pool, in kilobytes.
Limit	Maximum number of buffers that can be allocated to a pool.
InUse	Number of pools in use.
HiWat	Highest number of pools allocated to a task since the TAOS unit was brought up.
HeapAdrs	Memory address of pool.

Following the list of pools, the Pools command displays a summary of memory usage:

```
                 total pools:          175
          total buffers in use:        10593
                total memalloc:       261685
                 total memfree:       258558
              memalloc in use:         3129
             memalloc failures:            0
              memfree failures:            0
            memalloc high water:         3146

Histogram of memalloc'd memory block sizes:
    2659 buffers in range [64,127]
    632 buffers in range [128,255]
```

```
    2 buffers in range [256,511]
    22 buffers in range [512,1023]
    9 buffers in range [1024,2047]
    21 buffers in range [2048,4095]
    3 buffers in range [4096,8191]
    7 buffers in range [8192,16383]
    6 buffers in range [32768,65535]
    2 buffers in range [131072,262143]
    1 buffers in range [262144,524287]
Total memory in use: 1295104 bytes in 3364 buffers
Histogram of free memory block sizes:
    12 buffers in range [128,255]
    1 buffers in range [256,511]
    2 buffers in range [1024,2047]
    1 buffers in range [1048576,2097151]
Total free memory: 1503680 bytes in 16 buffers
```

Following are descriptions of some of the more important fields in this display:

Field	Description
`total pools`	Total number of pools in use.
`total buffers in use`	Number of buffers in use.
`total memalloc`	Total number of times the TAOS unit allocated a block of memory for use.
`total memfree`	Total number of times the TAOS unit freed a block of memory. This should be fairly close to total memalloc.
`memalloc in use`	Total number of memory pools in use. This is the difference between total allocated and total freed.
`memalloc failures`	Total number of times the TAOS unit failed to allocate a block of memory for use.
`memfree failures`	Total number of times the TAOS unit failed to free a block of memory.
`memalloc high water`	The highest number of memory pools in use at any one time.

PortInfo

Description: Displays information about the TAOS unit's ports.

Usage: **`portinfo port-number`**

Example:

```
admin> portinfo 1
Printing fixed/allocated ports for slot 1
Linear Port:   1
- fixed:       TRUE
- relative #:  0
```

```
- paired port: 65535
- slave:       FALSE
- physical:    FALSE
```

PPPdump

Description: Very similar to the WANdisplay diagnostic command. But the PPPdump command strips out escape characters that are present for asynchronous PPP users (who are dialing in with modems). The escape characters are necessary because of the asynchronous nature of the data stream. Stripping them out simply clarifies the presentation of the data.

If you enter the command while traffic streams heavily through your TAOS unit, the resulting amount of output can make it tedious to find the information you're looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen.

You might prefer to use the PPPdump command during a period of low throughput.

Usage: First open a session with a host card, then enter `pppdump` *n*

where **n** is the number of octets to display per frame. Specifying a value of 0 (zero) disables the logging of this data.

Example: Following are two examples of the display of an asynchronous call, one produced by WANdisplay and the other by PPPdump.

The following frames were logged by entering **`wandisplay 64`**:

```
7E FF 7D 23 C0 21 7D 21 7D 21 7D 20 7D 37 7D 22 7D 26 7D 20 7D 2A 7D
20 7D 20 2D 7D 23 7D 26 3A AA 7E
7E FF 7D 23 C0 21 7D 21 7D 21 7D 20 23 7D 20 7D 24 7D 20 7D 20 7D 22
7D 7E
```

To get the data stream without escape characters, the 0x7D bytes need to be stripped, and the byte following each 0x7D byte needs to be decremented by 0x20.

With PPP dump, the data is automatically converted and displayed:

```
7E FF 03 C0 21 01 01 00 17 02 06 00 0A 00 00 2D 03 06 3A AA 7E 7E
FF 03 C0 21 01 01 00 23 00 24 00 00 02 7E
```

See Also: WANdisplay, WANnext, WANopen

PPPFSM

Description: Displays changes to the PPP state machine as PPP users connect. The command is a toggle that alternately enables and disables the debug display.

Usage: First open a session with a host card, then enter **`pppfsm`** at the command prompt.

Example: The following display shows the complete establishment of a PPP session:

```
admin> pppfsm
PPPFSM state display is ON
PPPFSM-97: Layer 0   State INITIAL     Event OPEN...
```

```
PPPFSM-97: ...New State STARTING
PPPFSM-97: Layer 0   State STARTING    Event UP...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 1   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 2   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 3   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 4   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 5   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 6   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 7   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 8   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 9   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 0   State REQSENT     Event RCONFREJ...
PPPFSM: irc_new scr 4
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 0   State REQSENT     Event RCONFACK...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 0   State ACKRECD     Event RCONFREQ...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 0   State ACKRECD     Event RCONFREQ...
PPPFSM-97: Layer 1   State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: ...New State OPENED
PPPFSM: PAP Packet
PPPFSM-97: Layer 6   State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 4   State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 4   State REQSENT     Event RCONFREQ...
PPPFSM-97: ...New State REQSENT
PPPFSM: ccp Packet code 1
PPPFSM-97: Layer 6   State REQSENT     Event RCONFREQ...
PPPFSM-97: ...New State REQSENT
PPPFSM: ccp Packet code 2
PPPFSM-97: Layer 6   State REQSENT     Event RCONFACK...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 4   State REQSENT     Event RCONFACK...
PPPFSM-97: ...New State ACKRECD
```

PPPinfo

Description: Displays information about established PPP sessions. The command has little practical use other than as a tool for developmental engineering.

Usage: **`pppinfo`** ***`index`*** **`[ all ]`**

Syntax element	Description
`index`	Selects a particular PPP information table.
`all`	Displays information about embedded structures.

Example:

```
admin> pppinfo 1
Ncp[LCP]        = B02B396C
Ncp[AUTH]       = B02B39BC
Ncp[CHAP]       = B02B3A0C
Ncp[LQM]        = B02B3A5C
Ncp[IPNCP]      = B02B3AAC
Ncp[BNCP]       = B02B3AFC
Ncp[CCP]        = B02B3B4C
Ncp[IPXNCP]     = B02B3B9C
Ncp[ATNCP]      = B02B3BEC
Ncp[UNKNOWN]    = B02B3C3C
Mode            = async
nOpen pending   = 0
LocalAsyncMap   = 0
RemoteAsyncMap  = 0
Peer Name       = N/A
Rmt Auth State  = RMT_NONE
aibuf           = 0
ipcp            = B03E502C
vJinfo          = 0
localVjInfo     = 0
bncpInfo        = B03E559C
ipxInfo         = B03E55DC
remote          = no
Bad FCS         = a
```

PPPstate

Description: Displays the state of a PPP connection. Different PPP calls can be routed (call routing, as opposed to IP or IPX routing) through a TAOS unit differently. The command is a toggle that alternately enables and disables the debug display.

The command has little practical use other than as a tool for developmental engineering.

Usage: Enter **`pppstate`** at the command prompt.

Example: The following message indicates that data is moved directly from the WAN to the Ethernet segment. WAN data can be redirected to other resources (X.75 handler or V.120 handler) before it is ready to be sent to the Ethernet segment.

```
PPP-116: Redirect async wan direct
```

PRIdisplay

Description: Displays all ISDN PRI D-channel signaling packets that are either received or sent through the PRI interfaces.

Usage: To use this command, first open a session with a network card configured for PRI signaling (for example, a T1 or E1 card). Then enter the PRIdisplay command. The command uses the following syntax:

`pridisplay number-of-octets-to-display line`

Syntax element	Description
`number-of-octets-to-display`	Specifies the number of octets in the PRI messages to display. Specify 0 (zero) to disable the display.
`line`	The PRI line to display. Specify 0 (zero) to display any line.

Example:

```
e1-1/15> pridisplay 128 0
Display the first 128 bytes of PRI messages
e1-1/15> PRI-XMIT-7: 10:37:00: 4 of 4 octets
800F1020: 00 01 01 73                                          ...s
PRI-RCV-7: 10:37:00: 4 of 4 octets
800F3CA0: 00 01 01 73                                          ...s
PRI-XMIT-7: 10:37:10: 4 of 4 octets
800F1020: 00 01 01 73                                          ...s
PRI-RCV-7: 10:37:10: 4 of 4 octets
800F3CA0: 00 01 01 73                                          ...s
PRI-XMIT-7: 10:37:20: 4 of 4 octets
800F1020: 00 01 01 73                                          ...s
PRI-RCV-7: 10:37:20: 4 of 4 octets
800F3CA0: 00 01 01 73                                          ...s
PRI-XMIT-7: 10:37:30: 4 of 4 octets
800F38E0: 00 01 01 73                                          ...s
PRI-RCV-7: 10:37:30: 4 of 4 octets
800F3CE0: 00 01 01 73                                          ...s
pridisplay 0
PRI message display terminated
```

RADacct

Description: Displays RADIUS accounting information. The RADacct command displays very few messages if RADIUS Accounting is functioning correctly.(`RADif` displays more detailed information for troubleshooting RADIUS-related issues.) The RADacct command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`radacct`** at the command prompt.

Example:

```
admin> radacct
RADACCT debug display is ON
```

A user hangs up and a stop record is generated.

```
RADACCT-147:stopRadAcct
```

The following message indicates that there is some load on the network, and the sending of a stop record is delayed. This is not necessarily an indication of a problem.

```
RADACCT-147:_endRadAcct: STOP was delayed
```

RADif

Description: Displays RADIUS-related messages. RADif is a powerful diagnostic command, because it displays RADIUS messages the TAOS unit receives as well as messages that it sends. Output from `RADif`, in conjunction with running your RADIUS daemon in debug mode (using the `-x` option), gives you virtually all the information you need to clarify issues relating to user authentication.

You can also validate the IP port that you have configured (or think you have configured), and the user name that is being sent by the client.

The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`radif`** at the command prompt.

Example: Following are messages you might see for a successful RADIUS authentication:

```
RADIF: authenticating <8:my_name> with PAP
RADIF: _radiusRequest: id 41, user name <9:my_name>
RADIF: _radiusRequest: challenge len = <0>
```

The IP address and RADIUS Daemon Authentication port are displayed:

```
RADIF: _radiusRequest: socket 5 len 89 ipaddr 01010101 port
65534->1645
RADIF: _radCallback
RADIF: _radCallback, buf = B05BBFA0
```

The response is sent back from RADIUS. In this case, the user `my_name` has passed authentication. Following is a list of the most common responses:

```
1 - Authentication Request
2 - Positive acknowledgement
3 - Rejection
4 - Accounting request
5 - Accounting response
7 - Password change request
8 - Password change positive acknowledgement
9 - Password change rejection
11 - Access challenge
29 - Password - next code
30 - Password New PIN
31 - Password Terminate Session
32 - Password Expired
RADIF: _radCallback, authcode = 2
RADIF: Authentication Ack
```

After, authenticating a user, the RADIUS daemon sends the attributes from the user profile to the TAOS unit. The TAOS unit creates the user's Connection profile from these attributes, and RADif displays them. (See the *TAOS RADIUS Guide and Reference* for a complete list of attribute numbers.)

```
RADIF: attribute 6, len 6, 00 00 00 02
RADIF: attribute 7, len 6, 00 00 00 01
RADIF: attribute 8, len 6, ff ff ff fe
RADIF: attribute 9, len 6, ff ff ff 00
RADIF: attribute 11, len 12, 73 74 64 2e
RADIF: attribute 12, len 6, 00 00 05 dc
RADIF: attribute 10, len 6, 00 00 00 00
RADIF: attribute 13, len 6, 00 00 00 01
RADIF: attribute 244, len 6, 00 00 11 94
RADIF: attribute 169, len 6, 00 00 11 94
RADIF: attribute 170, len 6, 00 00 00 02
RADIF: attribute 245, len 6, 00 00 00 00
RADIF: attribute 235, len 6, 00 00 00 01
```

A RADIUS Accounting Start packet is sent to the RADIUS Accounting Server (using port 1646):

```
RADIF: _radiusAcctRequest: id 42, user name <9:my_name>
RADIF: _radiusAcctRequest: socket 6 len 82 IP cf9e400b port 1646,
ID=42
RADIF: _radCallback
RADIF: _radCallback, buf = B05433C0
RADIF: _radProcAcctRsp: user:<9:my_name>, ID=42
```

RADservdump

Description: Use this command to verify the configuration you have set in the External-Auth profile.

Usage: Enter **`radservdump`** at the command prompt.

This does not display any information related to the configuration of either your RADIUS Authentication server or your RADIUS Accounting server.

Example: For the following example, the TAOS unit has been configured with two RADIUS servers, 1.1.1.1 and 2.2.2.2. The port has not been changed from its default of 1700.

```
admin> radservdump
Rad serv vars: port=1700,sockId=8
 0) clients=1010101
 1) clients=2020202
 2) clients=0
 3) clients=0
 4) clients=0
 5) clients=0
 6) clients=0
 7) clients=0
 8) clients=0
```

RADsessdump

Description: Displays the state of all RADIUS Accounting sessions.

Usage: Enter **radsessdump** at the command prompt.

Example:

```
admin> radsessdump
RadActSess:  state route sessID   nasPort authM  evTime
             loadd 00289 252365175 012032 local  523932
             loadd 00288 252365174 012032 local  523946
             loadd 00287 252365173 012032 local  523945
             loadd 00286 252365172 012032 local  523946
             loadd 00227 252355493 012032 local  370610
             loadd 00226 252355492 012032 local  370611
             loadd 00225 252355491 012032 local  370608
             loadd 00224 252355490 012032 local  370609
             loadd 00004 252332182 012032 none   29
             loadd 00003 252332181 012032 none   28
             loadd 00002 252332180 012032 none   27
             loadd 00001 252332179 012032 none   26
```

The RADsessdump command displays the following information:

Column Name:	Description
Route	Internal route ID.
SessID	Session ID. This depends on the route ID.
NASPort	Statistics about the call. The first two digits indicate the type of call: 1 indicates a digital call, 2 indicates an analog call. The next two digits indicate the line on which the call was received. The last two digits indicate the channel on which the call was received.
authM	Method of authentication.
evTime	Event time. This is a time stamp.

RADstats

Description: Displays a compilation of RADIUS Authentication and Accounting statistics.

Usage: Enter radstats at the command prompt.

Example:

```
admin> radstats
RADIUS authen stats:
```

In the following message, A denotes *Authentication*. O denotes *Other*. There were 612 Authentication requests sent and 612 Authentication responses received:

```
0  sent[A,O]=[612,15], rcv[A,O]=[612,8]
```

602 were authenticated successfully, and 18 were not:

```
timout[A,O]=[0,6], unexp=0, bad=18, authOK=602
```

In the next message, the IP address of the RADIUS server is 1.1.1.1, and the `curServerFlag` indicates whether or not this RADIUS server is the current authentication server. (You can have several configured RADIUS servers, but only one is current at any one time.) `0` indicates *no*. `1` indicates *yes*.

```
IpAddress 1.1.1.1, curServerFlag 1
RADIUS accounting stats:
```

The next message indicates that the TAOS unit sent 1557 Accounting packets and received 1555 responses (`ACKs` from the Accounting server). Therefore, the `unexp` value is `2`. This is not necessarily an indication of a problem, but might be the result of the TAOS unit timing out a particular session before receiving an `ACK` from the RADIUS server. Momentary traffic load might cause this condition. The value of `bad` is the number of packets that were formatted incorrectly by either the TAOS unit or the RADIUS server.

```
0  sent=1557, rcv=1555, timout=0, unexp=2, bad=0
```

In the next message, note that the Accounting server is different from the Authentication server. The Accounting and Authentication servers do not need to be running on the same host, although they can be.

```
IpAddress 2.2.2.2, curServerFlag 1
Local Rad Acct Stats:
```

The next two messages can be used to look for traffic congestion problems or badly formatted Accounting packets. Under typical conditions, you might see a few packets whose acknowledgments fail.

The following message indicates whether any RADIUS requests have been dropped by the TAOS unit. With this particular message, no requests were dropped. 1557 were sent successfully.

```
nSent[OK,fail]=[1557,0], nRcv=1557, nDrop[QFull,Other]=[0,0]
```

The following message indicates whether any session timeouts resulted from failure to receive RADIUS responses. The message also indicates responses that are received by the TAOS unit but do not match any expected responses. The TAOS unit keeps a list of sent requests, and expects a response for each request. In the following message, one response was received from the RADIUS server that did not match any of the requests that the TAOS unit had sent out. This might be caused by a corrupted response packet, or by the TAOS unit timing out the session before the response was received.

```
nRsp[TimOut,NoMatch]=[0,1], nBackoff[new,norsp]=[0,0]
```

The following messages display a summarized list of RADIUS server statistics.

```
Local Rad Serv Stats:
unkClient=0
index 0 #Sent = 0, #SendFail=0 badAuthRcv = 0, badPktRcv = 0
```

Reset

Description: This command resets the TAOS unit. When you reset the unit, it restarts and all active connections are terminated. All users are logged out and the default security level is

reactivated. In addition, any active WAN lines are temporarily shut down due to loss of signaling or framing information. After a reset, the TAOS unit runs POST (power-on self-tests).

Usage: **`reset`**

Example: To reset the unit:

```
admin> reset
```

See Also: NVRAM

Resrcmgr

Description: Displays the information from the TAOS unit's shelf controller.

Usage: Enter **`resrcmgr`** at the command prompt.

Example: The following syntax is supported.

```
admin> ? resrcmgr
usage: resrcmgr -i|u|?
        -i  list resource (i)tem information
        -u  list resource (u)sage information
        -?  display this summary
```

Revision

Description: Displays the serial number of the box.

Usage: Enter **`revision`** at the command prompt.

Example: In the following message, `7172461` is the serial number of the TAOS unit.

```
admin> revision
revision = 0 1 10 7172461
```

RoutMgr

Description: Displays information about the routing of incoming calls to either the Ethernet or modem ports. RoutMgr, when used in conjunction with Networki, can show valuable call routing information. If you have problems with users not connecting, and the incoming calls disconnect within one or two seconds of being presented to the TAOS unit , use RoutMgr and Networki to look for possible clues.

The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`routmgr`** at the command prompt.

Example:

```
admin> routmgr
ROUTMGR debug is now ON
ROUTMGR: buildIncomingRoute, port 0, phone <4990>
ROUTMGR: routMgrTask routeID=106, port=0, phone=4990
ROUTMGR-106: _matchPhoneNumber
```

There are no port limitations configured in the T1 profile:

```
ROUTMGR-106: _matchAnyPort
```

The next two messages show that the Bearer Capability in the ISDN setup message for the call indicates that it is a *voice* call, and that the call is routed to an available modem:

```
ROUTMGR-106: voice call
ROUTMGR: giving call to lan/hostif
```

At this point, the call is passed to other TAOS unit functions to continue the connection setup.

Following is output from RoutMgr when a call is cleared.

```
ROUTMGR: destroyRoute routeID = 106, cause = CLEAR
ROUTMGR-106: port is 59
ROUTMGR: deallocateCapabilityrouteID=106, capability=ALL
ROUTMGR: route 106 destroyed
```

SNTP

Description: Displays messages related to the Simple Network Time Protocol (SNTP) functionality of the TAOS unit. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`sntp`** at the command prompt.

Example: Following are three examples of messages displayed with SNTP enabled.

The TAOS unit accepts time from a configured NTP server. The following message appears if the TAOS unit does not accept a supplied time:

```
Reject:li= x stratum= y tx= z
```

The following message indicates that the TAOS unit accepts the time from a specified NTP server:

```
Server= 0 Time is b6dd82ed d94128e
```

Because the stored time is off by more than one second, it is adjusted:

```
SNTP: x Diff1= y Diff2= z
```

StackLimit

Description: If any TAOS unit function uses all but 128 or fewer of the bytes available for the stack, this command enables a checking routine that logs a warning to the Fatal-History log. The command is a toggle that alternately enables and disables the debug display.

Description: This command will enable a checking routine that will log a warning to the Fatal-History log whenever any TAOS unit's function usage gets within 128 bytes from the end of the stack. The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`stacklimit`** at the command prompt.

TDM

Description: Used to set up or query the TDM bus.

Usage: **`tdm [-option ] [ itemA itemB ][ connectionId ]`**

where ***`-option`*** is one of the following:

Option	Description
`-a`	Allocate by first available. (Used when setting up a TDM connection to test).
`-c`	Connect channels.
`-d`	Disconnect a channel.
`-f`	
`-r`	Allocate a TDM channel by round robin.
`-s`	Display TDM manager statistics.
`-l`	List all connections.
`-t`	Toggle TDM manager debug output.
`-u`	Display TDM channel usage statistics.
`-?`	Display this summary.

The other syntax elements are:

Element	Description
`-x` *`number`*	Set the next TDM channel to check.
`itemA`	Logical address to connect from.
`itemB`	Logical address to connect to.
`connectionID`	ID of connection to disconnect.

Example: Following are some examples of output from the TDM command.

```
admin> tdm -l
--id-- --cstate-- cnt  tdm#  ---src(A)---  ---dst(B)---
     1 connected    8    32  01:02:04/001  01:11:01/001
                        33  01:02:04/002  01:11:01/002
                        34  01:02:04/003  01:11:01/003
                        35  01:02:04/004  01:11:01/004
                        36  01:02:04/005  01:11:01/005
                        37  01:02:04/006  01:11:01/006
                        38  01:02:04/007  01:11:01/007
                        39  01:02:04/008  01:11:01/008
     2 connected   24    40  01:02:06/001  01:11:01/009
                        41  01:02:06/002  01:11:01/010
                        42  01:02:06/003  01:11:01/011
                        43  01:02:06/004  01:11:01/012
```

```
admin> tdm -s
        Number of total connections: 9
        Number of active connections: 9
        Number of available channels: 839
        Number of used channels: 185
        Number of disconnection errors: 0
        Number of bad received messages: 0
        Number of invalid events: 0
        Number of missing connections: 0
        Number of bad events: 0
        Number of bad states: 0

admin> tdm -u
(non-empty entries ONLY)
  timslot    nUsed  --currSrc--- --currDst---
       32        1  01:02:04/001 01:11:01/001
       33        1  01:02:04/001 01:11:01/001
       34        1  01:02:04/001 01:11:01/001
       35        1  01:02:04/001 01:11:01/001
       36        1  01:02:04/001 01:11:01/001
       37        1  01:02:04/001 01:11:01/001
       38        1  01:02:04/001 01:11:01/001
       39        1  01:02:04/001 01:11:01/001
       40        1  01:02:06/001 01:11:01/009
```

TDMtst

Description: TDMtst runs on the HDLC card and tests the TDM bus. You can use it to verify communication between HDLC cards. Because the command tests byte-stream communication on the TDM bus, which must use a known time slot, it requires some setup before it can verify TDM traffic.

Usage: **`tdmtst`** *-option*

where ***`-option`*** is one of the following:

Option	Description
`-o` *`channel physical-address logical-address`*	Open a TDM channel between the physical address and the logical address.
`-c channel`	Close the TDM channel.
`-e` *`channel count size`*	Send packets across the TDM bus on the open channel.
`-b` *`channel count size`*	Send packets across the TDM bus on the open channel.
`-x` *`channel string`*	Send the specified string over the TDM channel.
`-s`	Display the TDM test statistics.

Option	Description
`-t`	Toggle debug level.

TelnetDebug

Description: Displays messages as Telnet connections are attempted or established. The Telnet protocol negotiates several options as sessions are established, and TelnetDebug displays the Telnet option negotiations.

The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`telnetdebug`** at the command prompt.

Example: The following session shows a successful Telnet connection from the TAOS unit's terminal server to another UNIX host.

```
admin> telnetdebug
TELNET debug is now ON
```

The far-end UNIX host has been contacted:

```
TELNET-4: TCP connect
```

For this Telnet session, the TAOS unit will support options 24 and 1. The UNIX host should respond with either `DO` or `WONT`:

```
TELNET-4: send WILL 24
TELNET-4: recv WILL 1
```

The UNIX host will support option 1:

```
TELNET-4: repl DO 1
```

The TAOS unit receives a request to support option 3:

```
TELNET-4: recv WILL 3
```

The TAOS unit will support option 3:

```
TELNET-4: repl DO 3
```

The UNIX host will support option 3:

```
TELNET-4: recv DO 3
```

The UNIX host will not support option 24:

```
TELNET-4: recv DONT 24
```

The TAOS unit will not support option 24:

```
TELNET-4: repl WONT 24
```

The UNIX host will support options 1 and 3:

```
TELNET-4: recv WILL 1
TELNET-4: recv WILL 3
```

TNTMP

Description: Displays information about MP and MP+ bundles and their channels. You can execute the TNTMP command on a shelf controller or on an HDLC card. You must first execute the Open command to open a session with the card.

Permission level: Debug

Usage: **`tntmp -i`**

Example: To display information about MP and MP+ bundles and their channels:

```
admin> tntmp -i
mpBundleID=13 masterSlot=1/15 masterMpID=2 ifCount=2 rtIf=1/17:6
           routeID     slot    ifNum localIfNum  localMpID
                32     1/15        1          1          2
                33     9/ 2      193          1          2
```

This command works on HDLC cards as well. First, open a session with HDLC card, and then execute the TNTMP command. For example:

```
admin> open 1 15
```

```
hdlc-1/15> tntmp -i
mpBundleID=13 masterSlot=1/15 masterMpID=2 ifCount=2 rtIf=1/17:6
           routeID     slot    ifNum localIfNum  localMpID
                32     1/15        1          1          2
                33     9/ 2      193          1          2
```

In this example, the output shows a two-channel MP or MP+ bundle, with the first channel in slot 1/15 and the second (slave) channel in slot 9/2.

The command displays the following information:

Field	Description
`mpBundleID`	The globally known bundle ID for the whole system. If the connection adds channels for additional bandwidth on demand, the call for those channels is compared to the current bundle and assigned the same bundle ID as the other channels of the call.
`masterSlot`	The channel that was established as the base channel of the connection. After the TAOS unit authenticates a call that is not part of an existing bundle, it establishes the base channel of the connection. That channel becomes the *master* of the multilink connection.
`masterMpID`	The bundle ID at the master slot card. (The masterMpID is always the same as the localMpID for channels on the master slot card.)
`ifCount`	The number of channels in the bundle.
`rtIf`	The shelf/slot:id for the Route Logical Interface.
`routeID`	The globally known ID for each call.
`slot`	The shelf/slot numbers of the channels in the MP or MP+ bundle.
`ifnum`	Channel number on the master slot card.

Field	Description
`localIfNum`	The channel number on the local slot card. For HDLC cards, the channels are numbered 1–192. In the output in the example, the master slot (1/15) shows channel number 1. The interface number for the slave slot (9/2) is also 1, meaning the first channel on that card. However, at the master slot card, the slave interface number is mapped to a pseudo-interface number greater than 192, so it is not confused with channels on the master slot.
`localMpID`	The bundle ID known locally to the slot card.

TSshow

Description: Displays uptime and revision information about the TAOS unit. The Uptime command and the Software-Version parameter display the same information.

Usage: **`tsshow`** [**`?`**] [***`uptime`***] [***`revision`***]

Syntax element:	Description:
`?`	List all options.
`uptime`	Display system uptime.
`revision`	Display software and version currently running.

Example: Following are some samples of TSshow output:

```
admin> tsshow
Show what? Type 'tsshow ?' for help.
admin> tsshow ?
tsshow ?            Display help information
tsshow uptime       Display system uptime.
tsshow revision     Display system revision.
admin> tsshow uptime
system uptime: up 36 days, 9 hours, 59 minutes, 27 seconds
admin> tsshow revision
system revision: tntsr 2.0.0
```

TunnelDebug

Description: Displays messages related to setting up Generic Routing Encapsulation (GRE) tunnels on the TAOS unit. The command is a toggle that alternately enables and disables the debug display.You would normally use this command with the ATMPdebug command.

Usage: Enter **`tunneldebug`** at the command prompt.

Example: The following example shows an ATMP tunnel being set up:

```
TUNNELTNT.CB[1/7]: Event=Start-Tunnel SN=80
TUNNELTNT[1/7]: DUMP [Start-Tunnel] SN=80  MC=1/17/24/10052400
  HN=[] priHA=[200.67.1.254] secHA=[] Udp=5150 pass=[ascend]
  IP=141.111.40.55  Mask=255.255.255.255   IPX=00000000:000000000000
```

```
TUNNEL: createFAsession: priHA=[200.67.1.254]  secHA=[]  udpPort=5150
        ifNum=1/17/24/10052400  MajDev=7  password=ascend
        mcIpAddr=141.111.40.55/32
TUNNEL-411: Alloc 1019F660  Id=411 TN=411
TUNNEL-411: resolving 200.67.1.254, port=5150,  SN=411
TUNNEL-START: In progress
TUNNELTNT[1/7]: DUMP [Start-Tunnel-Rsp] SN=411  MC=1/7/4/10059440
  LocalSN=80  GlobalSN=411  Status=In progress
TUNNEL: _dnsCallback: name=[200.67.1.254],  ip=200.67.1.254  DNS=411
TUNNEL-411: tunnelSetStatus: status=Good completion
TUNNELTNT[1/7]: DUMP [Update-Tunnel] SN=411
  TunnelNumber=405  mcRtIf=1/7/4/10059440  HomeRtIf=0/0/0/0
  HomeAgent=200.67.1.254:5150  HomeNetwork=[]   Flags=10  AgentMode=2
  IP=141.111.40.55  Mask=255.255.255.255   IPX=00000000:000000000000
TUNNELTNT[1/7]: DUMP [Set-Status] SN=411  ErrorCode=0
TUNNELTNT[1/7]: DUMP [Start-Tunnel-Rsp] SN=411  MC=1/7/4/10059440
  LocalSN=80  GlobalSN=411  Status=In progress
```

TunnelSlot

Description: The command has little practical use other than as a tool for developmental engineering.

Update

Description: Modifies optional functionality of the TAOS unit. To enable some options, you must obtain a set of hash codes (supplied by a Lucent Technical Support representative) that will enable the functionality in your TAOS unit. After each string is entered, the word *complete* appears, indicating that the TAOS unit accepted the hash code.

If you enter `update` without a text string modifier, the TAOS unit displays a list of current configuration information.

Usage: `update` [*`text_string`*]

Example:

```
admin> update
Host interfaces: 4
Net interfaces: 4
Port 1 channels: 255
Port 2 channels: 255
Port 3 channels: 255
Port 4 channels: 255
Field features 1: 182
Field features 2: 33
Field features 3: 54
Protocols: 1
admin> update 5 1023 12321312312312321
```

The following two messages indicate that the text strings were entered incorrectly:

```
update command: invalid arg 3!
update command: disallowed
```

The following message indicates that the TAOS unit accepted the update string:

```
update command: command complete.
```

WANdisplay

Description: Displays all packets received from, or sent to any of the WAN interfaces. Because WANdisplay output shows what the TAOS unit is receiving from and sending to the remote device, the information can be very helpful in resolving PPP negotiation problems.

If you enter the command on your TAOS unit while traffic is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which means that not all output can be displayed on the screen.

Depending on the types of information you need to gather, you might prefer to use the WANdisplay command during a period of low throughput, or to use WANdsess, WANopen or WANnext to focus the display.

Usage: `wandisplay number-of-octets-to-display`

Enter **`wandisplay 0`** to disable the logging of this information.

Example: Following are several examples of WANdisplay output. Note that the bytes are displayed in hexadecimal format.

```
admin> wandisplay 24
Display the first 24 bytes of WAN messages

> RECV-272:: 1 octets @ 5E138F74
  [0000]: 0D
RECV-272:: 13 octets @ 5E13958C
  [0000]: 0A 41 63 63 65 70 74 3A 20 69 6D 61 67
XMIT-276:: 1011 octets @ 2E12D8A4
  [0000]: 7E 21 45 00 03 EE 54 2B 40 00 37 06 BA 09 CF 2B
  [0010]: 00 86 D0 93 91 90 1A 0A
admin> wandisplay 0
WAN message display terminated
```

WANdsess

Description: Shows WAN data as it is received and transmitted for a particular user. The WANdsess command is very similar to the WANdisplay command, but when you use WANdsess, the TAOS unit displays only incoming and outgoing packets for a specific user. WANdsess is particularly helpful on a TAOS unit with several simultaneous active connections. The command acts as a filter, allowing you to focus your troubleshooting.

Use the WANdsess command with host cards only. You must first execute the Open command to open a session with the modem or HDLC card.

Usage: **`wandsess session-name octets`**

Syntax element	Description
`session-name`	Name of a local Connection profile or a RADIUS user profile.
`octets`	Maximum number of octets to display per packet. If you specify 0 (zero), the TAOS unit does not display any data.

Example: To open a session with a modem card, and activate the display of WAN data for Tim's sessions:

```
admin> open 1 7
modem-1/7> wandsess tim
RECV-tim:300:: 1 octets @ 3E13403C
  [0000]: 7E 21 45 00 00 3E 15 00 00 00 20 7D 31 C2 D2
RECV-tim:300:: 15 octets @ 3E133A24
  [0000]: D0 7D B3 7D B1 B3 D0 7D B3 90 02 04 03 00 35
XMIT-tim:300:: 84 octets @ 3E12D28C
  [0000]: 7E 21 45 00 00 4E C4 63 00 00 1C 7D 31 17 5F D0
  [0010]: 93 90 02 D0 93 91 B3 00
```

Note that the bytes are displayed in hexadecimal format.

See Also: WANdisplay, WANopening

WanEventsStats

Description: Displays statistics about WAN events of interest on a host card.

Usage: First, open a session to a host card, then enter **`waneventstats`** at the command prompt.

Example:

```
modem-1/2> wanEventStats
Output:
_sendCachedData() Counts:
NullWanInfo 0
BufLen: 0
NullHandle: 0
BadState: 0
QueuingFails: 0
ToMbufFails: 0
SendOk: 0

_loseCachedData() Counts:
NoBuf: 0
LoseOk: 0

_cachePrioData() Counts:
BadData: 0
MallocFails: 0
PrevCache: 0
CacheOk: 0
```

```
WanInfo Instance Error Counts:
_wanBufferSent: 0
_wanBufferRcvd: 0
_wanBreakRcvd: 0
_modemEventHandlerInstanceMismatch: 0

WanInfo TxPending Error Counts: 0

wanSendData() Counts:
_wanSendDataOk: 1fd2e
_wanSendDataHighPriority: 1fd2e
_wanSendDataNormPriority: 0
_wanSendDataNoInpMbuf: 0
_wanSendDataBadLen: 0
_wanSendDataNormPrioNoBuf: 0
_wanSendDataNoRoute: 0
```

In this output, the following counters should always be set to zero (a non-zero value indicates an error condition):

```
NullWanInfo 0
BufLen: 0
NullHandle: 0
BadState: 0
NoBuf: 0
BadData: 0
_wanBufferSent: 0
_wanBufferRcvd: 0
_wanBreakRcvd: 0
_modemEventHandlerInstanceMismatch: 0
WanInfo TxPending Error Counts: 0
_wanSendDataNoInpMbuf: 0
_wanSendDataBadLen: 0
```

The rest of the counters can have non-zero values, although most of them indicate how busy the system is and should have small values. For example, the following counters record high-priority message caching events:

```
SendOk: 0
LoseOk: 0
CacheOk: 0
```

The next counters record send message requests. These are the only counters that record normal events rather than errors. The first _wanSendDataOk counter represents the count of all HDLC packets sent out, which may be quite a large number. The other two counters represent the two types of HDLC data, normal and high priority. Their sum should equal the value of _wanSendDataOk in the absence of errors. For example:

```
_wanSendDataOk: 1fd2e
_wanSendDataHighPriority: 1fd2e
_wanSendDataNormPriority: 0
```

The next counter records dropped normal priority messages. A non-zero value indicates the number of normal messages dropped due to lack of a buffer. To some extent this indicates how

busy the system is, but because sessions have a buffer quota, it is possible to drop a normal message and increment this counter even when the system is not overloaded and when it is not out of buffers.

```
_wanSendDataNormPrioNoBuf: 0
```

The next counter reports requests to send a packet being processed after the session has been terminated. This is a normal occurrence when a call terminates during data transfer. (Its value should normally be relatively small but not necessarily non-zero.)

```
_wanSendDataNoRoute: 0
```

The following counters record the system's inability to obtain a DRAM or HDLC buffer for high priority message caching:

```
QueuingFails: 0
ToMbufFails: 0
MallocFails: 0
```

The following counter records high priority messages that have been dropped from the cache due to the arrival of another high priority message for the same session:

```
PrevCache: 0
```

WANopening

Description: Shows WAN data as it is received and transmitted during connection establishment for all users. The WANopening command is particularly helpful for troubleshooting connection problems in which users make the initial connection, but are disconnected within a few seconds. The output of WANopening is very similar to the output of WANdisplay, but WANopening only shows packets until the connection has been completely negotiated.

Use the WANopening command with host cards only. You must first execute the Open command to open a session with the modem or HDLC card.

Usage: `wanopening octets`

The *`octets`* value specifies the maximum number of octets to display per packet. If you specify 0 (zero), the TAOS unit does not log WAN data

Example: To open a session with a modem card, and activate the display of WAN data received and transmitted during connection establishment:

```
admin> open 1 7

modem-1/7> wanopening
Display the first 24 bytes of WAN messages
RECV-272:: 1 octets @ 5E138F74
  [0000]: 0D
RECV-272:: 13 octets @ 5E13958C
  [0000]: 0A 41 63 63 65 70 74 3A 20 69 6D 61 67

XMIT-276:: 1011 octets @ 2E12D8A4
  [0000]: 7E 21 45 00 03 EE 54 2B 40 00 37 06 BA 09 CF 2B
  [0010]: 00 86 D0 93 91 90 1A 0A
```

Note that the bytes are displayed in hexadecimal format.

See Also: WANdisplay, WANdsess

WANtoggle

Description: Displays messages from the WAN drivers on the TAOS unit, including the status of calls that are passed from the TAOS unit's call routing routines as the connection is prepared to be passed to the Ethernet drivers.

If you enter the command while traffic through your TAOS unit is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen. You might prefer to use this command during a period of low throughput.

The command is a toggle that alternately enables and disables the debug display.

Usage: Enter **`wantoggle`** at the command prompt.

Example: Following is a typical example of output produced by a modem call into the TAOS unit. After the incoming call is determined to be an analog call, a modem is directed to answer it.

```
WAN-389: wanOpenAnswer
WAN-389: modem redirected back to wan
WAN-389: Startup frame received
WAN-389: Detected unknown message
WAN-389: Detected ASYNC PPP message
WAN-389: wanRegisterData, I/F 58
```

The next two messages appear when the call is cleared.

```
WAN-389: wanCloseSession, I/F 58
```

The last message is not an indication of a problem. The modem clears the call a split second before the software releases its resources. The software does a check on the modem, which has already been released. This message is not an indication of a problem.

```
WAN-??: no modem assoc w WanInfo
```

Special administrative debug commands

Generating warning messages from a Coredump server

When coredumps are set up and enabled, you can specify an additional range of warning messages that will cause a coredump. The following new parameters (shown with default values) enable you to specify an additional range of Warning message index values to cause a coredump:

```
[in DEBUG/{ any-shelf any-slot 0 }]
min-warning-core-dump = 0
max-warning-core-dump = 0
```

Parameter	Specifies
Min-Warning-Core-Dump	Minimum Warning message index value to cause a coredump. This value must be less than or equal to the Max-Warning-Core-Dump value. The default zero means that only Warnings from 101 to 121 cause a coredump. The valid range is from 1 to 9999.
Max-Warning-Core-Dump	Maximum Warning message index value to cause a coredump. This value must be greater than or equal to the Min-Warning-Core-Dump value. The default zero means that only Warnings from 101 to 121 cause a coredump. The valid range is from 1 to 9999.

For example, the following command specify that in addition to Warnings 101 through 121, Warnings 500 through 600 will generate a coredump:

```
admin> read debug { 1 1 1}
DEBUG/{ shelf-1 slot-1 1 } read

admin> set min-warning-core-dump = 500

admin> set max-warning-core-dump = 600

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

Changes to the Debug profile are effective immediately.

Creating User Profiles

5

User profiles are for TAOS unit system administration. Do not confuse them with Connection profiles. User profiles are used by administrators who need access to the TAOS unit's command line interface to monitor or configure the unit. Connection profiles contain authentication and configuration information for a remote device or user and allow the remote user to connect to the TAOS unit for WAN or LAN access.

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

The TAOS unit ships with two predefined User profiles, named Admin and Default. The Admin account is the super-user, with full read-write permissions. Default is set to the other extreme. It authorizes the minimal use of commands.

Many sites choose to create some administrative accounts in a read-only mode, to allow those users to check status windows, read log buffers, and execute diagnostic commands. You need at least one administrative account in read-write mode, but you may choose to create several such accounts.

Understanding the User profile parameters

Table 5-1 describes common tasks you might have to perform to configure a User profile. The table includes a brief description of each task and lists the parameters you will use.

Table 5-1. Overview of User profile tasks

Task	Description of task	Associated parameters
Setting the name and password	When you create a new User profile with the New command, the system creates a default instance of the profile and reads it into the edit buffer. The name and password you assign to the profile represent a user or host name and a password used to authenticate that user at login.	Name Password
Activating the profile	The User profile is activated when you first create it. If you set Active-Enabled to No, the profile is not available for use.	Active-Enabled
Assigning permissions	Permissions control which actions the user who logs in with this profile can perform on the TAOS unit.	Allow-Termserv Allow-System Allow-Diagnostic Allow-Update Allow-Password Allow-Code
Logging the user out when idle	With the Idle-Timeout setting, you can specify the number of seconds a Telnet session can remain logged in with no keyboard activity.	Idle-Timeout
Setting the command-line prompt	The default command-line prompt is `TNT>`. If you set the prompt to an asterisk, the TAOS unit uses the name parameter as the prompt. For example, for the `admin` User profile, the prompt would be `admin>`.	Prompt
Specifying which status windows are displayed at login	You can display status windows by default at login, and you can specify what information should be displayed initially in the top, bottom, and left windows.	Default-Status Left-Status Top-Status Bottom-Status
Defining which log messages will be displayed	You can specify that log messages should be displayed immediately in the interface, instead of written to a log. You can also specify at which level the immediate display should begin. The lowest level is `none`, indicating that no messages should be displayed in the command-line interface. The highest level is `debug`.	Log-Message-Level

Understanding command permissions

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

```
admin> ?
?                               ( user )
arptable                        ( system )
auth                            ( user )
cadslLines                      ( system )
callroute                       ( diagnostic )
cgCtrl                          ( system )
clear                           ( user )
clock-source                    ( diagnostic )
clr-history                     ( system )
connection                      ( system )
dadslLines                      ( system )
date                            ( update )
debug                           ( diagnostic )
delete                          ( update )
device                          ( diagnostic )
dir                             ( system )
dircode                         ( system )
dnstab                          ( system )
ds3AtmLines                     ( system )
ether-display                   ( diagnostic )
fatal-history                   ( system )
```

Typically, read-write accounts enable the System command class. They might also enable the Update and Code command classes. Read-only accounts might be limited to the Diagnostic command class. Table 5-2 shows the commands associated with each permission:

Table 5-2. Permissions and associated commands

Permission	Command class	Commands in this class	
N/A (always enabled)	User	? Auth Clear	Help Quit Whoami

Table 5-2. Permissions and associated commands (continued)

Permission	Command class	Commands in this class	
Allow-System	System	ARPtable BRIChannels Clr-History Connection Dir Dircode DNStab Fatal-History Get HDLC IGMP IPcache IP-Pools IProute Line List Log Modem	Netstat New OSPF Power Quiesce Read Refresh Screen Set Show Status SWANlines T1channels UDS3lines Userstat Version View
Allow-Diagnostic	Diagnostic	Callroute Clock-Source Debug Device DS3ATMlines Ether-Display If-Admin NSlookup	OAMLoop Open Ping Rlogin Slot Telnet Traceroute Uptime
Allow-Update	Update	Date Delete Load Nvram	Reset Save Write
Allow-Code	Code	Format	Fsck
Allow-Termserv	Termserv. This permission enables the user to invoke the Terminal-Server command and use the terminal-server interface.	Terminal-Server	

Table 5-2. Permissions and associated commands (continued)

Permission	Command class	Commands in this class
Allow-Password	N/A	The Allow-Password permission enables the user to view passwords. If set to No, the user sees a row of asterisks instead of the actual configured password. If the administrator that backs up system configurations does not have the Allow-Password permission set to Yes, passwords are not saved as part of the configuration.

Sample User profiles

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

When you create a new profile by specifying its index on the command line, the Default profile is used as the template. In the following is an example, an administrator creates a read-write administrative login named Bill, which has access to System, Diagnostic, and Update command classes:

```
admin> new user admin
USER/admin read
admin> set name = bill
admin> set password = my-password
admin> set allow-password = yes
admin> set allow-code = no
admin> write
USER/bill written
```

Following is an example of creating a User profile named Test, which is based on the Admin profile but restricts some permissions and has a different password:

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

In the following example, an administrator creates a profile that enables the user to use the terminal-server commands but not to perform any other actions:

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

To log in by means of the new profile:

```
admin> auth techpubs
Password: december
```

Customizing the environment for a User profile

In addition to authentication and permission information, User profiles also contain parameters that affect how the user's environment appears at login. You can customize the following areas:

- The system prompt
- Whether the status window is displayed by default
- Information contained in the status window
- The level of log messages displayed

Setting the system prompt

The default command-line prompt is `TNT>`. You configure the prompt with the Prompt parameter. An asterisk in this setting causes the TAOS unit to substitute the value of the profile's name parameter upon successful login. For example, for the Admin profile, the prompt would be as follows:

```
admin>
```

Specifying status window information

The TAOS unit generates a continuous stream of statistics about its activities. You can specify in a User profile whether these statistics should always be displayed when a user logs in using that profile, what the areas of the window should display by default, and the size of the status windows. Opening the status window requires an 80-column by 24-row VT100 window.

The contents of the status window are determined by the following parameters in a User profile (show with their default values):

- Left-Status = Connection-List
- Top-Status = General-Info
- Bottom-Status = Log-Window

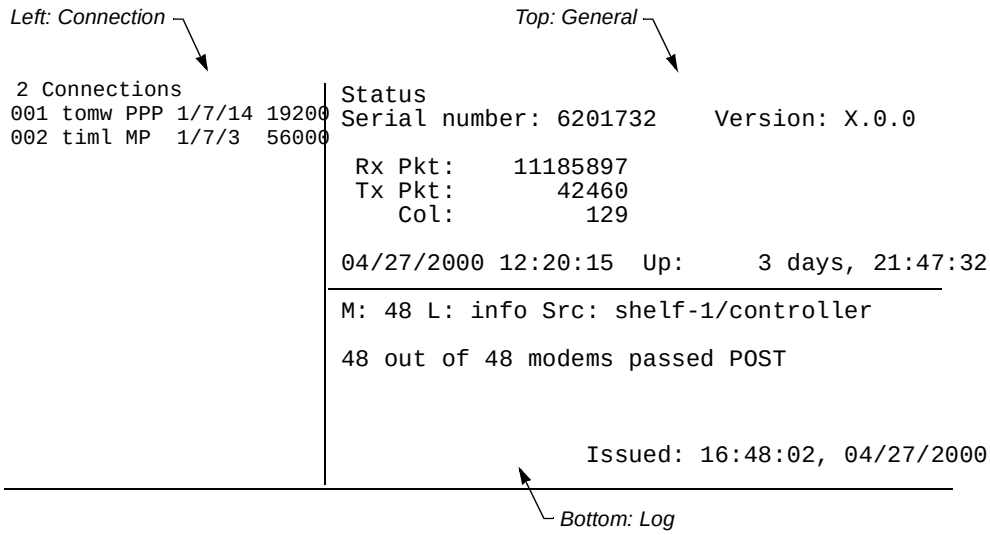
The size of the status window are determined by the following parameters in a User profile (shown with their default values)

- Screen-Length = 24
- Status-Length = 18

See the *APX 8000/MAX TNT Reference* for details of using these parameters.

Figure 5-1 shows the default contents for each area of the status window:

Figure 5-1. Information in the status window



Following is an example of configuring the User profile to display the status window upon login, and to show line information in the bottom area of the window. It also configures a larger terminal emulator window and status screens:

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

Note that Status-Length must be at least 6 lines smaller than Screen-Length.

Setting log levels for each login

You can configure the User profile to display a certain level of log messages immediately in the interface, in addition to writing them to a log file. Following is an example that causes critical, alert, and emergency messages to be displayed in the interface, interrupting whatever work might be going on at the prompt:

```
admin> read user test

USER/test read

admin> set log-display-level = critical

admin> write
USER/test written
```

Critical messages indicate that an interface has gone down or a security condition has been noted. Alert messages indicate that something undesirable has happened but probably will not prevent normal operation of the system. Emergency messages indicate that something undesirable has happened and will probably prevent normal operation.

Other levels include Error messages (an error condition has occurred), Warning messages (something out of the ordinary has occurred, such as a login failure), Notice (events in normal operation, such as a link going up or down), Info (changes that are not normally of interest), Debug (messages related to debugging configurations), and None (no messages are displayed).

Logging in as a different user

To login with a different User profile, use the Auth command, as in the following example:

```
admin> auth test

Password:@3wPZHd2
```

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

Specifying a timeout for logins

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

1. Read the System profile:

   ```
   admin> read system
   ```

2. Specify an idle time period:

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

3. Write the profile:

   ```
   admin> write
   SYSTEM written
   ```

Finding the current user

To find out which User profile you are currently using, enter the Whoami command. For example:

```
admin> whoami
admin
```

Creating and managing remote user profile filters

You can create RADIUS pseudo-user profiles that define data filters, and then apply the filters to multiple local Connection or RADIUS profiles by referring to the pseudo-user profile name.

When the TAOS receives a Filter-ID in an Access-Accept packet from RADIUS, it searches for a matching local filter. If it does not find one, the TAOS unit requests the filter from the RADIUS server. You can specify how the system should behave if the filter referred to in a profile is not found. The system can either establish the session and log a message about the missing filter, or terminate the call if a filter is not found.

Externally defined filters are cached locally for a configurable interval. The FiltCache command displays statistics about each cached RADIUS filter profile, and enables you to flush profiles from the cache.

Current limitations

In this release, the remote filter implementation is subject to the following limitations:

- Filters applied to dialout calls are not supported in this release.
- Call filters, route filters, and TOS filters are not supported in this release. Only data filters are currently supported.

Overview of local profile settings

Following are the local parameters related to dynamic remote filters:

```
[in ANSWER-DEFAULTS:session-info]
filter-required = no

[in CONNECTION:session-options]
filter-required = no
data-filter = ""

[in IP-GLOBAL]
default-filter-cache-time = 1440
```

Parameter	Specifies
Filter-Required	Whether access to the filter is required for the session. With the default value of No, the system establishes the session even if the specified filter is not found. If the parameter is set to `yes`, the system disconnects the call if the filter is not found. This setting does not apply if the profile does not refer to a filter by name. The Answer-Defaults setting is used for RADIUS user profiles that apply a filter and do not explicitly specify a value for Ascend-Filter-Required (50).
Data-Filter	Name of a Filter profile associated with the connection. The name can be of a local profile or a filter pseudo-user profile in RADIUS. However, if a local Connection profile does not use authentication, it cannot specify a RADIUS filter profile.
Default-Filter-Cache-Time	Number of minutes to cache RADIUS filter profiles that do not include a value for Ascend-Cache-Time (57). The default is `1440` (24 hours). Once the cache timer expires, cached profiles are deleted from system memory. The next time a remote filter is needed, the system retrieves the profile from RADIUS and stores it in cache again. Keeping a profile in cache increases the performance of establishing sessions that use the filter, at the cost of some system memory. If this parameter is set to `0` (zero), the default timer is disabled so that only RADIUS profiles that specify a cache time are cached.

Overview of RADIUS user profile settings

RADIUS user profile support for filter profiles is provided by the following vendor-specific attributes (VSAs):

RADIUS attribute	Value
Filter-ID (11)	Name of a local or remote filter profile associated with the connection.
Ascend-Filter-Required (50)	Whether access to the filter is required for the session. With the default value of Required-No (0), the system establishes the session even if the specified filter is not found. If the attribute is set to Required-Yes (1), the system disconnects the call if the filter is not found. This setting does not apply if the profile does not refer to a filter by name. If this attribute is not specified, the Answer-Defaults setting is used to determine system behavior when the specified filter is not found.

Overview of RADIUS pseudo-user profile settings

A filter profile is a pseudo-user profile in which the first two lines have the following format:

```
profile-name Password = "ascend" Service-Type = Outbound
```

The *profile-name* value is any name you assign to the profile. Duplicate filter names are not allowed. If a local Filter profile is already stored, the TAOS does not retrieve a filter profile of the same name from the RADIUS server. Filter profile definitions can include the following attribute-value pairs:

RADIUS attribute	Value

Ascend-Data-Filter (242)	An abinary-format filter specification using one of the following formats:
	`"generic dir action offset mask value compare [more]"`
	`"ip dir action [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ][ proto ] [ destport cmp value ] [ srcport cmp value ] [est]]"`

Ascend-Cache-Refresh (56)	Whether the timer for cached routes in this profile is reset each time a new session becomes active that refers to the pseudo-user profile. Refresh-No (0) does not reset the timer. Refresh-Yes (1) resets the cache timer when a session referring to the profile becomes active.
Ascend-Cache-Time (57)	Number of minutes to cache the profile. Once the cache timer expires for a RADIUS profile, the profile is deleted from system memory. The next time it is needed, the system retrieves it from RADIUS and stores it in cache again. Keeping a profile in cache increases the performance of route lookups, at the cost of some system memory. The minimum possible cache time is 0 minutes, which causes the system to retrieve the profile for every route lookup in the table. This setting is usually not desirable. If this attribute is not specified, the IP-Global setting is used.

To use these attributes, the RADIUS server must support vendor-specific attributes (VSAs) and the TAOS must be configured in VSA compatibility mode. Following are the relevant settings:

```
[in EXTERNAL-AUTH]
auth-type = radius
```

```
[in EXTERNAL-AUTH:rad-auth-client]
auth-radius-compat = vendor-specific
```

For details about these settings, see the *APX 8000/MAX TNT Reference*. For details about defining data filters in RADIUS, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide*.

Examples of configuring a filter profile in RADIUS

Following is a sample RADIUS filter profile:

```
filter-c Password = "ascend", Service-Type = Outbound
   Ascend-Cache-Time = 20,
   Ascend-Cache-Refresh = Refresh-Yes,
   Ascend-Data-Filter = "ip out forward tcp dstip 10.1.1.3/16",
   Ascend-Data-Filter = "ip out drop"
```

The cache timer has been set to 20 minutes, and the timer is reset each time the filter is applied to a session.

The following commands configure a default cache time for RADIUS filter profiles:

```
admin> read ip-global
IP-GLOBAL read

admin> set default-filter-cache-time = 180

admin> write
IP-GLOBAL written
```

Following is a sample RADIUS filter profile that makes use of the default because a value for Ascend-Cache-Time (57) is not explicitly specified:

```
filter-e Password = "ascend", Service-Type = Outbound
   Ascend-Data-Filter = "ip out forward tcp dstip 10.2.2.2/28",
   Ascend-Data-Filter = "ip out drop"
```

Examples of applying remote filters

The following commands modify a Connection profile so that the session uses a remote filter and the system disconnects the call if the filter is not found:

```
admin> read connection p50-v2
CONNECTION/p50-v2 read

admin> set session-options data-filter = filter-c

admin> set session-options filter-required = yes

admin> write
CONNECTION/p50-v2 written
```

Following is a sample RADIUS profile that applies the same filter profile with the same requirements. This profile also specifies how the filters must be cached for this connection:

```
p50-v2 Password = "my-password", Service-Type = Framed
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.1.1.1,
    Framed-IP-Netmask = 255.0.0.0,
    Filter-ID = "filter-c",
    Ascend-Filter-Required = Required-Yes
```

The following commands configure the system to reject incoming calls when the RADIUS user profile specifies a filter that is not found, and the user profile does not explicitly say what to do if the filter is not found:

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

```
admin> set session-info filter-required = yes

admin> write
ANSWER-DEFAULTS written
```

Following is a sample RADIUS profile that makes use of the default because a value for Ascend-Filter-Required (55) is not explicitly specified:

```
p50-v2 Password = "my-password", Service-Type = Framed
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.1.1.1,
    Framed-IP-Netmask = 255.0.0.0,
    Filter-ID = "filter-c"
```

Managing remote filters

Filters defined in RADIUS pseudo-user profiles are accessible in the command-line interface as if they were local Filter profiles. For example, in the following listing, the profiles named `filter-a` and `filter-b` are local Filter profiles, and the profile named `filter-c` is a filter profile obtained from RADIUS:

```
admin> dir filter
   464  01/04/2000 19:01:49  filter-a
   470  01/04/2000 19:10:57  filter-b
  3901  01/04/2000 20:01:50  filter-c
```

You can read and list the contents of the remote filters in the usual way, as if they were local profiles. For example:

```
admin> read filter filter-c
FILTER/filter-c read (read-only)

admin> list
[in FILTER/filter-c]
filter-name* = filter-c
input-filters = [ { no no generic-filter { 0 0 no no +
output-filters = [ { yes no ip-filter { 0 0 no no +
```

Note: You cannot change RADIUS filter specifications from the command-line interface.

You can delete RADIUS filter profiles by using the `delete` command. For example:

```
admin> delete filter filter-c
Delete profile FILTER/filter-c? [y/n] y
FILTER/filter-c deleted
```

Parameter reference entries

Default-Filter-Cache-Time

Description: Specifies the default time (in minutes) during which the RADIUS filter profile remains locally cached on the TAOS.

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`

Dependencies: IP-Global

See Also: Filter-Required

Filter-Required

Description: Specifies whether the TAOS establishes a call if the filter profile applied in the caller's Connection profile cannot be found locally or in RADIUS.

Usage: Specify `yes` or `no`. The default is `no`.

- `yes` specifies that the TAOS does not establish a call if the filter profile applied in the caller's Connection profile cannot be found locally or in RADIUS.
- `no` specifies that the TAOS 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 uses the Filter-Required value in the Answer-Defaults profile.

Location: Answer-Defaults > Session-Info, Connection > Session-Options

SNMP Administration

6

The TAOS unit supports SNMP (Simple Network Management Protocol) on a TCP/IP network. An SNMP management station that uses supported Management Information Bases (MIBs) can query the TAOS unit, set some parameters, sound alarms when certain conditions appear in the TAOS unit, and so forth. The TAOS unit has its own SNMP password security (community strings), which you should set up to protect the TAOS unit from being reconfigured from an SNMP station.

The TAOS unit supports profiles that control which classes of events generate traps to be sent to an SNMP manager, which SNMP managers can access the unit, and community strings to protect that access.

SNMP support

This section describes the SNMP supported on the TAOS unit.

Standard MIBs

This section describes the standard MIBs supported on the TAOS unit.

RFC 1213 (MIB-II)

The MIB-11 enables you to monitor and configure basic components of the TAOS unit's system, interfaces, and protocols. Note that the interface table in MIB-II is superseded by RFC 2233 (Interface MIB).

RFC 1253 (OSPF MIB)

The OSPF MIB enables you to monitor and configure OSPF version 2.

RFC 1315 (Frame Relay MIB)

The Frame Relay MIB specifies SNMP MIB variables for Frame Relay DTEs. The TAOS unit's HDLC cards support this MIB.

RFC 1317 (RS232 MIB)

The RS232 MIB enables you to monitor and configure asynchronous or synchronous serial links with RS-232-like control signals.

RFC 1398 (Ethernet MIB)

The Ethernet MIB enables you to monitor the TAOS unit's Ethernet interfaces.

RFC 1406 (DS1 MIB)

The DS1 MIB enables you to query the state and configuration of T1 or E1 lines. The TAOS unit supports all tables in this MIB *except* the `dsx1FracTable`.

In addition, TAOS unit's also support loopback modes using the Get and Set requests on the `dsx1LoopBackConfig` object of the DS1 MIB (RFC 1406).The `dsx1NoLoop` and `dsx1LineLoop` loopback modes are supported on both T1 and E1 lines. The `dsx1PayloadLoop` loopback mode is not supported.

RFC 1407 and RFC 2496 (DS3 MIB)

The DS3 MIB enables you to query the state and configuration of T3 or E3 lines.

RFC 1695 and RFC 2515 (ATM MIB)

The ATM MIB enables you to manage the ATM interface on the TAOS unit's DS3-ATM2 slot card. The TAOS unit supports the following groups in the ATM MIB related to network endpoints:

- (1) ATM Interface configuration group
- (2) ATM Interface DS3 PLCP group
- (3) ATM Interface TC Sublayer group
- (5) ATM Interface VCL configuration group
- (8) ATM Interface AAL5 VCC performance statistics group

Currently it is not possible to define new connections solely by using SNMP management, so many of the read-write and read-create parameters were changed to read-only.

RFC 1696 (Modem MIB)

The Modem MIB defines managed objects for modems. The TAOS unit supports all objects in the Modem MIB.

The Modem MIB defines an `mdmIndex` object whose value is used as an index into the tables defined in the MIB, with each modem in a managed system assigned a unique index value.

This object is supported in the TAOS unit as a read-only Modem-Table-Index parameter in the Admin-State profile.

The value of this parameter is allocated by the system when it first detects the presence of a modem card.

The fact that the TAOS unit supports hot-swapable cards requires a relaxation of the MIB definition of the `mdmIndex` object in the same manner that RFC 1573 relaxes the `ifIndex` definition. The MIB definition of `mdmIndex` specifies that

- the index value must be in the range of 1 to mdmNumber, and
- the value must remain constant from one reinitialization of the network management agent to the next.

A modem card may be added to or removed from the TAOS unit without reinitializing the SNMP agent, which affects both of these definitions. For example, if a modem card is inserted into slot 1 of a new TAOS unit's system, its 48 modems are allocated the index values 1 through 48. If another modem card is inserted into slot 3, its modems are allocated the index values 49 through 96. If the TAOS unit is rebooted, these values remain constant. If the modem card in slot 1 is removed and the TAOS unit is rebooted again, the index values for the modem card in slot 3 still remain constant with the range 49 through 96, even though the value of mdmNumber is now 48.

RFC 1850 (OSPF Traps, Version 2 MIB)

TAOS units support OSPF traps as defined in RFC 1850, *OSPF Version 2 Management Information Base.* For an OSPF trap to be generated when the trap condition occurs, OSPF traps must be enabled, either in the Trap profile or by setting the corresponding bit in the new MIB object, `ospfSetTrap`, defined in RFC 1850. In addition, the individual trap that represents the trap condition must be enabled.

RFC 2233 (Interface MIB)

The TAOS unit supports the Interface MIB based on RFC 2233, which supersedes the SNMP MIB-II interface table defined in RFC1213. The interface table contains only the system's physical interfaces and nailed (permanent) interfaces.

The index value of an interface does not change following a system reset, and if an entry is removed from the interface table dynamically, its index value is not reused until the management station has been reinitialized. The interface table does not contain virtual circuit interfaces, such as a Frame Relay datalink configured on a channelized DS1 interface.

Table 6-1 describes the TAOS unit's support for RFC 2233.

Table 6-1. TAOS unit support for RFC 2233

RFC 2233 Table	Comment
`ifTable`	The ifTable from MIB-II (RFC 1213) and is fully supported on the TAOS unit.

Table 6-1. TAOS unit support for RFC 2233 (continued)

RFC 2233 Table	Comment
`ifXTable`	The TAOS unit supports this table with the following exceptions: • The `OwnerString` object is not supported. • The `InterfaceIndexOrZero` object is not supported. • The 64-bit HighCounter objects are not supported. • The `ifPromiscuousMode` object is read-only.
`ifStackTable`	Not supported on the TAOS unit.
`ifRcvAddressTable`	Not supported on the TAOS unit.
`ifTestTable`	Not supported on the TAOS unit.

RFC 2515 (ATM MIB)

The ATM MIB enables you to manage the ATM interface on the TAOS unit's DS3-ATM2 slot card. The TAOS unit supports Get operations on the following tables of the ATM MIB described in RFC 2515, *Definitions of Managed Objects for ATM Management*:

- ATM Interface configuration table
- ATM Interface DS-3 Physical Layer Convergence Protocol (PLCP) table
- ATM Interface transmission convergence (TC) sublayer table
- ATM Interface virtual channel link (VCL) configuration table
- ATM Interface ATM Adaptation Layer 5 (AAL5) virtual channel connection (VCC) performance statistics table

Set operations are not yet supported. In addition, the following SNMPv2-related changes were made to `rfc2514.mib`:

- The definition of `atmMIB` and `atmMIBObjects` were moved here from `rfc2515.mib`.
- All the definitions were modified to SNMPv1 Structure of Management Information (SMI).
- The SNMPv1 entries `atmNoTrafficDescriptor`, `atmClpNoTaggingNoScr`, and `atmClpTaggingNoScr` are deprecated.

The following SNMPv2-related changes were made to `rfc2515.mib`:

- The definitions of `atmMIB` and `atmMIBObjects` were moved to `rfc2514.mib`.
- All MIB fields with Current Status were changed to Mandatory.
- MAX-Access syntax was changed to Access for all the fields.
- Fields with read-create access were changed to read-write.
- Set functions are not supported on the following parameters, so they have been changed from read-write to read-only:

  - `atmInterfaceConfEntry` parameters
  - `atmVclReceiveTrafficDescrIndex`, `atmVclTransmitTrafficDescrIndex` and `atmVclAdminStatus` in `atmVclTable`
  - `atmVccAalType`, `atmVccAal5CpcsTransmitSduSize`, `atmVccAal5CpcsReceiveSduSize`, `atmVccAal5EncapsType`, `atmVclRowStatus`, `atmVclCastType` and `atmVclConnKind` in `atmVclTable`
- Read-write permissions were changed to read-only permission in the following tables:
  - `atmTrafficDescrParamTable`
  - `atmVplTable`
- The `atmVpCrossConnectTable` and `atmVcCrossConnectTable` tables are not supported.

RFC 2574 (SNMPv3 User-based Security Model (USM) MIB)

TAOS units support security enhancements based on the SNMP version 3 (SNMPv3) User-based Security Model (USM) described in RFC 2574. In TAOS release 9.0, SNMPv3 encryption for authentication and privacy for SNMPv3 USM is supported. Data present in the unencrypted Protocol Data Unit (PDU) might be copied and interpreted by unauthorized listeners on the wire, but privacy support remedies this situation.

Enabling privacy causes the TAOS unit to accept encrypted requests from the manager and send responses in encrypted format. The encryption uses a 64-bit Data Encryption Standard (DES) algorithm. The system generates the private key for the encryption by using the user's privacy password.

In addition to the security enhancement features, SNMPv3 supports the `GetBulkRequest` PDU. It minimizes the number of protocol exchanges required to retrieve a large amount of management information. The `GetBulkRequest` PDU allows an SNMPv3 manager to request a response that is as large as possible given the constraints on message size.

To use SNMPv3, the network-management license must be enabled in the system. The following commands verify that the network management license has been enabled on the system:

```
admin> get base network-management
[in BASE:network-management-enabled]
network-management-enabled = yes
```

SNMPv3 security management provides TAOS units with the following management features, which use the SNMPv3 User-based Security Model (USM):

SNMPv3 USM feature	Description
• Authentication	Provides data integrity and data origin authentication. The message authentication is coded with either the MD5 or the SHA hash function.
• Privacy	Protects messages from being copied and interpreted by unauthorized listeners on the network.
• Timeliness	Protects against message delay or replay.

SNMPv3 USM feature	Description
• Discovery	Allows one SNMP engine to obtain sufficient information about more than one TAOS units' SNMP engine to establish communication between an SNMP manager station and the TAOS units.
• GetBulkRequest	Added from SNMPv2 to allow the SNMPv3 manager to minimize the number of protocol exchanges required to retrieve a large amount of management information. The GetBulkRequest Protocol Data Unit (PDU) allows an SNMPv3 manager to request as large a response as possible.

Network-management software option enforcement

The network-management software must be installed on the TAOS units for SNMPv3 USM to be functional. Verify that the network management software is installed by entering a **`get base`** command. Look for a line containing `network-management-enabled = yes`.

```
admin> get base network-management
[in ASE:network-management-enabled]
network-management-enabled = yes
```

Note: If this feature is not enabled, SNMPv3 USM is disabled.

Here is an example of a typical SNMPv3 USM configuration when network management software is enabled.

```
admin> read base
BASE read (read-only)
admin> list
[in BASE]
shelf-number = 1
software-version = 8
software-revision = 0
software-level = b
d-channel-enabled = yes
aim-enabled = no
switched-enabled = yes
multi-rate-enabled = yes
frame-relay-enabled = yes
maxlink-client-enabled = disabled
data-call-enabled = yes
r2-signaling-enabled = no
serial-number = 8011064
hardware-level = 0
countries-enabled = 256
domestic-enabled = yes
phs-2-1-support = yes
modem-dialout-enabled = no
firewalls-enabled = yes
ipsec-enabled = not-installed
network-management-enabled = yes  <-- required for SNMP3 USM
```

Command line interface changes

In TAOS 9.0, there are several changes to the command line interface (CLI). Two new parameters have been added to the SNMP profile. The SNMPV3-USM-User profile is also new.

SNMP profile

Two parameters in the SNMP profile, Snmp-Message-Type and Security Level, support SNMP system security configuration. The Snmp-Message-Type parameter specifies the SNMP protocol type that communicates on TAOS units. The Security Level parameter specifies the security level of the SNMP agent. Definitions of the two SNMP parameters follow.

Parameter	**Specifies**
SNMP-Message-Type	SNMP protocol used by the SNMP agent in the unit. • `v1-and-v3` (default value): Enables the SNMP agent to communicate with both the SNMPv1 and SNMPv3 protocols. • `v1-only`: Forces the SNMP agent to communicate using only the SNMPv1 protocol. Any SNMP messages that arrive at the agent with a protocol type other than SNMPv1 are discarded. • `v3-only`: Forces the SNMP agent to communicate using only the SNMPv3 protocol. Any SNMP messages that arrive at the agent with a protocol type other than SNMPv3 are discarded.
Security-Level	Security level of the SNMP agent when SNMPv3 is in use. • `none` (default value): No security level checking is required for incoming messages. • `auth-nopriv`: SNMPV3-USM-User profile of the users sending the message must have the Auth-Profile parameter set to `md5-auth` or `sha-auth.` Otherwise, the SNMP agent returns a REPORT message, which means the security level is not supported. This parameter does not apply to SNMPv1 messages. **Note:** This value is applicable only if SNMP-Message-Type is configured to support SNMPv3. • `auth-priv`: SNMPV3 USM users should send messages that are authenticated and encrypted. All other messages are received with a REPORT message, which means the security level is not supported.

SNMPV3-USM-USER profile

The `SNMPV3-USM-User` profile provides the ability to create and edit users profiles. The following are configurable parameters within the `SNMPV3-USM-USER` profile.

- Name
- Auth-key

- Priv-key
- Active-Enabled
- Read-Write-Access
- Auth-Protocol
- Priv-Protocol

Following is a sample configuration of the relevant parameters in an `SNMP-USM-User` profile.

```
admin> new snmpv3 testv3
SNMPv3-USM-USER/testv3 read
admin> list
in SNMPv3-USM-USER/testv3]
name* = testv3
active-enabled = yes
read-write-access = no(*)
auth-protocol = md5-auth(*)
priv-protocol = no-priv(*)
auth-key = (*)
priv-key = (*)
```

Note: (*) This symbol represents a factory default value setting.

Parameter	Specifies
Name	Username. Messages sent to or from the SNMP engine on behalf of this name use the security parameters specified in this profile. The value can contain up to 23 characters and can include special characters by using the \xNN format with the ASCII code for the character. For example, the value `test\x20\x21` represents the string "`test !`".
Active-Enabled	Enable/disable SNMPV3 USM features for this user. The default value is `no`.
Read-Write-Access	Enable/disable read-write access to the TAOS unit's MIBs for this user. When the value is `no` (default), the user has read access only, which enables viewing but not modification of the MIBs.
Auth-Protocol	Enable/disable authentication of messages sent on behalf of this user to or from the SNMP engine, and if enabled, the type of authentication protocol to use. If this parameter is set to a value other than `no-auth`, the Password parameter must specify the password to be used. Following are the valid values: • `no-auth:` no authentication required. • `md5-auth:` (the default value) specifies that the MD5 protocol must be used for authentication. • `sha-auth:` enables authentication and specifies that SHA protocol must be used.

Parameter	Specifies
Priv-Protocol	Enable/disable encryption of messages sent on behalf of the user to or from the SNMP engine, and if enabled, the type of privacy protocol to be used. Default setting is `no-priv`. Following are the valid values: • `No-Priv` (the default): no encryption is required and that privacy is disabled. • `DES-Priv`: DES-based privacy is required. Incoming messages that are DES-encrypted are interpreted, and outgoing responses are encrypted using DES. Note that outgoing reports are not encrypted.

Auth-Key	Specifies an authentication key for SNMPv3 USM users. In most cases, you do not set this string directly. Instead, use the SnmpAuthPass command to generate the value. If you have permission to view passwords, the authentication key appears as a string with escape sequences for save and restore purposes. Otherwise, the authentication key appears as a row of asterisks. The default is null.
	
	If you change the value of Auth-Key directly, keep in mind that the length of the escape sequence must be 10 (16d in hexadecimal) if Message Digest 5 (MD5) is in use and 14 (20d in hexadecimal) if the Secure Hash Algorithm (SHA) is in use. If you specify an invalid value, the unit uses the previous key, if any, to communicate with the SNMP manager. If no previous key exists, this USM user cannot communicate with the network until a valid key is set by means of the snmpAuthPass command.
	
	Suppose you use the snmpAuthPass command to generate the following 16-byte string:
	`27 0a dc 75 f8 98 e5 7c 4c 03 22 7d dd ac 0d ef`
	
	The system displays it as the following Auth-Key value:
	`'\x0a\xdcu\xf8\x98\xe5|L\x03"}\xdd\xac\x0d\xef`
	
	Consider the following:
	• 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), 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 Auth-Protocol is No-Auth, Auth-Key does not apply.

Parameter	Specifies

Priv-Key	Specifies a privacy key for SNMPv3 USM users.
	
	In most cases, you do not set this string directly. Instead, use the snmpPrivPass command to generate the value. If you have permission to view passwords, the privacy key appears as a string with escape sequences for save and restore purposes. Otherwise, the privacy key appears as a row of asterisks. The default is null.
	
	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. The escape sequence must be 14 (20d in hexadecimal) if the Secure Hash Algorithm (SHA) is in use. If you specify an invalid value, the unit uses the previous key, if any, to communicate with the SNMP manager. If no previous key exists, this USM user cannot communicate with the network until a valid key is generated by means of the snmpPrivPass command.
	
	Suppose you use the snmpPrivPass command to generate the following 16-byte string:
	
	`27 0a dc 75 f8 98 e5 7c 4c 03 22 7d dd ac 0d ef`
	
	The system displays it as the following Priv-Key value:
	
	`'\x0a\xdcu\xf8\x98\xe5|L\x03"}\xdd\xac\x0d\xef`
	
	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 No-Auth, Priv-Key does not apply.

SNMPv3 USM Commands

The following commands support SNMPv3 USM:

- snmpAuthPass
- snmpPrivPass

A description of each command follows:

Command	Specifies
snmpAuthPass	Generates the authentication key of an SNMPv3 USM user. The snmpAuthPass command can accept a username in escape sequence format. To generate the authentication key of the user `robin` with the password `abc123,` first type the snmpAuthPass command followed by the user name and password: `admin> snmpAuthPass robin abc123` 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.
snmpPrivPass	Generates the privacy key of an SNMPv3 USM user. The snmpPrivPass command can accept a username in escape sequence format. To generate the privacy key of the user `robin` with the password `abc123,` first type the snmpPrivPass command followed by the user name and password: `admin> snmpPrivPass robin abc123` 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.

Sample SNMPv3 USM configuration

To configure the USM features for a user, you must specify a name for the SNMPV3-USM-User profile and set the Active-Enabled parameter to `yes`. You must also specify a password if the Auth-Protocol parameter is set to anything but `no-auth`.

The following sample commands specify the use of MD5 authentication for messages sent on behalf of a user named `testv3` to or from the SNMP engine. The user is assigned read-write access to the unit's MIBs.

```
admin> new snmpv3-usm-user testv3
SNMPV3-USM-USER/testv3 read
admin> set active-enabled = yes
admin> set read-write-access = yes
admin> set priv-protocol = des-priv
admin> write
SNMPV3-USM-USER/testv3 written

admin> snmpAuthPass testv3 abc123
admin> snmpPrivPass testv3 abc123

admin> read snmpv3-usm-user testv3
SNMPV3-USM-USER/testv3 read
admin> list
[in SNMPV3-USM-USER/testv3]
name* = testv3
active-enabled = yes
read-write-access = yes
```

```
auth-protocol = md5-auth
priv-protocol = des-priv
auth-key = \xfd\xcd\xb2V\xa7\x81\xa7\x89n"\xd5\x02\x8b\xb2\xe7K
priv-key = \xfd\xcd\xb2V\xa7\x81\xa7\x89n"\xd5\x02\x8b\xb2\xe7K
```

Sample configuration of agent restriction to SNMPv3

The following commands configure the SNMP agent to use only SNMPv3 and to check a user's security level before allowing access:

```
admin> read snmp
SNMP read
admin> set snmp-message-type = v3-only
admin> set security-level = auth-nopriv
admin> write
SNMP written
```

USM MIB Support

The USM MIB enables you to use an SNMP manager to create, modify and delete SNMPv3 USM users by means of Set and Get requests. When you create, modify, and delete SNMPv3 USM users by means of SNMP Set and Get commands, you can perform the following tasks:

- Change user status from In-Service to Not In-Service, and vice-versa.
- Modify authentication and privacy keys.
- Disable authentication and privacy.

However, you must use the local interface rather than SNMP to enable authentication and privacy. In addition, you cannot create or modify more than one user in the same SNMP request.

Creating, modifying, and deleting SNMPv3 USM users

When creating, modifying, and deleting SNMPv3 USM users from an SNMP manager, consider the following:

- This implementation does not support the creation or modification of multiple users by means of a single request Protocol Data Unit (PDU).
- The system processes only those PDUs that contain a combination of Set requests recommended by RFC 2574 to create, modify and delete users. For example, a PDU containing `SET-usmUserAuthProtocol` and `SET-usmUserAuthKeyChange` generates an error. These two requests must be sent in two separate PDUs in the appropriate order.

Refer to RFC 2574 for complete details about how to create, modify and delete entries in the USM User Table.

Creating an SNMPv3 USM user

Any existing user can be used as a template. For this reason, use the local interface to create a set of profiles for users with different security parameters. The profiles you create can, in turn, be used as templates. To create a new user, proceed as follows:

1. Clone a new user from a template that has appropriate security levels.
2. To specify privacy for the user, set the privacy key by using the `keyChange` value. Otherwise, set the protocol to `usmNoPrivProtocol`.
3. To specify authentication for the user, set the authentication key by using the `keyChange` value. Otherwise, set the protocol to `usmNoAuthProtocol`.
4. Activate the new user.

Modifying an SNMPv3 USM user

Use SNMP Get and Set requests to modify security levels, privacy and authentication protocols, privacy and authentication keys, and service status (In-Service to Not-In-Service, and vice versa).

If the password for the user is different from the password of the cloned user configuration, you must generate new keys from the configured password before the SNMP manager attempts to communicate with the TAOS unit. Failure to generate a proper authentication and/or privacy key results in an authentication error.

Deleting an SNMPv3 USM user

Delete an SNMPv3 USM user by setting `usmUserStatus` to `rowStatusDestroy`.

Ascend SNMP-Framework and SNMP-User-Based MIB groups

The SNMP-Framework and SNMP-User-Based MIBs are registered with the Internet Assigned Numbers Authority (IANA).

RFC 2571: SNMP-Framework MIB groups

The SNMP-FRAMEWORK-MIB consists of the following SNMP engine groups:

- snmpEngineID
- snmpEngineBoots
- snmpEngineTime
- snmpEngineMaxMessageSize

SNMP Group	Description
snmpEngineID	An SNMP engine's unique administrative identifier. • **Syntax:** SnmpEngineID • **Access:** Read-only • **Status:** Mandatory

SNMP Group	Description
snmpEngineBoots	The number of times that the SNMP engine has started or restarted itself since the snmpEngineID was last configured. • **Syntax:** Integer (1 to 2147483647) • **Access:** Read-only • **Status:** Mandatory
snmpEngineTime	The number of seconds since the value of the snmpEngineBoots object last changed. If incrementing this objects value exceeds the maximum, snmpEngineBoots is incremented as if a restart occurred and the value reverts to zero. • **Syntax:** Integer (0 to 2147483647) • **Access:** Read-only • **Status:** Mandatory
snmpEngineMaxMessageSize	The maximum length in octets of an SNMP message that this SNMP engine can send, receive, or process. The message length is determined by message size values supported by all of the transports available by the engine. • **Syntax:** Integer (484 to 2147483647) • **Access:** Read-only • **Status:** Mandatory

RFC#2574: SNMP-USER-BASED-SM MIB groups

The SNMP-USER-BASED-SM MIB consists of the following SNMP engine groups:

- usmStatsUnsupportedSecLevels
- usmStatsNotInTimeWindows
- usmStatsUnknownUserNames
- usmStatsUnknownEngineIDs
- usmStatsWrongDigests
- usmStatsDecryptionErrors

SNMP Group	Specifies
usmStatsUnsupportedSecLevels	The total number of packets received by the SNMP engine that were dropped because the requested security level was either unknown or unavailable. • **Syntax:** Counter32 • **Access:** Read-only • **Status:** Mandatory

SNMP Group	Specifies
usmStatsNotInTimeWindows	This group provides information on the total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window. • **Syntax:** Counter32 • **Access:** Read-only • **Status:** Mandatory
usmStatsUnknownUserNames	The total number of packets received by the SNMP engine that were dropped because they referenced a user that was unknown to the SNMP engine. • **Syntax:** Counter32 • **Access:** Read-only • **Status:** Mandatory
usmStatsUnknownEngineIDs	The total number of packets received by the SNMP engine that were dropped because they referenced an snmpEngineID that was unknown to the SNMP engine. • **Syntax:** Counter32 • **Access:** Read-only • **Status:** Mandatory
usmStatsWrongDigests	The total number of packets received by the SNMP engine that were dropped because they contained an unexpected digest value. • **Syntax:** Counter32 • **Access:** Read-only • **Status:** Mandatory
usmStatsDecryptionErrors	The total number of packets received by the SNMP engine that were dropped because they could not be decrypted. • **Syntax:** Counter32 • **Access:** Read-only • **Status:** Mandatory

SNMPv3 notifications

TAOS units using TAOS 9.0 and higher now authenticate and encrypt Protocol Data Units (PDUs) as required by SNMPv3 and generate traps in SNMP version 2 (SNMPv2) Trap2 format. Depending on your configuration, a TAOS unit can send PDUs in SNMPv2 format or in pre-TAOS 9.0 format. You can specify the destinations for traps and the format of outgoing trap PDUs. In addition, two new MIBs—SNMP-TARGET-MIB and SNMP-NOTIFICATION-MIB—have been added. With SNMPv3 notifications support enabled you can configure the TAOS unit to perform the following tasks:

- Send SNMPv1 traps (Trap PDUs) or SNMPv2 Traps (Trap2 PDUs).
- Send traps to a specified IP address and port.
- Send Trap2 PDUs with different levels of security.

- Send Trap2 PDUs with different user names.

The SNMPv3 notifications feature follows the specifications in RFC 2573.

Configuring SNMPv3 notifications support

To set up SNMPv3 notifications support, you need to configure the SNMPv3-Notification profile, and the SNMPv3-Target-Param profile.

You must also configure new and existing parameters in the Trap profile. To configure these parameters from the CLI, you need to perform these steps in the following order.

- Create an SNMPv3-Notification profile, and set a tag to the profile.
- Create a SNMPv3-Target-Param profile.
- Set the message processing model to V1 or V3 option, and the security model to V1 or V3-USM option. If the V3-USM option is selected, set the security-name parameter to a valid SNMPv3-USM-User profile name.
- Create a Trap profile, and set the name, destination IP address, and destination port.
- Set the tag list. This tag list should contain tags that were set in the Notification profile. Multiple tags can be configured in this tag list, separated by spaces. Then, set the Target Param profile name to the `target-param` value.

  Note: All notification profiles in the system connect Trap profiles with matching tags. The parameters in the Trap profiles are used to send traps to the network.

Note: When you upgrade to software that supports the SNMPv3 notifications, the system automatically creates an SNMPv3-Notification profile and an SNMPv3-Target-Param profile; both are called `default`. SNMPv1 traps configured in an earlier version of the software are still generated when you upgrade. You need not create new profiles. However, removing or modifying the `default` profiles might affect the transmission of SNMPv1 traps.

Configuring an SNMPv3-Notification profile

Following is a listing of the new SNMPv3-Notification profile and its default settings:

```
admin> read snmpv3-notification
[in SNMPV3-NOTIFICATION/"" (new)]
    name* = ""
    active-enabled = no
    tag = ""
    type =
```

Set the following parameters:

Parameter	Specifies
Name	Unique name for the profile, up to 16 characters.
Active-Enabled	Whether the profile is used to generate notifications. Yes specifies that the profile is used to generate notifications. No (the default) specifies that it is not used to generate notifications.
Tag	Value that links the SNMPv3-Notification profile with the Trap profile specifying the host address to which notification messages are sent. You can specify up to 255 characters. The default is null.
Type	*Not currently implemented.*

Configuring an SNMPv3-Target-Param profile

Following is a listing of the new SNMPv3-Target-Param profile and its default settings:

```
[in SNMPV3-TARGET-PARAM/""]
    name* = ""
    active-enabled = no
    msg-proc-model = v1
    security-model = v1
    security-name =
    security-level = none
```

Set the following parameters:

Parameter	Specifies
Name	Unique name for the profile, up to 16 characters. The default is null.
Active-Enabled	Whether the profile is used to generate notifications. Yes specifies that the profile is used to generate notifications. No (the default) specifies that it is not used to generate notifications.
Msg-Proc-Model	Message-processing model to use when generating SNMP messages. V1 (the default) specifies SNMP version 1. V3 specifies SNMP version 3. For SNMPv3 Notifications support, specify V3.
Security-Model	Security model to use when generating SNMP messages. V1 (the default) specifies the SNMP version 1 security model. V3-USM specifies the SNMP version 3 User-based Security Model (USM). For SNMPv3 Notifications support, specify V3-USM. 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 for the SNMPv3-Target-Param profile to have any effect.
Security-Name	Security name that identifies the user on whose behalf SNMPv3 USM messages are generated. You can specify up to 22 characters. The default is null. Security-Name applies only if Security-Model is set to V3-USM.
Security-Level	Level of security to use when generating messages. None (the default) specifies no authentication and no privacy. Auth-NoPriv specifies authentication and no privacy. Auth-Priv specifies authentication and privacy. For Auth-Priv to apply, you must set the Priv-Protocol and Priv-Password parameters in the SNMPv3-USM-User profile.

Configuring a Trap profile

Following are the new parameters in the existing Trap profile and their default settings:

```
[in Trap/"" (new)]
    active-enabled = yes
    host-port = 162
    inform-time-out =
    inform-retry-count =
```

```
notify-tag-list = default
target-params-name = default
```

Set the following parameters:

Parameter	Specifies
Active-Enabled	Whether traps are sent to the host specified by the profile. Yes (the default) specifies that traps are sent. No specifies that traps are not sent.
Host-Address	IP address to which traps are sent. The default is 0.0.0.0.
Host-Port	Port to which traps are sent. Specify a number from 1 to 65535. The default is 162.
Inform-Time-Out	*Not currently implemented.*
Inform-Retry-Count	*Not currently implemented.*
Notify-Tag-List	List of the Tag value(s) in each SNMPv3-Notification profile.
Target-Params-Name	Value of the Name parameter in the SNMPv3-Target-Param profile, up to 22 characters.

For further information on these SNMPv3 Notifications parameters see the *APX 8000/MAX TNT Reference.*

Parameter references

This section contains complete descriptions of each new parameter you use to configure SNMPv3 Notifications. The descriptions are arranged in alphabetical order.

Parameter	Specifies
Active-Enabled	**Description:** In an SNMPv3-Notifications or SNMPv3-Target-Param profile, specifies whether the profile is used to generate notifications. In a Trap profile, specifies whether traps are sent to the host specified by the profile. **Usage:** Specify Yes or No. • Yes specifies that the profile is used to generate notifications or that traps are sent. • No (the default) specifies that the profile is not used to generate notifications or that traps are not sent. **Example:** `set active-enabled = yes`
Host-Port	**Description:** Specifies the port to which traps are sent. **Usage:** Specify a number from 1 to 65535. The default is 162. **Example:** `set host-port = 20`

Parameter	Specifies
Msg-Proc-Model	**Description:** Specifies the message-processing model to use when generating SNMP messages. **Usage:** Specify one of the following values: • V1 (the default) specifies SNMP version 1. • V3 specifies SNMP version 3. For SNMPv3 Notifications support, specify V3. **Example:** `set msg-proc-model = v3`
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 indicated in one or more SNMPv3-Notification profiles. **Example:** `set notify-tag-list = default1`
Security-Level	**Description:** Specifies the level of security to use when generating messages. **Usage:** Specify one of the following settings: • None (the default) specifies no authentication and no privacy. • Auth-NoPriv specifies authentication and no privacy. • Auth-Priv specifies authentication and privacy. **Example:** `set security-level = auth-priv`
Security-Model	**Description:** Specifies the security model to use when generating SNMP messages. **Usage:** Specify one of the following values: • V1 (the default) specifies the SNMP version 1 security model. • V3-USM specifies the SNMP version 3 User-Based Security Model (USM). For SNMPv3 Notifications support, specify V3-USM. **Example:** `set security-model = v3-usm`
Security-Name	**Description:** Specifies a security name that identifies the user on whose behalf SNMPv3 USM messages are generated. **Usage:** Specify up to 22 characters. The default is null. **Example:** `set security-name = newuser`
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`

Parameter	Specifies
Target-Params-Name	**Description:** Specifies the value indicated by the Name setting in the SNMPv3-Target-Param profile. **Usage:** Specify up to 22 characters. **Example:** **`set target-params-name = profile1`**

Changes to MIBs

The following sections describe changes to SNMP.

New MIBs

Two new MIBs are defined in the files `rfc2573_1.mib` and `rfc2573_2.mib`:

```
snmpTargetMIB MODULE-IDENTITY
    ORGANIZATION "IETF SNMPv3 Working Group"
    DESCRIPTION
        "This MIB module defines MIB objects which provide
         mechanisms to remotely configure the parameters used
         by an SNMP entity for the generation of SNMP messages."
    REVISION    "9808040000Z"
    DESCRIPTION "Clarifications, published as
                 RFC2573."
    REVISION    "9707140000Z"
    DESCRIPTION "The initial revision, published as RFC2273."
    ::= { snmpModules 12 }


snmpNotificationMIB MODULE-IDENTITY
    ORGANIZATION "IETF SNMPv3 Working Group"
    DESCRIPTION
        "This MIB module defines MIB objects which provide
         mechanisms to remotely configure the parameters
         used by an SNMP entity for the generation of
         notifications."
    REVISION    "9808040000Z"
    DESCRIPTION "Clarifications, published as
                 RFC2573"
    REVISION    "9707140000Z"
    DESCRIPTION "The initial revision, published as RFC2273."
    ::= { snmpModules 13 }
```

The `snmpTargetMIB` contains `snmpTargetObjects`.

`snmpTargetObjects` contains:

```
snmpTargetSpinLock
snmpTargetAddrTable
snmpTargetParamsTable
snmpUnavailableContexts
snmpUnknownContexts
```

`snmpTargetAddrTable` contains:

```
snmpTargetAddrName
snmpTargetAddrTDomain
snmpTargetAddrTAddress
snmpTargetAddrTimeout
snmpTargetAddrRetryCount
snmpTargetAddrTagList
snmpTargetAddrParams
snmpTargetAddrStorageType
snmpTargetAddrRowStatus
```

`snmpTargetParamsTable` contains:

```
snmpTargetParamsName
snmpTargetParamsMPModel
snmpTargetParamsSecurityModel
snmpTargetParamsSecurityName
snmpTargetParamsSecurityLevel
snmpTargetParamsStorageType
snmpTargetParamsRowStatus
```

`snmpNotificationMIB` contains `snmpNotifyObjects`.

`snmpNotifyObjects` contains `snmpNotifyTable`.

`snmpNotifyTable` contains:

```
snmpNotifyName
snmpNotifyTag
snmpNotifyType
snmpNotifyStorageType
snmpNotifyRowStatus
```

Trap2 PDU format

If configured, TRAP2 PDUs sent to the SNMP manager contain trap information as specified by RFC 1907. Trap OIDs are sent instead of generic and specific integers. Trap OIDs for generic traps are `snmpTraps.XX` where `XX` is the specific trap ID. OIDs for enterprise traps are `ascend.ascendNotifications.XX` where `XX` is the Ascend trap ID (as defined in `ascendv3.trp`). Other specific traps are sent with OIDs as defined in their respective MIBs.

Following are other common elements of the PDU and their values:

- `@ contextEngineID` is filled with `msgEngineID` as there is only one `snmpEngine` in the system that is identified by `msgEngineID`.
- `@ contextName` is filled with an empty string, for example `default context.`

A PDU is encrypted as specified in the corresponding profile SNMPv3-Target-Param. But if the security name specified in the profile does not have a corresponding USM user name in the system, outgoing PDUs are discarded and a log message with level `LOG_LEVEL_WARNING` generated.

Ascend enterprise MIBs

The enterprise MIB is registered with the IANA (Internet Assigned Numbers Authority) as `enterprises 529` with the value `1.3.6.1.4.1.529.`

Ascend MIB (ascend.mib)

The Ascend MIB consists of the following groups:

- products (1)
- slots (2)
- hostTypes (3)
- advancedAgent (4)
- lanTypes (5)
- doGroup (6)
- hostStatus (7)
- console (8)
- systemStatusGroup (9)
- eventGroup (10)
- callStatusGroup (11)
- sessionStatusGroup (12)
- radiusGroup (13)
- mCastGroup (14)
- lanModemGroup (15)
- firewallGroup (16)
- wanDialoutPkt (17)
- powerSupply (18)
- multiShelf (19)
- miscGroup (20)
- asgGroup (21)
- flashGroup (22)
- configuration (23)
- atmpGroup (24)
- srvcMgmtGroup (26)

Ascend Advanced Agent MIB (advanced.mib)

The TAOS unit supports the Ascend Advanced MIB, previously called the WAN MIB. The Advanced MIB defines objects related to WAN lines, channels, and ports.

The Advanced MIB includes `wanLineChannelUsageTable(29)`, immediately following `advancedAgent(4)`. The new table contains read-only integer variables that reflect the total count of B channels in any particular state for any given line usage. For example, you can use the table to retrieve the sum of all signaling channels (the number of connected calls) on all trunk lines, or to retrieve the sum of nailed, idle, or ringing channels, or the sum of connected DTPT channels on network (NT) lines.

The new table is indexed by the line usage and B channel state, as defined by the wanLineUsage and wanLineChannelState enumerations in advanced.mib. The MIB currently

identifies nine possible line usages and 24 B channel states, yielding a total of 216 new variables that represent the sum of all B channels in a given state for a given line usage.

Ascend Answer Profile MIB (mibanswer.mib)

Part of the Ascend MIB Configuration group (group 23), this MIB corresponds to the Answer-Defaults profile in the command line interface.

Ascend ATMP MIB (atmp.mib)

Enables you to configure and monitor Ascend Tunnel Management Protocol (ATMP) tunnels. For a complete description of ATMP, see RFC 2107, K. Hamzeh, "Lucent's Ascend Tunnel Management Protocol—ATMP."

Ascend Call MIB (call.mib)

Contains a table of entries for the status of each call in the system, including analog, digital, and Frame Relay-encapsulated calls. This MIB monitors the physical layer of the calls, including the slot and port. The Ascend Session MIB enables you to monitor the network layer of calls.

A number of new entries have been added to the `callStatus` and `callActive` tables in the Ascend Call MIB, making more information about the call available to the SNMP user.

The `callStatus` Table in the Ascend Call MIB includes the following new fields:

Field name	Reports
`callStatusCalledPartyID`	Called party number (if available).
`callStatusCallingPartyID`	Calling party number (if available). For outgoing calls, this field is set to null.
`callStatusMultiLinkID`	MP+ bundle ID for MP+ calls. For a non-MP+ call, this field is set to `0` (zero).

The `callActiveTable` in the Ascend Call MIB includes the following new fields:

Field name	Reports
`callActiveCalledParyID`	Called party number (if available).
`callActiveCallingPartyID`	Calling party number (if available). For outgoing calls, this field is set to null.
`callActiveMultiLinkID`	MP+ bundle ID for MP+ calls. For a non-MP+ call, this field is set to `0` (zero).

Ascend DS1 MIB (ds1.mib)

The DS1 MIB supports channelized T3 slot cards for individual T1 lines on the T3 card.

Ascend DS3 MIB (ds3.mib)

The DS3 MIB supports channelized T3 slot cards. TAOS units now support the following new values in the DS3 MIB for the Set commands:

- `dsx3LineType`
- `dsx3CircuitIdentifier`
- `dsxLoopbackConfig`

The T3 card has a new interface in the ifTable with the following values:

- `ifDescr—Channelize T3 Slot` *`slot/item`*
- `ifType—ds3(30)`
- `ifspeed—44736000`
- `ifName—ds3` *`shelf-slot-item`*
- `ifHighSpeed—45`
- `ifLinkUpDownTrapEnable—enabled(1)`
- `ifConnectorPresent—true(1)`

Note: To get these interface entries into the ifTable, enter the `slot -r` command to restart the T3 card and then initialize the slot again.

A link up/down trap is generated for the T3 line whenever the DS3 interface goes up or down.

Ascend DS3 Profile MIB (mibds3net.mib)

This MIB is part of the Ascend MIB Configuration group (group 23) and corresponds to the T3 profile in the command line interface.

Ascend Event MIB (event.mib)

This is a read-only MIB that includes connect progress and disconnect codes for calls. The MIB enables you to monitor the TAOS unit's events. In addition to displaying the idle time for an active session by using the `userstat -o %t` command, the same information is made available to SNMP management stations through the `ssnActiveIdleTime` object in the `sessionActiveTable`. The object uses Object ID `sessionActiveEntry.8`. Itshows the time the session has been idle in 0.01-second increments). Following is the object definition:

```
ssnActiveIdleTime   OBJECT-TYPE
    SYNTAX          TimeTicks
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "The time, current session has been idle.
                     For non-TNT and non-Max platforms 0 is always
                     reported."
    ::= { sessionActiveEntry 8 }
```

SNMP event MIB changes

When a TCP-Clear connection is successfully established, the login host's IP address is specified in the `eventUserIPAddress` object in the SNMP `callCleared` event. The

definition of the `eventUserIPAddress` object in the event MIB has been modified as follows:

```
eventUserIPAddress  OBJECT-TYPE
    SYNTAX          IpAddress
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "IP address of the remote user or login host.
    Applicable only if 'eventType' is serviceChanged(4)
    nameChanged(5) or callCleared. Value of a TCP-Clear
    login host IP address is returned once a TCP-Clear
    connection was successfully connected earlier in
    a serviceChanged event.
    The value 0.0.0.0 is returned if address is unknown
    or if not applicable."
::= { eventEntry 13 }
```

Syslog messages

When a TCP-Clear session is terminated, the login host's IP address is displayed instead of the zero address (0.0.0.0) in the Syslog message. For example:

```
[3/7/2/0] STOP: 'johnfan'; cause 11.; progress 43.; host 10.1.1.1
[MBID 2] [johnfan]
```

Userstat command output

For an active TCP-Clear session, the login host's IP address is displayed instead of the zero address (0.0.0.0) in the Userstat Address field. For example:

```
SessionID  Line/Chan   Slot:Item   Tx/Rx Rate  Svc Address     Username
286993415  3.01.08/012 3:07:03/000 26400/26400 TCP 10.1.1.1    johnfan

<end user list>  1 active user(s)
```

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

Ascend Firewall MIB (firewall.mib)

With this MIB you can dynamically configure Ascend Secure Access Firewalls that were created with Secure Access Manager (SAM). You can create or disable the firewall's dynamic rules.

Ascend Flash MIB (flash.mib)

The Ascend Flash MIB enables you to monitor the status of the TAOS unit's flash cards, store or retrieve configuration files, or format the flash cards.

The `flashOperationTftpPort` object has been added to the Ascend Flash MIB. This object adds the ability to configure the TFTP port setting for environments in which a network management station is running more than one management application, with a TFTP server local to each application.

The `flashOperationTftpPort` object is defined in the Flash MIB and used in the `load-config`, `save-config`, and `tftp-load` Flash MIB operations. The object's default setting is 69, which is the default port for TFTP operations. The object is defined as follows in the Flash MIB:

```
flashOperationTftpPort OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
    "This object defines the port # to use on the remote system
    when starting a TFTP operation using a flashOperationCommand. The
    default port is 69/(tcp/udp) Trivial File Transfer."
    ::= { flashOperation 8 }
```

The new Flash MIB has the following structure:

```
|-       1  flashDevice                 flashGroup.1
| |-     1  flashDevices                flashGroup.1.1
| \_     2  flashDeviceTable            flashGroup.1.2
|   \_   1  flashDeviceEntry            flashGroup.1.2.1
|     |- 1  flashDeviceSocket           flashGroup.1.2.1.1
|     |- 2  flashDeviceController       flashGroup.1.2.1.2
|     |- 3  flashDeviceControllerSocket flashGroup.1.2.1.3
|     |- 4  flashDeviceSize             flashGroup.1.2.1.4
|     |- 5  flashDeviceUsed             flashGroup.1.2.1.5
|     |- 6  flashDeviceState            flashGroup.1.2.1.6
|     |- 7  flashDeviceMaster           flashGroup.1.2.1.7
|     |- 8  flashDeviceFormatStatus     flashGroup.1.2.1.8
|     +- 9  flashDeviceDescription      flashGroup.1.2.1.9
|-       2  flashFileTable              flashGroup.2
| \_     1  flashFileEntry              flashGroup.2.1
|   |-   1  flashFileIndex              flashGroup.2.1.1
|   |-   3  flashFileSocket             flashGroup.2.1.3
|   |-   4  flashFileSize               flashGroup.2.1.4
|   |-   5  flashFileStatus             flashGroup.2.1.5
|   |-   6  flashFileName               flashGroup.2.1.6
|   |-   7  flashFileChecksum           flashGroup.2.1.7
|   |-   8  flashFileVersion            flashGroup.2.1.8
|   |-   9  flashFileAccess             flashGroup.2.1.9
|   +-   10 flashFileDateTimeStamp      flashGroup.2.1.10
\_       3  flashOperation              flashGroup.3
  |-     1  flashOperationStatus        flashGroup.3.1
  |-     2  flashOperationCommand       flashGroup.3.2
  |-     3  flashOperationHost          flashGroup.3.3
  |-     4  flashOperationDestFileName  flashGroup.3.4
  |-     5  flashOperationSrcFileName   flashGroup.3.5
  |-     7  flashOperationSocket        flashGroup.3.7
  |+-    8  flashOperationTftpPort      flashGroup.3.8
```

Ascend Frame Relay Profile MIB (mibfrmrl.mib)

The Ascend Frame Relay Profile MIB is part of the Ascend MIB Configuration group (group 23), and corresponds to the Frame-Relay profile in the command line interface.

Ascend Internet Profile MIB (mibinet.mib)

The Ascend Internet Profile MIB is part of the Ascend MIB Configuration group (group 23), and corresponds to the Connection profile in the command line interface.

Ascend Lan Modem MIB (lmodem.mib)

The Ascend Lan Modem MIB enables you to monitor the status of the TAOS unit's digital modems, including the number available, number of bad or suspect modems, and usage statistics. It also allows you to disable individual modems.

Ascend Multicast MIB (mcast.mib)

This read-only MIB enables you to view the status of the multicast heartbeat monitor.

Ascend Power Supply MIB (ps.mib)

This MIB manages the TAOS unit's power supplies.

Ascend Private MIB (private.mib)

This SNMP MIB provides support for the Layer 2 Tunneling Protocol (L2TP). Based on the Internet draft `draft-ietf-pppext-l2tp-mib-05`, the L2TP MIB is contained in the Ascend private MIB, `iso.org.dod.internet.private.enterprises.ascend`, using the identifier `tunnelGroup.asndL2tp`.

TAOS 9.0 implements this MIB with the following limitations:

- Some variables are currently unavailable.
- The `TunnelIfIndex` currently has no related interface in the interface MIB.
- Some counters return a zero.

The following portions of the MIB are implemented in TAOS 9.0 as read-only:

```
l2tpConfig:
    -l2pAdminState
l2tpStats:
    - l2tpProtocolVersion
    - l2tpVendorName
    - l2tpFirmwareRevision
l2tpDomainStatsTable:
    - l2tpDomainStatsIdentifier
    - l2tpDomainStatsTotalTunnels
    - l2tpDomainStatsFailedTunnels
    - l2tpDomainStatsFailedAuthentications
    - l2tpDomainStatsActiveTunnels
    - l2tpDomainStatsTotalSessions
    - l2tpDomainStatsFailedSessions
    - l2tpDomainStatsActiveSessions
```

The remaining counters are currently returned as zero:

```
l2tpTunnelStatsTable:
    - l2tpTunnelStatsIfIndex
    - l2tpTunnelStatsLocalTID
    - l2tpTunnelStatsRemoteTID
    - l2tpTunnelStatsState
    - l2tpTunnelStatsInitiated
    - l2tpTunnelStatsRemoteHostName
    - l2tpTunnelStatsRemoteVendorName
    - l2tpTunnelStatsRemoteFirmwareRevision
    - l2tpTunnelStatsRemoteProtocolVersion
    - l2tpTunnelStatsInitialRemoteRWS
    - l2tpTunnelStatsBearerCapabilities
    - l2tpTunnelStatsFramingCapabilities
    - l2tpTunnelStatsTotalSessions
    - l2tpTunnelStatsActiveSessions
l2tpSessionStatsTable:
    - l2tpSessionStatsTunnelIfIndex
    - l2tpSessionStatsLocalCID
    - l2tpSessionStatsRemoteCID
    - l2tpSessionStatsUserName
    - l2tpSessionStatsState
    - l2tpSessionStatsCallType
    - l2tpSessionStatsCallSerialNumber
    - l2tpSessionStatsTxConnectSpeed
    - l2tpSessionStatsRxConnectSpeed
    - l2tpSessionStatsCallBearerType
    - l2tpSessionStatsFramingType
    - l2tpSessionStatsDNIS (*)
    - l2tpSessionStatsCLID (*)
    - l2tpSessionStatsSubAddress (*)
    - l2tpSessionStatsPrivateGroupID (**)
    - l2tpSessionStatsProxyLcp
    - l2tpSessionStatsAuthMethod
    - l2tpSessionStatsSequencingState
    (*)  LNS only
    (**) not available at this time in TAOS
```

Ascend RADIUS MIB (radius.mib)

The Ascend Radius MIB enables you to view the status of Ascend RADIUS accounting and authentication servers, including client requests and the servers' responses. You can also use this MIB to mark a RADIUS server as the current server.

Ascend Remote Ping MIB (remoteping.mib)

Ping MIBs allow the creation of Ping tests that periodically issue a series of operations and generate traps or event notifications to report test results.

Supported tables

TAOS units support the following tables in the Remote Ping MIB:

- Ping Control Table (`pingCtlTable`)
- Ping Results Table (`pingResultsTable`)

Supported traps

TAOS units support the following traps (event notifications) in the Remote Ping MIB:

- `pingProbeFailed`. Generated when a probe failure is detected.
- `pingTestFailed`. Generated when a Ping test fails.
- `pingTestCompleted`. Generated at the completion of a Ping test.

Changes to the Remote Ping MIB

The following changes are made to the standard MIB:

- All the definitions have been changed for compliance with SNMPv1 Structure of Management Information (SMI).
- The syntax MAX-ACCESS has been changed to ACCESS for all the fields.
- All the MIB fields that had a STATUS value of Current have been assigned the Mandatory value instead.
- Fields with read-create access were changed to read-write.

Currently, you cannot modify the following variables, so they have been changed to read-only:

- `pingMaxConcurrentRequests`
- `pingCtlDataFill`
- `pingCtlMaxRows`
- `pingCtlStorageType`
- `pingCtlType`
- `pingCtlIfIndex`
- `pingCtlByPassRouteTable`

The `pingProbeHistoryTable` in the Remote Ping MIB is not supported in TAOS 9.0.

Ascend Resources MIB (resource.mib)

The Ascend Resources MIB enables you to report utilization and availability details about terminating access resources such as modems, HDLC channels, and MultiDSP devices.

For cards that support `resourceUsageTable` and `resourceTable` in `resource.mib`, the system can report utilization details such as the number of active, available, disabled, suspect, or inoperable devices. This information can be useful for capacity planning and resource management. The system also reports the percentage of available modems, HDLC channels, or DSPs within a device or device group, to enable immediate detection of modem, HDLC, or DSP failure.

The following host cards support this feature:

- Series56 II, and Series56 III Digital Modem
- MutiDSP
- Hybrid Access (HDLC2-EC)

The following object has been added to the Ascend Enterprise MIB (`ascend.mib`):

```
resourcesGroup OBJECT IDENTIFIER ::= { ascend 27 }
```

Ascend Service Management MIB (srvcmgmt.mib)

The Ascend Service Management MIB enables you to manage Dialed Number Information Service (DNIS) services on the TAOS unit. When the DNIS management mode is enabled, Network Management Stations (NMS) such as NavisAccess manages the TAOS unit's modem and HDLC resources.

Ascend Session MIB (session.mib)

The Ascend Session MIB contains a table of entries for the status of each session in the system, including the IP address, type of session (PPP, MPP, Telnet, and so on), and MPP statistics.

Ascend UDS3 Profile MIB (mibuds3net.mib)

The Ascend UDS3 Profile MIB corresponds to the UDS3 profile in the command line interface and is part of the Ascend MIB Configuration group (group 23).

Ascend WAN Dialout MIB (wandialout.mib)

The Ascend WAN Dialout enables you to monitor the packets a TAOS unit receives that causes it to dialout.

Lucent Chassis MIB (chassis.mib)

The Lucent Chassis MIB enables you to monitor the chassis of TAOS units.

Modified method for adding SNMP object IDs

Previously, algorithms used to assign Object IDs to new MIB members could result in dictionary conflicts across TAOS platforms and software versions. New methodologies make

such conflicts much less likely. The MIB files distributed with the TAOS unit's ensure that SNMP managers begin using the newer dictionaries that will be maintained across future upgrades.

Ascend Enterprise traps

Defines Ascend-specific traps that alert NMS when certain events have occurred on the TAOS unit, such as when a Telnet session fails to authenticate, the TAOS unit is reset, or a Frame Relay DLCI is brought up or torn down.

Configuring SNMP access and security

The SNMP profile contains SNMP-readable information related to the unit itself and its SNMP security. There are two levels of security: community strings, which must be known by a community of SNMP managers to access the box, and address security, which excludes SNMP access unless it is initiated from a specified IP address.

These are the related parameters:

```
SNMP
   enabled = no
   read-community = public
   read-write-community = write
   enforce-address-security = no
   read-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 ]
   write-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 ]
   contact = ""
   location = ""
```

SNMP profile configuration overview

Table 6-2 provides some background information on tasks you may need to perform to configure SNMP on the TAOS unit. For complete details on each parameter, see the *APX 8000/MAX TNT Reference*.

Table 6-2. SNMP profile configuration tasks

Task	Description
Enabling SNMP access	If the enabled parameter in the SNMP profile is set to No (the default), the TAOS unit cannot be accessed by SNMP utilities.
Setting community strings	The read-community parameter specifies the SNMP community name for read access (up to 32 characters), and the read-write-community parameter specifies SNMP community name for read/write access.

Table 6-2. SNMP profile configuration tasks (continued)

Task	Description
Setting up and enforcing address security	If the enforce-address-security parameter is set to No (its default value), any SNMP manager that presents the right community name will be allowed access. If it is set to Yes, the TAOS unit checks the source IP address of the SNMP manager and allows access only to those IP addresses listed in the read-access-host and write-access-host arrays. Each array can include up to five host addresses.
Specifying who to contact about problems and the location of the unit	The contact and location fields are SNMP readable and settable, and should indicate the person to contact about this unit, and its location.
Specifying a queue depth	The default queue depth for SNMP requests is zero, which means the packets will not be dropped, no matter how busy the SNMP subsystem gets. If the queue were to grow too large in an extremely loaded routing environment, the system could ultimately run out of memory. Valid values for the queue depth are 0–1024.

Sample SNMP profile configuration

The sample configuration enables SNMP access, enforces address security, and prevents write access:

```
admin> read snmp
SNMP read

admin> list

enabled = no
read-community = public
read-write-community = write
enforce-address-security = no
read-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 ]
write-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 ]
contact = ""
location = ""
admin> set enabled = yes
admin> set enforce-address-security = yes
admin> set read-access 1 = 10.2.3.4
admin> set read-access 2 = 10.2.56.123
admin> set queue-depth = 32
admin> write
SNMP written
```

Administering Read or Write Host Permissions

Before TAOS 9.0, you could specify up to five SNMP managers with Read or Write permission. You can specify up to eight SNMP managers in TAOS 9.0.

Reference descriptions

Following are the descriptions for the Read-Access-Hosts and Write-Access-Hosts parameters in the SNMP profile. For further information on Read and Write Host Permissions see the *APX 8000/MAX TNT Reference*.

Parameter	Specifies
Read-Access-Hosts	An array containing up to eight IP addresses of SNMP managers that have Read permission. If Enforce-Address-Security is set to Yes, the TAOS unit responds to SNMP Get and Get-Next commands only from the SNMP managers you specify in the array. You must set the Enforce-Address-Security parameter to Yes in the SNMP profile for the Read-Access-Hosts setting to have any effect.
Write-Access-Hosts	An array specifying up to eight IP addresses of SNMP managers with Write permission. The TAOS unit responds to SNMP Set, Get, and Get-Next commands from only the SNMP managers you specify. For the Write-Access-Hosts setting to restrict read-write access to the TAOS unit, you must set the Enforce-Address-Security parameter to Yes in the SNMP profile.

Setting up SNMP traps

An SNMP trap (event notification) is a mechanism for reporting system change in real time, such as reporting an incoming call. When a trap is generated by some condition, a traps-PDU (protocol data unit) is sent across the Ethernet to the SNMP manager.

You can configure the TAOS unit to send traps to an SNMP manager by specifying the address of the manager in a Trap profile. Traps can be enabled or disabled by class (error events, port state change events, or security events) or individually.

The following parameters relate to setting SNMP traps:

```
TRAP
   host-name* = ""
   community-name = ""
   host-address = 0.0.0.0
   alarm-enabled = yes
   security-enabled = no
   port-enabled = no
   slot-enabled=no
```

For details on the actual events that generate traps in the various classes, see the Ascend Enterprise MIB, or see the *APX 8000/MAX TNT Reference*.

TAOS unit trap support

The TAOS unit does not support the `systemUseExceeded` trap.

Port-State change events are currently not applicable to the TAOS unit. These include:

- portInactive
- portDualDelay
- portWaitSerial
- portHaveSerial
- portRinging
- portCollectDigits
- portWaiting
- portConnected
- portCarrier
- portLoopback
- portAcrPending
- portDteNotReady
- portUseExceeded

In addition, the TAOS unit does not support billing features that include these traps:

- portUseExceeded
- systemUseExceeded

Individual SNMP traps

Individual traps are enabled by default. The following parameters determine which traps are forwarded to an SNMP manager:

Parameter	Specifies
Slot-Enabled	The system generates a trap when a slot card is brought up or down.

Parameter	Specifies

Slot-Card-Reset-Enabled	An SNMP user can view the Fatal Log table, and the TAOS unit can inform the user of a reason for a restart when one is available. The following SNMP elements have been introduced to support this feature:
	• The `fatalLogTable` object
	• The `slotCardResetTrap` trap
	
	The `sysLastRestartReasonTrap` include `fatalLogIndex` and `sysAbsoluteCurrentTime` in its definition:
	
	`sysLastRestartReasonTrap TRAP-TYPE`
	`ENTERPRISE ascend`
	`VARIABLES { sysLastRestartReason, fatalLogIndex,`
	`sysAbsoluteCurrentTime }`
	`DESCRIPTION "This trap is sent to all managers having the`
	`alarm condition enabled if the`
	`sysLastRestartReason is not unknown`
	`(value of 0)."`
	`::= 26`
	
	A new `slotCardResetTrap` trap has been defined to inform the MIB manager that a slot card has been reset:
	
	`slotCardResetTrap TRAP-TYPE`
	`ENTERPRISE ascend`
	`VARIABLES { fatalLogIndex, fatalLogReason,`
	`sysAbsoluteCurrentTime, slotIndex }`
	`DESCRIPTION "This trap is sent to all managers having the`
	`alarm condition enabled"`

Coldstart-Enabled	The system generates a trap when the TAOS unit reinitializes itself such that the configuration of the SNMP manager or the system itself might be altered.
Warmstart-Enabled	The system generates a trap when the TAOS unit reinitializes itself such that neither the configuration of SNMP manager or the system itself is altered.
Linkdown-Enabled	The system generates a trap when a failure occurs in a communication link between the unit and the SNMP manager.
Linkup-Enabled	The system generates a trap when the communication link between the unit and the SNMP manager comes back up.
Ascend-Enabled	(Also known as the Ascend Enterprise trap.) When both this parameter and Port-Enabled are set to Yes, a trap is generated to indicate a change of state in a host interface. All port connections are monitored in a state machine and reported via this trap.

Parameter	Specifies
Call-Log-Dropped-Pkt-Enabled	If enabled (the default), 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). SNMP management stations can obtain the value of the variable at any time by using SNMP Get.
Console-Enabled	The system generates a trap when the console has changed state. The console entry can be read to see what its current state is.
Console-State-Change	The SNMP agent on the TAOS sends the console's IP address in addition to the console index in the Console-State-Change trap. The Console-State-Change trap carries the information displayed in the following example: `1999-07-02 12:07:26 eng-fast-4.ascend.com [192.168.25.4] enterprises.529: Enterprise Specific Trap (12)Uptime:0:16:43 enterprises.529.8.2.1.1.2=2 enterprises.529.12.2.1.4.2=IpAddress:10.40.40.133`
Config-Change-Enabled	Enables or disables the configuration-change trap (Trap 30). The trap is enabled by default, which causes the system to issue the trap whenever the system configuration is modified or a new software version is loaded. If the parameter is set to `no`, the system does not issue the trap for those events. An SNMP management station can receive a Trap (30) and a string containing the date, time, and information about the user that changed the configuration.
OSPF-Set-Trap-Enabled	For an OSPF trap to be generated when the trap condition occurs, OSPF traps must be enabled, either in the Trap profile or by setting the corresponding bit in the new MIB object, `ospfSetTrap`, defined in RFC 1850.
Use-Exceeded-Enabled	The system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it, or the system DS0 usage has been exceeded.
Password-Enabled	When both this parameter and Security-Enabled are set to Yes, all failed Telnet login attempts generate a trap.
FR-Linkup-Enabled	If both this parameter and Alarm-Enabled are set to Yes, a trap is sent whenever a DLCI is brought up.
FR-Linkdown-Enabled	If both this parameter and Alarm-Enabled are set to Yes, a trap is sent whenever a DLCI is brought down.
Event-Overwrite-Enabled	The system generates a trap when a new event has overwritten an unread event. This trap is sent only for systems which support the Ascend accounting MIB. Once sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events have occurred.
RADIUS-Change-Enabled	The system generates a trap when a new RADIUS server is being accessed. This trap returns the objectID and IP address of the new server.

Parameter	Specifies
Suspect-Access-Resource-Enabled	**Description:** Specifies that whenever a terminating modem has received four successive calls for which it cannot establish a connection, the unit sends a trap to all SNMP managers in the alarm group. Once the managing TAOS unit sends the trap, the suspect modem is not assigned to terminate calls until all available resources are exhausted. For example, if a modem drops five calls, the system generates the trap and places the offending modem at the end of the list of available terminating resources. **Usage:** Specify one of the following values: • `yes` directs the TAOS to send the `suspectAccessResource` trap when a terminating modem card has received four or more calls for which it could not establish a connection. • `no` instructs the TAOS not to send the `suspectAccessResource` trap. Example: **`set suspect-access-resource-enabled = yes`** **Dependencies:** The Suspect-Access-Resource-Enabled parameter has an effect only on TAOS units with one or more of the following slot cards installed: • Series56 II, and Series56 III Digital Modem • MultiDSP **Location:** Trap
Mcast-Monitor-Enabled	The system generates a trap when multicast heartbeat monitoring is configured and the system did not receive the configured number of heart-beat packets on a multicast interface.
LAN-Modem-Enabled	The system generates a trap when a digital modem is moved to the suspect list.
Dirdo-Enabled	The system generates a trap when a T-Online call comes in and no answer/subaddress has been received.
Slot-Profile-Change-Enabled	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 states.
Power-Supply-Enabled	The system generates a trap when a power supply module is added or removed.
Authentication-Enabled	The system generates a trap when an authentication failure occurs.

Activating the SNMP agent

Access to the SNMP agent is protected by community strings. The NMS software must supply the community strings to access the TAOS unit. In addition, you can use address security to

exclude SNMP access from host addresses other than those you have specified. Address security is optional but recommended.

Following are the relevant parameters, shown with default settings:

```
[in SNMP]
enabled = no
read-community = public
read-write-enabled = no
read-write-community = write
enforce-address-security = no
read-access-hosts 1 = 0.0.0.0
read-access-hosts 2 = 0.0.0.0
read-access-hosts 3 = 0.0.0.0
read-access-hosts 4 = 0.0.0.0
read-access-hosts 5 = 0.0.0.0
read-access-hosts 6 = 0.0.0.0
read-access-hosts 7 = 0.0.0.0
read-access-hosts 8 = 0.0.0.0
write-access-hosts 1 = 0.0.0.0
write-access-hosts 2 = 0.0.0.0
write-access-hosts 3 = 0.0.0.0
write-access-hosts 4 = 0.0.0.0
write-access-hosts 5 = 0.0.0.0
write-access-hosts 6 = 0.0.0.0
write-access-hosts 7 = 0.0.0.0
write-access-hosts 8 = 0.0.0.0
contact = ""
location = ""
queue-depth = 0
csm-modem-diag = no
snmp-message-type = v1-and-v3
security-level = none
```

For details about these parameters, see the *APX 8000/MAX TNT Reference*.

Activating the agent

To activate the SNMP agent, set the `enabled` parameter to yes. To avoid a security lapse, immediately change the default setting for the `read-community` string. Proceed as follows:

```
admin> read snmp
SNMP read

admin> set enabled = yes

admin> set read-community = securestring

admin> write
SNMP written
```

Enabling read-write access

When you enable read-write access, immediately change the read-write community string from the well-known `write` value, to prevent a security lapse. Proceed as follows:

```
admin> set read-write-enabled = yes

admin> set read-write-community = securestring
```

```
admin> write
SNMP written
```

Setting up address security

To set up address security, set the `enforce-address-security` parameter to `yes` and set `read-access-hosts` *`N`* and `write-access-hosts` *`N`* parameters to specify the hosts that have access to the TAOS unit. For example, the following commands give read/write access to one host and read-only access to another:

```
admin> set enforce-address-security = yes
admin> set read-access-hosts 1 = 1.1.1.1
admin> set read-access-hosts 2 = 2.2.2.2
admin> set write-access-hosts 1 = 1.1.1.1
admin> write
SNMP written
```

Access from any other IP addresses is denied.

Activating SNMP traps

TAOS units generate traps (notifications) for important events. When a trap is generated by some condition, a trap protocol data unit (PDU) is sent to a specified host. You enable traps and specify their destinations by modifying the Trap profile. You cannot configure traps through SNMP.

Following are the Trap parameters, shown with default settings:

```
[in TRAP/""]
host-name* = ""
active-enabled = yes
community-name = ""
host-address = 0.0.0.0
host-port = 162
inform-time-out = 1500
inform-retry-count = 4
notify-tag-list = default
target-params-name = default
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
```

```
lan-modem-enabled = yes
slot-profile-change-enabled = yes
power-supply-enabled = yes
authentication-enabled = yes
config-change-enabled = yes
sys-clock-drift-enabled = yes
suspect-access-resource-enabled = yes
watchdog-warning-enabled = yes
controller-switchover-enabled = no
call-log-serv-change-enabled = yes
wan-line-state-change-enabled = yes
call-log-dropped-pkt-enabled = yes
lim-sparing-enabled = no
interface-sparing-enabled = no
secondary-controller-state-change-enabled = no
pctfi-trunk-status-change-enabled = yes
no-resource-available-enabled = yes
dsl-thresh-trap-enabled = no
atm-pvc-failure-trap-enabled = no
```

For details about these parameters, see the *APX 8000/MAX TNT Reference*.

Specifying trap destinations

The following sample commands instruct the unit to send traps to an SNMP manager at the IP address 1.1.1.1:

```
admin> new trap test
TRAP test read

admin> set host-address = 1.1.1.1

admin> write
TRAP test written
```

If the host address is zero and a name service such as the Domain Name System (DNS) or Network Information Service (NIS) is supported, you can specify the hostname instead. The system uses the name to look up the host address.

Trap classes

Traps are grouped into classes: alarm events, security events, and port or slot state change events. These classes allow for enabling or disabling sets of traps. When a trap class is enabled, you can enable or disable individual traps within the class.

Note: Enabling an individual trap has no effect if the trap class to which it belongs is not enabled.

Alarm class traps

By default, the alarm class is enabled. For the TAOS unit to send one or more of the traps listed in Table 6-3, the following parameter must be set to `yes`:

```
[in TRAP/""]
alarm-enabled = yes
```

If the `alarm-enabled` parameter is set to `no`, the unit does not send any of the traps listed in Table 6-3.

Table 6-3. Traps in the alarm class

Trap	Parameter that enables/disables this individual trap
ColdStart	coldstart-enabled
WarmStart	warmstart-enabled
LinkDown	linkdown-enabled
LinkUp	linkup-enabled
FRLinkUp	fr-linkup-enabled
FRLinkDown	fr-linkdown-enabled
EventOverwrite	event-overwrite-enabled
LanModem	lan-modem-enabled
PowerSupply	power-supply-enabled
ConfigChange	config-change-enabled
SysClockDrifted	sys-clock-drift-enabled
SuspectAccessResrc	suspect-access-resource-enabled
WatchdogWarning	watchdog-warning-enabled
Controllerswitchover	controller-switchover-enabled
WanLineStateChange	wan-line-state-change-enabled
CallLogDroppedPkt	call-log-dropped-pkt-enabled
limSparing	lim-sparing-enabled
interfaceSparing	interface-sparing-enabled
CntrReduAvail	secondary-controller-state-change-enabled
NoResourceAvailable	no-resource-available-enabled
dslThreshTrap	dsl-thresh-trap-enabled
atmPvcFailureEnabled	atm-pvc-failure-trap-enabled
slotCardReset*	N/A
sysLastRestartReason*	N/A
AdslInitFailureTrap*	N/A

* You cannot disable these traps individually. They are always sent when the corresponding event occurs and alarm class traps are enabled.

Security class traps

By default, the security class is disabled. For the TAOS unit to send one or more of the traps listed in Table 6-4, the following parameter must be set to `yes`:

```
[in TRAP/""]
security-enabled = yes
```

If the `security-enabled` parameter is set to `no`, the unit does not send any of the traps listed in Table 6-4.

Table 6-4. Traps in the security class

Trap	Parameter that enables/disables this individual trap
`Authentication`	`authentication-enabled`
`Console`	`console-enabled`
`UseExceeded`	`use-exceeded-enabled`
`Password`	`password-enabled`
`RadiusChange`	`radius-change-enabled`
`CallLogServChange`	`call-log-serv-change-enabled`

Port class trap

By default, the port class is disabled. For the TAOS unit to send the trap listed in Table 6-5, the following parameter must be set to `yes`:

```
[in TRAP/""]
port-enabled = yes
```

If the `port-enabled` parameter is set to `no`, the unit does not send the trap listed in Table 6-5.

Table 6-5. Trap in the port class

Trap	Parameter that enables/disables this individual trap
`Ascend`	`ascend-enabled`

Slot class trap

By default, the slot class is disabled. For the TAOS unit to send the trap listed in Table 6-6, the following parameter must be set to `yes`:

```
[in TRAP/""]
slot-enabled = yes
```

If the `slot-enabled` parameter is set to `no`, the unit does not send the trap listed in Table 6-6.

Table 6-6. Trap in the slot class

Trap	Parameter that enables/disables this individual trap
SlotProfileChange	slot-profile-change-enabled

Examples of enabling traps and trap classes

The following commands cause the system to send trap PDUs when line interface module (LIM) redundancy takes effect, the secondary controller becomes primary, a digital subscriber line (DSL) threshold is reached, and a permanent virtual circuit (PVC) failure occurs. Note that the `alarm-enabled` parameter must be set to `yes` for the system to send these traps.

```
admin> set lim-sparing-enabled = yes
admin> set secondary-controller-state-change-enabled = yes
admin> set dsl-thresh-trap-enabled = yes
admin> set atm-pvc-failure-trap-enabled = yes
admin> write
TRAP test written
```

The following commands enable security class traps:

```
admin> set security-enabled = yes
admin> write
TRAP test written
```

RFC 1850 OSPF traps

TAOS units support OSPF traps as defined in RFC 1850, *OSPF Version 2 Management Information Base.* For an OSPF trap to be generated when the trap condition occurs, OSPF traps must be enabled, either in the Trap profile or by setting the corresponding bit in the new MIB object, `ospfSetTrap`, defined in RFC 1850. In addition, the individual trap that represents the trap condition must be enabled.

Overview of trap definitions

Following are the relevant parameters (shown with default values) in an ospfSet Trap profile:

```
[in TRAP/""]
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
```

Parameter	Specifies
OSPF-enabled	Enable/disable generation of OSPF traps. When set to `no` (the default), no OSPF traps are generated regardless of individual OSPF trap settings in the profile. When set to `yes`, trap generation depends on whether the specific OSPF trap is enabled.
OSPF-if-config-error-enabled	Enable/disable trap generation if a packet has been received on a nonvirtual interface from a router whose configuration conflicts with this router's configuration. The system generates this trap when it detects configuration error types from 1 to 9, as defined in RFC 1850. Generation of the trap typically indicates a failure to form an adjacency, although this is not always the case. Traps for error type 10 (optionsMismatch) are not currently supported. (OSPF Trap 4)
OSPF-if-auth-failure-enabled	Enable/disable trap generation if a packet has been received on a nonvirtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. (OSPF Trap 6)
OSPF-if-state-change-enabled	Enable/disable trap generation if the state of a nonvirtual OSPF interface has changed. 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). (OSPF Trap 16)
OSPF-if-rx-bad-packet	Enable/disable trap generation if an OSPF packet has been received on a nonvirtual interface that cannot be parsed. (OSPF Trap 8)
OSPF-tx-retransmit-enabled	Enable/disable trap generation if an OSPF packet has been retransmitted on a nonvirtual interface. 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. (OSPF Trap 10)
OSPF-nbr-state-change-enabled	Enable/disable trap generation if the state of a nonvirtual OSPF neighbor has changed. This trap 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 an 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. (OSPF Trap 2)

Parameter	Specifies
OSPF-virt-if-config-error-enabled	Enable/disable trap generation if a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. The system generates this trap when it detects configuration error types from 1 to 9, as defined in RFC 1850. Generation of the trap typically indicates a failure to form an adjacency, although this is not always the case. Traps for error type 10 (optionsMismatch) are not currently supported. (OSPF Trap 5)
OSPF-virt-if-auth-failure-enabled	Enable/disable trap generation if a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. (OSPF Trap 7)
OSPF-virt-if-state-change-enabled	Enable/disable trap generation if the state of an OSPF virtual interface has changed. (OSPF Trap 1)
OSPF-virt-if-rx-bad-packet	Enable/disable trap generation if an OSPF packet has been received on a virtual interface that cannot be parsed. (OSPF Trap 9)
OSPF-virt-if-tx-retransmit-enabled	Enable/disable trap generation if an OSPF packet has been retransmitted on a virtual interface. All packets that are retransmitted are associated with an LSDB entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry. (OSPF Trap 11)
OSPF-virt-nbr-state-change-enabled	Enable/disable trap generation if the state of an OSPF virtual neighbor has changed. (OSPF Trap 3)
OSPF-originateLsa-enabled	Enable/disable trap generation if a new LSA has been originated by this router due to a topology change. (OSPF Trap 12)
OSPF-maxAgeLsa-enabled	Enable/disable trap generation if an LSA in the router's link-state database has aged to MaxAge. (OSPF Trap 13)
OSPF-lsdb-overflow-enabled	Enable/disable trap generation if the number of LSAs in the router's link-state database has exceeded OSPFExtLsdbLimit. (OSPF Trap 14)
OSPF-approaching-overflow-enabled	Enable/disable trap generation if the number of LSAs in the router's link-state database has exceeded 90 percent of OSPFExtLsdbLimit. (OSPF Trap 15)

Example of setting traps in the Trap profile

The following commands cause the system to generate traps when the router receives a packet from an OSPF router in which a configuration mismatch (such as an invalid OSPF version number or an address conflict) or an authentication failure occurs:

```
admin> read trap monitor-ospf
TRAP/monitor-ospf read

admin> set ospf-enabled = yes

admin> set ospf-if-config-error-enabled = yes

admin> set ospf-if-auth-failure-enabled = yes
```

```
admin> write
TRAP/monitor-ospf written
```

SNMP support for OSPF traps

In addition to the Trap profile changes, a new MIB (`rfc1850.mib`) is distributed as part of this release. Management stations and browsers used to manage OSPF load `rfc1850.mib` instead of the old `rfc1253.mib`. A new MIB object, `ospfSetTrap` is defined according to RFC 1850 for enabling trap events:

```
.iso.org.dod.internet.mgmt.mib-2. ospf.ospfTrap.ospfTrapCon-
trol.ospfSetTrap
```

This object defaults initially to the octet string `{'\0x0', '0x0', '0x0', '0x0'}` (or the hex value 0x0), which disables all trap events. The value of this object is stored in NVRAM.

SNMP support for the Idle Time variable

In addition to displaying the idle time for an active session by using the `userstat -o %t` command, the same information is made available to SNMP management stations through the `ssnActiveIdleTime` object in the `sessionActiveTable`. The object uses Object ID `sessionActiveEntry.8`. It shows the time the session has been idle in 0.01-second increments). Following is the object definition:

```
ssnActiveIdleTime   OBJECT-TYPE
    SYNTAX          TimeTicks
    ACCESS          read-only
    STATUS          mandatory
    DESCRIPTION     "The time, current session has been idle.
                     For non-TNT and non-Max platforms 0 is always
                     reported."
    ::= { sessionActiveEntry 8 }
```

SNMP trap configuration overview

Table 6-7 provides some background information about tasks you might need to perform to configure the TAOS unit to send SNMP traps. For complete details on each parameter, see the *APX 8000/MAX TNT Reference*.

Table 6-7. SNMP trap configuration tasks

Task	Description	Associated parameters
Specifying the host running the SNMP manager	The Host-Name field is the index for the Trap profile, so it must contain a name. If DNS or YP/NIS is supported, it can contain the hostname of a system running an SNMP manager. If the host-address field contains an IP address, the specified name is not used to actually locate the host. The host-address can specify an IP address of the destination host. If DNS or YP/NIS is not supported, it must contain the host's address.	Host-Name

Table 6-7. SNMP trap configuration tasks (continued)

Task	Description	Associated parameters
The community string for communicating with the SNMP manager	The community name field must contain the community name associated with the SNMP PDU.	Community-Name
Classes of traps to be sent to the specified host	The next three fields specify whether the TAOS unit traps alarm events, security events, and port events and sends a trap-PDU to the SNMP manager. For a description of the events that generate these traps, see the *APX 8000/MAX TNT Reference*.	Alarm-Enabled Security-Enabled Port-Enabled
Individual traps to be sent to the specified host	In addition to enabling whole classes of traps, you can specify individual SNMP traps to forward to an SNMP manager. Individual traps are enabled by default.	Slot-Enabled Coldstart-Enabled Warmstart-Enabled Linkdown-Enabled Linkup-Enabled Ascend-Enabled Console-Enabled Use-Exceeded-Enabled Password-Enabled FR-Linkup-Enabled FR-Linkdown-Enabled Event-Overwrite-Enabled RADIUS-Change-Enabled Mcast-Monitor-Enabled LAN-Modem-Enabled Dirdo-Enabled Slot-Profile-Change-Enabled Power-Supply-Enabled Multishelf-Enabled Authentication-Enabled

Example SNMP trap configuration

In the following example, the host-name is used only as a profile index, not to locate the actual host on the network. A community name is specified, security-class traps are added to the default alarm-class traps, and this host receives a trap if the multishelf link goes down.

```
admin> new trap
TRAP/"" read
admin> list
host-name* = ""
community-name = ""
host-address = 0.0.0.0
alarm-enabled = yes
security-enabled = no
port-enabled = no
slot-enabled = no

admin> set host-name = security-traps
```

```
admin> set community-name = Ascend
admin> set host-address = 10.2.3.4
admin> set security-enabled = yes
admin> set slot-enabled = yes
admin> write
TRAP/security-traps written
```

Because security traps and the Password-Enabled and Authentication-Enabled individual traps are enabled, two traps are sent when either of the related conditions occur. The individual trap provides additional information about the specific event that triggered the trap.

Managing SNMP interfaces

The TAOS unit supports the Interface MIB based on RFC 2233, which supersedes the SNMP MIB-II defined in RFC1213. The interface table contains only the system's physical interfaces and nailed (permanent) interfaces.

The index value of an interface does not change following a system reset, and if an entry is removed from the interface table dynamically, its index value is not reused until the management station has been reinitialized. The interface table does not contain virtual circuit interfaces, such as a Frame Relay datalink configured on a channelized DS1 interface.

The If-Admin command is a diagnostic tool for managing SNMP interfaces. To see its usage:

```
admin> if-admin
usage: if-admin -a|d|l|r|u|? [ interface ]
       -a  list (a)available SNMP interface numbers
       -d  administratively (d)own an SNMP interface
       -l  (l)ist SNMP interface/device address mapping
       -r  (r)eset SNMP interface/device address mappings
       -u  administratively (u)p an SNMP interface
       -?  display this summary
```

To see a list of available SNMP interface numbers, use the `-a` option:

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

To see a list of all SNMP interface numbers assigned by the system:

```
admin>if-admin -l

SNMP-IF   DEVICE ADDRESS   STATUS

     1   -   { 1 17 1}     1
     2   -   { 1 1 1 }     1
     3   -   { 1 1 2 }     1
     4   -   { 1 1 3 }     1
     5   -   { 1 1 4 }     1
     6   -   { 1 1 5 }     1
     7   -   { 1 1 6 }     1
```

```
      8   -   { 1 1 7 }     1
      9   -   { 1 1 8 }     1
..
..
```

To bring an SNMP interface up or down, use the If-Admin command with the `-d` option, and specify the interface number. For example:

```
admin> if-admin -d 2
interface 2 state change forced
```

To bring a downed device back up, use the If-Admin command with the `-u` option, and specify the interface number. For example:

```
admin> if-admin -u 2
interface 2 state change forced
```

Initiating interface state changes

To bring an SNMP interface up or down, use the If-Admin command.

To bring an interface down:

```
admin> if-admin -d 2
interface 2 state change forced
```

To bring an interface up:

```
admin> if-admin -u 2
interface 2 state change forced
```

Resetting SNMP interface table sequentially

By default, the SNMP interface table is built as slot-cards are installed in the TAOS unit. The If-admin command `–r` option enables the administrator to reset the order of the table to be sequential based on slot number.

When you use the If-Admin command with the `–r` option, the order of the SNMP interface table is reset to a deterministic order. The T1 lines will appear in the SNMP interface table before the packet-passing interfaces such as Ethernet, modem, and HDLC cards. The T1 line interfaces will be ordered based on slot number order.

Note: You must reset the TAOS unit for the new order to take effect.

For example:

```
admin> if-admin -r
SNMP interface mappings reset.
Reset system in order to take effect.
```

Note: This command should not fail, but if for some reason it does, attempt it again. If it fails a second time, you should bring down all slot cards (`Slot –d`), remove all slot cards by using `Slot –r`, reset the system, and run the `If-admin –r` command again.

Ascend MIB hierarchy

Figure 6-1 illustrates the Ascend MIB hierarchy.

Figure 6-1. Ascend MIB hierarchy

products (1)

The `products` group is defined as:

`products ::= { enterprise ascend1 }` with this value:
1.3.6.1.4.1.529.1

It contains the following objects:

multiband (1)
max (2)
pipeline (3)
max-tnt (4)

slots (2)

The `slots` group is defined as:

`slots ::= { enterprise ascend 2 }` with this value:
1.3.6.1.4.1.529.2

It contains the following objects:

slotNumber(1)
slotTable(2)
slotEntry (1)
slotIndex (1)
slotName (2)
slotType (3)
slotFixed (4)
slotItems (5)
slotSpecific (6)
slotSerialNumber (7)
slotStatus (8)
slotLastChange (9)
slotItemTable (3)
slotItemEntry (1)
slotItemSlotIndex (1)
slotItemIndex (2)
slotItemFirstIf (3)
slotItemIfCount (4)
slotItemSpecific (5)
slotItemStatus (6)
slotIfTable (4)
slotifEntry (1)
slotSlotIfIndex (1)

hostTypes (3)

The `hostTypes` group is defined as:

`hostTypes ::= { enterprise ascend 3 }` with this value:
1.3.6.1.4.1.529.3

It contains the following objects:

hostTypeAny (1)
hostTypeDual (2)
hostTypeQuad (3)
hostTypeAim2 (4)
hostTypeAim6 (5)

advancedAgent (4)

The `advancedAgent` group is defined as:

`advancedAgent ::= { enterprise ascend 4 }` with this value:
1.3.6.1.4.1.529.1

It contains the following objects:

wanUseTrunkGroups(20)
wanLineTable (21)
wanLineEntry (1)
wanLineIfIndex (1)
wanLineName (2)
wanLineType (3)
wanLineChannels (4)
wanLineState (5)
wanLineStateString (6)
wanLineActiveChannels (7)
wanLineUsage (8)
wanLineHuntGrpPhoneNumber1 (9)
wanLineHuntGrpPhoneNumber2 (10)
wanLineHuntGrpPhoneNumber3 (11)
wanLineAvailableChannels (12)
wanLineSwitchedChannels (13)
wanLineDisabledChannels (14)
wanLineNailedChannels (15)
wanLineOutOfServiceChannels (16)
wanLineChannelTable(22)
wanLineChannelEntry (1)
wanLineChannelIfIndex (1)
wanLineChannelIndex (2)
wanLineChannelState (3)
wanLineChannelStateString (4)
wanLineChannelErrorCount (5)
wanLineChannelUsage (6)
wanLineChannelTrunkGroup (7)
wanLineChannelPhoneNumber (8)
wanLineChannelSlot (9)
wanLineChannelPort (10)
wanLineChannelNailedState (11)
wanAvailableChannels (23)
wanSwitchedChannels (24)

lanTypes (5)

The `lanTypes` group is defined as:

`products ::= { enterprise ascend 5}` with this value:
1.3.6.1.4.1.529.5

The Ascend MIB `lanTypes` group contains the following objects:

lanTypeAny (1)
lanTypeEthernet (2)
lanTypeEtherData (3)

doGroup (6)

The `doGroup` is defined as:

`products ::= { enterprise ascend 6 }` with this value:
1.3.6.1.4.1.529.6

The Ascend MIB `doGroup` contains the following objects:

doTable (1)
doEntry (1)
doSlotIndex (1)
doItemIndex (2)
doDial (3)
doHangUp (4)
doAnswer (5)
doExtendBW (6)
doContractBW (7)
doBegEndRemoteLB (8)

hostStatus (7)

The `hostStatus` group is defined as:

`hostStatus ::= { enterprise ascend 7 }` with this value:
1.3.6.1.4.1.529.7

It contains the following objects:

hostStatusTable (1)
hostStatusEntry (1)
hostStatusSlotIndex (1)
hostStatusItemIndex (2)
hostStatusLocalName (3)
hostStatusDialNum (4)
hostStatusCallType (5)
hostStatusCallMgm (6)
hostStatusDataSvc (7)
hostStatusCallState (8)
hostStatusRemName (9)
hostStatusChannels (10)

console (8)

The `console` group is defined as:

`console ::= { enterprise ascend 8 }` with this value:
1.3.6.1.4.1.529.8

It contains the following objects:

consoleNumber (1)
consoleTable (2)
consoleEntry (1)
consoleIndex (1)
consoleIf (2)
consoleType (3)
consoleSecurity (4)
consoleSpecific (5)

systemStatusGroup (9)

The `systemStatusGroup` is defined as:

`systemStatusGroup ::= { enterprise ascend 9 }` with this value:
1.3.6.1.4.1.529.9

It contains the following objects:

sysAbsoluteStartupTime (1)
sysSecsSinceStartup (2)
sysMibVersionNum (3)
sysMibMinorRevNum (4)
sysConfigTftp (5)
  sysConfigTftpCmd (1)
  sysConfigTftpStatus (2)
  sysConfigTftpHostAddr (3)
  sysConfigTftpFilename (4)
  sysConfigTftpPort (5)
  sysConfigTftpParameter (6)
sysConfigRadius (6)
  sysConfigRadiusCmd (1)
  sysConfigRadiusStatus (2)
sysAbsoluteCurrentTime (7)
sysReset (8)
sysLoadName (9)
sysAuthPreference (10)
sysSPROM (11)
  sysSPROMSerialNumber (1)
  sysSPROMOptions1 (2)
  sysSPROMOptions2 (3)
  sysSPROMCountries1 (4)
resetStat (12)
  resetStatEther (1)

eventGroup (10)

The `eventGroup` is defined as:

`eventGroup ::= { enterprise ascend 10 }` with this value:
1.3.6.1.4.1.529.10

It contains the following objects:

eventMaximumNumberOfEvents (1)
eventOldestEventIdNumber (2)
eventLatestEventIdNumber (3)
eventTable(4)
eventEntry (1)
eventIdNumber (1)
eventTimeStamp (2)
eventType (3)
eventCallReferenceNum (4)
eventDataRate (5)
eventSlotNumber (6)
eventSlotLineNumber (7)
eventSlotChannelNumber (8)
eventModemSlotNumber (9)
eventModemOnSlot (10)
eventCurrentService (11)
eventUserName (12)
eventUserIPAddress (13)
eventUserSubnetMask (14)
eventDisconnectReason (15)
eventConnectProgress (16)
eventCallCharge (17)
eventCalledPartyID (18)
eventCallingPartyID (19)
eventInOctets (20)
eventOutOctets (21)
eventMultiLinkID (22)
eventXmitRate (23)
eventCurrentActiveCalls (5)
eventCurrentActiveSessions (6)
eventTotalCalls (7)
eventTotalSessions (8)
eventTotalCallsAnswered (9)
eventTotalCallsOriginated (10)
eventTotalCallsCleared (11)

callStatusGroup (11)

The `callStatusGroup` is defined as:

`callStatusGroup ::= { enterprise ascend 11 }` with this value:
1.3.6.1.4.1.529.11

It contains the following objects:

callStatusMaximumEntries (1)
callStatusTable (2)
callStatusEntry (1)
callStatusIndex (1)
callStatusValidFlag (2)
callStatusStartingTimeStamp (3)
callStatusCallReferenceNum (4)
callStatusDataRate (5)
callStatusSlotNumber (6)
callStatusSlotLineNumber (7)
callStatusSlotChannelNumber (8)
callStatusModemSlotNumber (9)
callStatusModemOnSlot (10)
callStatusIfIndex (11)
callSessionIndex (12)
callStatusType (13)
callStatusXmitRate (14)
callStatusPortType (15)
callStatusHighWaterMark (3)
callCurrentAnalogOutgoing (4)
callCurrentAnalogIncoming (5)
callTotalAnalogOutgoing (10)
callTotalAnalogIncoming (11)
callTotalDigitalOutgoing (12)
callTotalDigitalIncoming (13)
callTotalFROutgoing (14)
callTotalFRIncoming (15)
callActiveTable (16)
callActiveEntry (1)
callActiveCallReferenceNum (1)
callActiveIndex (2)
callActiveValidFlag (3)
callActiveStartingTimeStamp (4)
callActiveDataRate (5)
callActiveSlotNumber (6)
callActiveSlotLineNumber (7)
callActiveSlotChannelNumber (8)
callActiveModemSlotNumber (9)
callActiveModemOnSlot (10)
callActiveIfIndex (11)

sessionStatusGroup (12)

The `sessionStatusGroup` is defined as:

`sessionStatusGroup ::= { enterprise ascend 12 }` with this value:
1.3.6.1.4.1.529.12

It contains the following objects:

ssnStatusMaximumSessions (1)
sessionStatusTable (2)
sessionStatusEntry (1)
ssnStatusIndex (1)
ssnStatusValidFlag (2)
ssnStatusUserName (3)
ssnStatusUserIPAddress (4)
ssnStatusUserSubnetMask (5)
ssnStatusCurrentService (6)
ssnStatusCallReferenceNum (7)
sessionActiveTable (3)
sessionActiveEntry (1)
ssnActiveCallReferenceNum (1)
ssnActiveIndex (2)
ssnActiveValidFlag (3)
ssnActiveUserName (4)
ssnActiveUserIPAddress (5)
ssnActiveUserSubnetMask (6)
ssnActiveCurrentService (7)
mppActiveStatsTable (4)
mppActiveStatsEntry (1)
mppStatsMpID (1)
mppStatsRemoteName (2)
mppStatsQuality (3)

radiusGroup (13)

The `radiusGroup` is defined as:

`radiusGroup ::= { enterprise ascend 13 }` with this value:
1.3.6.1.4.1.529.13

It contains the following objects:

radiusNumAuthServers (1)
radiusNumAcctServers (2)
radiusAuthStatsTable (3)
radiusAuthStatsEntry (1)
radAuthServerIndex (1)
radAuthLoginRqstSent (2)
radAuthOtherRqstSent (3)
radAuthRqstTimedOut (4)
radAuthOtherRqstTimedOut (5)
radAuthRspRcvd (6)
radAuthOtherRspRcvd (7)
radAuthUnexpRspRcvd (8)
radAuthBadRspRcvd (9)
radAuthAckRspRcvd (10)
radAuthHostIPAddress (11)
radAuthCurrentServerFlag (12)
radiusAcctStatsTable (4)
radiusAcctStatsEntry (1)
radAcctServerIndex (1)
radAcctRqstSent (2)
radAcctRqstTimedOut (3)
radAcctRspRcvd (4)

mCastGroup (14)

The `mCastGroup` is defined as:

`mCastGroup ::= { enterprise ascend 14 }` with this value:
1.3.6.1.4.1.529.14

It contains the following objects:

eartBeatMulticastGroupAddress (1)
eartBeatSourceAddress (2)
eartBeatSlotTimeInterval (3)
eartBeatSlotCount (4)

lanModemGroup (15)

The `lanModemGroup` is defined as:

`lanModemGroup ::= { enterprise ascend 15 }` with this value:
1.3.6.1.4.1.529.15

It contains the following objects:

availLanModem (1)
availLanModemTable (2)
availLanModemEntry (1)
availLanModemSlotIndex (1)
availLanModemPortIndex (2)
availLanModemUsedCount (3)
availLanModemBadCount (4)
availLanModemLast32 (5)
suspectLanModem (3)
suspectLanModemTable (4)
suspectLanModemEntry (1)
suspectLanModemSlotIndex (1)
suspectLanModemPortIndex (2)
suspectLanModemUsedCount (3)
suspectLanModemBadCount (4)
suspectLanModemLast32 (5)
disabledLanModem (5)
disabledLanModemTable (6)
disabledLanModemEntry (1)
disabledLanModemSlotIndex (1)
disabledLanModemPortIndex
deadLanModem (7)
deadLanModemTable (8)
deadLanModemEntry (1)
deadLanModemSlotIndex (1)
deadLanModemPortIndex (2)
deadLanModemState (3)
busyLanModem (9)
busyLanModemTable (10)
busyLanModemEntry (1)
busyLanModemSlotIndex (1)
busyLanModemPortIndex (2)
busyLanModemUsedCount (3)
busyLanModemBadCount (4)
busyLanModemLast32 (5)
busyDirection (6)
suspectTrapState (11)

firewallGroup (16)

The `firewallGroup` is defined as:

`firewallGroup ::= { enterprise ascend 16 }` with this value:
1.3.6.1.4.1.529.16

It contains the following objects:

firewallStatus (1)
firewallControl (2)
fwallCtrlRuleName (1)
fwallCtrlExecute (2)
fwallCtrlTimeOut (3)
fwallCtrlExtAddr (4)
fwallCtrlExtAddrMask (5)
fwallCtrlExtPort (6)
fwallCtrlExtPortMax (7)
fwallCtrlIntAddr (8)
fwallCtrlIntAddrMask (9)
fwallCtrlIntPort (10)
fwallCtrlIntPortMax (11)
fwallCtrlRoutAddr (12)

wanDialoutPkt (17)

The `wanDialoutPkt` group is defined as:

`wanDialoutPkt ::= { enterprise ascend 17 }` with this value:
1.3.6.1.4.1.529.17

It contains the following objects:

wanDialoutPktTableSize (1)
wanDialoutPktMaxSize (2)
wanDialoutPktCount (3)
wanDialoutPktTable (4)
  wanDialoutPktEntry (1)
    wanDialoutPktIndex (1)
    wanDialoutPktTime (2)
    wanDialoutPktPhoneNumber (3)

powerSupply (18)

The `powerSupply` group is defined as:

`powerSupply ::= { enterprise ascend 18 }` with this value:
1.3.6.1.4.1.529.18

It contains the following objects:

powerSupplyCount (1)
powerSupplyTable (2)
  powerSupplyEntry (1)
    powerSupplyIndex (1)
    powerSupplyState (2)
    powerSupplyOperationalState (3)
powerSupplyStateTrapState (3)

multiShelf (19)

The `multiShelf` group is defined as:

`multiShelf ::= { enterprise ascend 19 }` with this value:
1.3.6.1.4.1.529.19

It contains the following objects:

myShelfNumber (1)
myShelfOperation (2)
masterShelfNumber (3)
multiShelfTableSize (4)
multiShelfTable (5)
multiShelfTable (1)
multiShelfIndex (1)
multiShelfState (2)
multiShelfResentFrames (3)
multiShelfNLinkUp (4)
multiShelfTxQs (5)
multiShelfTxSeq (6)
multiShelfRxSeq (7)
multiShelfTimerValue (8)

miscGroup (20)

The `miscGroup` is defined as:

`miscGroup ::= { enterprise ascend 20 }` with this value:
1.3.6.1.4.1.529.20

It contains the following objects:

iscGroupFRTable (1)
iscGroupFREntry (1)
MiscGroupFRLMIIndex (1)
MiscGroupFRLMIDlci (2)

flashGroup (22)

The `flashGroup` is defined as:

`flashGroup ::= { enterprise ascend 22 }` with this value:
1.3.6.1.4.1.529.22

It contains the following objects:

flashDevice (1)
flashDevices (1)
flashDeviceTable (2)
flashDeviceEntry (1)
flashDeviceIndex (1)
flashDeviceController (2)
flashDeviceSlot (3)
flashDeviceSize (4)
flashDeviceUsed (5)
flashDeviceState (6)
flashDeviceMaster (7)
flashDeviceFormatStatus (8)
flashDeviceDescription (9)
flashFileTable (2)
flashFileEntry (1)
flashFileIndex (1)
flashFileController (2)
flashFileCard (3)
flashFileSize (4)
flashFileStatus (5)
flashFileName (6)
flashFileChecksum (7)
flashFileVersion (8)
flashFileAccess (9)
flashFileDateTimeStamp (10)
flashOperation (3)
flashOperationStatus (1)
flashOperationCommand (2)
flashOperationHost (3)
flashOperationDestFileName (4)
flashOperationSrcFileName (5)

configuration (23)

The `configuration` group is defined as:

`configuration ::= { enterprise ascend 23 }` with this value: 1.3.6.1.4.1.529.23

It contains the following objects:

mibinternetProfile (1)
mibframeRelayProfile (2)
mibanswerProfile (3)
mibud3NetworkProfile (4)
mibuds3NetworkProfile (5)
mibcadslNetworkProfile (6)
mibdadslNetworkProfile (7)
mibsdslNetworkProfile (8)

mibinternetProfile (1)

The `mibInternetProfile` has the value:
1.3.6.1.4.1.529.23.1

The `mibInternetProfile` in the `configuration` group contains the following objects:

MibinternetProfileTable (1)
MibinternetProfileEntry (1)
internetProfile__station (1)
internetProfile__active (2)
internetProfile__encapsulation_protocol(3)
internetProfile__called_number_type(4)
internetProfile__dial_number(5)
internetProfile__clid(6)
internetProfile__ip_options__ip_routing_enabled(7)
internetProfile__ip_options__vj_header_prediction(8)
internetProfile__ip_options__remote_address(9)
internetProfile__ip_options__local_address(10)
internetProfile__ip_options__routing_metric(11)
internetProfile__ip_options__preference(12)
internetProfile__ip_options__down_preference(13)
internetProfile__ip_options__private_route(14)
internetProfile__ip_options__multicast_allowed(15)
internetProfile__ip_options__address_pool(16)
internetProfile__ip_options__ip_direct(17)
internetProfile__ip_options__rip(18)
internetProfile__ip_options__route_filter(19)
internetProfile__ip_options__source_ip_check(20)
internetProfile__ip_options__ospf_options__active(21)
internetProfile__ip_options__ospf_options__area(22)
internetProfile__ip_options__ospf_options__area_type(23)
internetProfile__ip_options__ospf_options__hello_interval(24)
internetProfile__ip_options__ospf_options__dead_interval(25)
internetProfile__ip_options__ospf_options__priority(26)
internetProfile__ip_options__ospf_options__authen_type(27)
internetProfile__ip_options__ospf_options__auth_key(28)
internetProfile__ip_options__ospf_options__key_id(29)
internetProfile__ip_options__ospf_options__cost(30)
internetProfile__ip_options__ospf_options__down_cost(31)
internetProfile__ip_options__ospf_options__ase_type(32)
internetProfile__ip_options__ospf_options__ase_tag(33)
internetProfile__ip_options__ospf_options__transit_delay(34)
internetProfile__ip_options__ospf_options__retransmit_interval(35)
internetProfile__ip_options__ospf_options__non_multicast(36)
internetProfile__ip_options__multicast_rate_limit(37)
internetProfile__ip_options__multicast_group_leave_delay(38)
internetProfile__ip_options__client_dns_primary_addr(39)
internetProfile__ip_options__client_dns_secondary_addr(40)
internetProfile__ip_options__client_dns_addr_assign(41)
internetProfile__ip_options__client_default_gateway(42)
internetProfile__ip_options__tos_options__active(43)
internetProfile__ip_options__tos_options__precedence(44)
internetProfile__ip_options__tos_options__type_of_service(45)
internetProfile__ip_options__tos_options__apply_to(46)
internetProfile__ip_options__tos_filter(47)
internetProfile__ipx_options__ipx_routing_enabled(48)
internetProfile__ipx_options__peer_mode(49)
internetProfile__ipx_options__rip(50)
internetProfile__ipx_options__sap(51)
internetProfile__ipx_options__dial_query(52)
internetProfile__ipx_options__net_number(53)
internetProfile__ipx_options__net_alias(54)
internetProfile__ipx_options__sap_filter(55)
internetProfile__ipx_options__ipx_spoofing(56)
internetProfile__ipx_options__spoofing_timeout(57)
internetProfile__ipx_options__ipx_sap_hs_proxy(58)
internetProfile__ipx_options__ipx_header_compression(59)
internetProfile__bridging_options__bridging_group(60)
internetProfile__bridging_options__dial_on_broadcast(61)
internetProfile__bridging_options__ipx_spoofing(62)
internetProfile__bridging_options__spoofing_timeout(63)
internetProfile__bridging_options__bridge_type(64)
internetProfile__session_options__call_filter(65)
internetProfile__session_options__data_filter(66)
internetProfile__session_options__filter_persistence(67)
internetProfile__session_options__idle_timer(68)
internetProfile__session_options__ts_idle_mode(69)
internetProfile__session_options__ts_idle_timer(70)
internetProfile__session_options__backup(71)
internetProfile__session_options__secondary(72)
internetProfile__session_options__atmp_gateway(73)
internetProfile__session_options__max_call_duration(74)
internetProfile__session_options__vtp_gateway(75)
internetProfile__session_options__blockcountlimit(76)
internetProfile__session_options__blockduration(77)
internetProfile__session_options__max_atmp_tunnels(78)
internetProfile__session_options__max_vtp_tunnels(79)
internetProfile__session_options__redial_delay_limit(80)
internetProfile__session_options__ses_rate_type(81)
internetProfile__session_options__ses_rate_mode(82)
internetProfile__session_options__ses_adsl_cap_up_rate(83)
internetProfile__session_options__ses_adsl_cap_down_rate(84)
internetProfile__session_options__ses_adsl_dmt_up_rate(85)
internetProfile__session_options__ses_adsl_dmt_down_rate(86)
internetProfile__session_options__rx_data_rate_limit(87)
internetProfile__session_options__tx_data_rate_limit(88)
internetProfile__telco_options__answer_originate(89)
internetProfile__telco_options__callback(90)
internetProfile__telco_options__call_type(91)
internetProfile__telco_options__nailed_groups(92)
internetProfile__telco_options__ft1_caller(93)
internetProfile__telco_options__force_56kbps(94)
internetProfile__telco_options__data_service(95)
internetProfile__telco_options__call_by_call(96)
internetProfile__telco_options__billing_number(97)
internetProfile__telco_options__transit_number(98)
internetProfile__telco_options__expect_callback(99)
internetProfile__telco_options__dialout_allowed(100)
internetProfile__telco_options__delay_callback(101)
internetProfile__ppp_options__send_auth_mode(102)
internetProfile__ppp_options__send_password(103)
internetProfile__ppp_options__substitute_send_name(104)
internetProfile__ppp_options__recv_password(105)
internetProfile__ppp_options__link_compression(106)
internetProfile__ppp_options__mru(107)
internetProfile__ppp_options__lqm(108)
internetProfile__ppp_options__lqm_minimum_period(109)
internetProfile__ppp_options__lqm_maximum_period(110)
internetProfile__ppp_options__cbcp_enabled(111)
internetProfile__ppp_options__mode_callback_control(112)
internetProfile__ppp_options__delay_callback_control(113)
internetProfile__ppp_options__trunk_group_callback_control(114)
internetProfile__ppp_options__split_code_dot_user_enabled(115)
internetProfile__ppp_options__ppp_interface_type(116)
internetProfile__mp_options__base_channel_count(117)
internetProfile__mp_options__minimum_channels(118)
internetProfile__mp_options__maximum_channels(119)
internetProfile__mp_options__bacp_enable(120)
internetProfile__mpp_options__aux_send_password(121)
internetProfile__mpp_options__dynamic_algorithm(122)
internetProfile__mpp_options__bandwidth_monitor_direction(123)
internetProfile__mpp_options__increment_channel_count(124)
internetProfile__mpp_options__decrement_channel_count(125)
internetProfile__mpp_options__seconds_history(126)
internetProfile__mpp_options__add_persistence(127)
internetProfile__mpp_options__sub_persistence(128)
internetProfile__mpp_options__target_utilization(129)

internetProfile__fr_options__frame_relay_profile(130)
internetProfile__fr_options__dlci(131)
internetProfile__fr_options__circuit_name(132)
internetProfile__fr_options__fr_direct_enabled(133)
internetProfile__fr_options__fr_direct_profile(134)
internetProfile__fr_options__fr_direct_dlci(135)
internetProfile__tcp_clear_options__detect_end_of_packet(136)
internetProfile__tcp_clear_options__end_of_packet_pattern(137)
internetProfile__tcp_clear_options__flush_length(138)
internetProfile__tcp_clear_options__flush_time(139)
internetProfile__ara_options__recv_password(140)
internetProfile__ara_options__maximum_connect_time(141)
internetProfile__comb_options__password_required(142)
internetProfile__comb_options__interval(143)
internetProfile__comb_options__base_channel_count(144)
internetProfile__comb_options__compression(145)
internetProfile__x25_options__x25_profile(146)
internetProfile__x25_options__lcn(147)
internetProfile__x25_options__x3_profile(148)
internetProfile__x25_options__max_calls(149)
internetProfile__x25_options__vc_timer_enable(150)
internetProfile__x25_options__x25EncapsType(151)
internetProfile__x25_options__auto_call_x121_address(152)
internetProfile__x25_options__reverse_charge(153)
internetProfile__x25_options__call_mode(154)
internetProfile__x25_options__answer(155)
internetProfile__x25_options__inactivity_timer(156)
internetProfile__x25_options__if_mtu(157)
internetProfile__x25_options__x25_rpoa(158)
internetProfile__x25_options__x25_cug_index(159)
internetProfile__x25_options__x25_nui(160)
internetProfile__x25_options__pad_banner(161)
internetProfile__x25_options__pad_prompt(162)
internetProfile__x25_options__pad_nui_prompt(163)
internetProfile__x25_options__pad_nui_pw_prompt(164)
internetProfile__x25_options__pad_alias1(165)
internetProfile__x25_options__pad_alias2(166)
internetProfile__x25_options__pad_alias3(167)
internetProfile__x25_options__pad_diag_disp(168)
internetProfile__x25_options__pad_default_listen(169)
internetProfile__x25_options__pad_default_pw(170)
internetProfile__eu_options__dce_addr(171)
internetProfile__eu_options__dte_addr(172)
internetProfile__eu_options__mru(173)
internetProfile__x75_options__k_frames_outstanding(174)
internetProfile__x75_options__n2_retransmissions(175)
internetProfile__x75_options__t1_retran_timer(176)
internetProfile__x75_options__frame_length(177)
internetProfile__appletalk_options__atalk_routing_enabled(178)
internetProfile__appletalk_options__atalk_static_ZoneName(179)
internetProfile__appletalk_options__atalk_static_NetStart(180)
internetProfile__appletalk_options__atalk_static_NetEnd(181)
internetProfile__appletalk_options__atalk_Peer_Mode(182)
internetProfile__usrRad_options__acct_type(183)
internetProfile__usrRad_options__acct_host(184)
internetProfile__usrRad_options__acct_port(185)
internetProfile__usrRad_options__acct_key(186)
internetProfile__usrRad_options__acct_timeout(187)
internetProfile__usrRad_options__acct_id_base(188)
internetProfile__calledNumber(189)
internetProfile__dhcp_options__reply_enabled(190)
internetProfile__dhcp_options__pool_number(191)
internetProfile__dhcp_options__maximum_leases(192)
internetProfile__sharedprof_options(193)
internetProfile__t3pos_options__x25_profile(194)
internetProfile__t3pos_options__max_calls(195)
internetProfile__t3pos_options__auto_call_x121_address(196)
internetProfile__t3pos_options__reverse_charge(197)
internetProfile__t3pos_options__answer(198)
internetProfile__t3pos_options__t3PosHostInitMode(199)
internetProfile__t3pos_options__t3PosDteInitMode(200)
internetProfile__t3pos_options__t3PosEnqHandling(201)
internetProfile__t3pos_options__t3PosMaxBlockSize(202)
internetProfile__t3pos_options__t3PosT1(203)
internetProfile__t3pos_options__t3PosT2(204)
internetProfile__t3pos_options__t3PosT3(205)
internetProfile__t3pos_options__t3PosT4(206)
internetProfile__t3pos_options__t3PosT5(207)
internetProfile__t3pos_options__t3PosT6(208)
internetProfile__t3pos_options__t3PosMethodOfHostNotif(209)
internetProfile__t3pos_options__t3PosPidSelection(210)
internetProfile__t3pos_options__t3PosAckSuppression(211)
internetProfile__t3pos_options__x25_rpoa(212)
internetProfile__t3pos_options__x25_cug_index(213)
internetProfile__t3pos_options__x25_nui(214)
internetProfile__t3pos_options__data_format(215)
internetProfile__t3pos_options__link_access_type(216)
internetProfile__framed_only(217)
internetProfile__altdial_number1(218)
internetProfile__altdial_number2(219)
internetProfile__altdial_number3(220)
internetProfile__x32_options__x32_profile(221)
internetProfile__x32_options__call_mode(222)
internetProfile__tunnel_options__profile_type(223)
internetProfile__tunnel_options__tunneling_protocol(224)
internetProfile__tunnel_options__max_tunnels(225)
internetProfile__tunnel_options__atmp_ha_rip(226)
internetProfile__tunnel_options__primary_tunnel_server(227)
internetProfile__tunnel_options__secondary_tunnel_server(228)
internetProfile__tunnel_options__udp_port(229)
internetProfile__tunnel_options__password(230)
internetProfile__tunnel_options__home_network_name(231)
internetProfile__tunnel_options__unused(232)
internetProfile__pri_numbering_plan_id(233)
internetProfile__vrouter(234)
internetProfile__atm_options__atm1483type(235)
internetProfile__atm_options__vpi(236)
internetProfile__atm_options__vci(237)
internetProfile__action__(238)
mibinternetProfile__tcp_clear_options__portTable (2)
internetProfile__tcp_clear_options__port__station (1)
internetProfile__tcp_clear_options__port__index__ (2)
internetProfile__tcp_clear_options__port (3)
mibinternetProfile__tcp_clear_options__hostTable (3)
internetProfile__tcp_clear_options__host__station (1)
internetProfile__tcp_clear_options__host__index__ (2)
internetProfile__tcp_clear_options__host (3)
mibinternetProfile__ipx_options__ipx_sap_hs_proxy_netTable (4)
internetProfile__ipx_options__ipx_sap_hs_proxy_net__station (1)
internetProfile__ipx_options__ipx_sap_hs_proxy_net__index__ (2
internetProfile__ipx_options__ipx_sap_hs_proxy_net (3)

mibframeRelayProfile (2)

The `mibframeRelayProfile` has the value:
1.3.6.1.4.1.529.23.2

The `mibframeRelayProfile` in the `configuration` group contains the following objects:

mibframeRelayProfileTable (1)
mibframeRelayProfileEntry (1)
frameRelayProfile__fr_name (1)
frameRelayProfile__active (2)
frameRelayProfile__nailed_up_group (3)
frameRelayProfile__nailed_mode (4)
frameRelayProfile__called_number_type (5)
frameRelayProfile__switched_call_type (6)
frameRelayProfile__phone_number (7)
frameRelayProfile__billing_number (8)
frameRelayProfile__transit_number (9)
frameRelayProfile__link_mgmt (10)
frameRelayProfile__call_by_call_id (11)
frameRelayProfile__link_type (12)
frameRelayProfile__n391_val (13)
frameRelayProfile__n392_val (14)
frameRelayProfile__n393_val (15)
frameRelayProfile__t391_val (16)
frameRelayProfile__t392_val (17)
frameRelayProfile__MRU (18)
frameRelayProfile__dceN392_val (19)
frameRelayProfile__dceN393_val (20)

mibanswerProfile (3)

The `mibAnswerProfile` has the value:
1.3.6.1.4.1.529.23.3

The `mibanswerProfile` in the `configuration` group contains the following objects:

mibanswerProfileTable (1)
mibanswerProfileEntry (1)
answerProfile__index (1)
answerProfile__use_answer_for_all_defaults (2)
answerProfile__force_56kbps (3)
answerProfile__profiles_required (4)
answerProfile__clid_auth_mode (5)
answerProfile__ppp_answer__enabled (6)
answerProfile__ppp_answer__receive_auth_mode (7)
answerProfile__ppp_answer__disconnect_on_auth_timeout (8)
answerProfile__ppp_answer__bridging_group (9)
answerProfile__ppp_answer__link_compression (10)
answerProfile__ppp_answer__mru (11)
answerProfile__ppp_answer__lqm (12)
answerProfile__ppp_answer__lqm_minimum_period (13)
answerProfile__ppp_answer__lqm_maximum_period (14)
answerProfile__mp_answer__enabled (15)
answerProfile__mp_answer__minimum_channels (16)
answerProfile__mp_answer__maximum_channels (17)
answerProfile__mp_answer__bacp_enable (18)
answerProfile__mpp_answer__enabled (19)
answerProfile__mpp_answer__dynamic_algorithm (20)
answerProfile__mpp_answer__bandwidth_monitor_direction (21)
answerProfile__mpp_answer__increment_channel_count (22)
answerProfile__mpp_answer__decrement_channel_count (23)
answerProfile__mpp_answer__seconds_history (24)
answerProfile__mpp_answer__add_persistence (25)
answerProfile__mpp_answer__sub_persistence (26)
answerProfile__mpp_answer__target_utilization (27)
answerProfile__fr_answer__enabled (28)
answerProfile__tcp_clear_answer__enabled (29)
answerProfile__ara_answer__enabled (30)
answerProfile__v120_answer__enabled (31)
answerProfile__v120_answer__frame_length (32)
answerProfile__x25_answer__enabled (33)
answerProfile__x25_answer__x25_profile (34)
answerProfile__x25_answer__x3_profile (35)
answerProfile__x25_answer__max_calls (36)
answerProfile__x25_answer__vc_timer_enable (37)
answerProfile__x25_answer__auto_call_x121_address (38)
answerProfile__x25_answer__reverse_charge (39)
answerProfile__x25_answer__x3_custom_prof (40)
answerProfile__comb_answer__enabled (41)
answerProfile__comb_answer__password_required (42)
answerProfile__comb_answer__interval (43)
answerProfile__comb_answer__compression (44)
answerProfile__eu_answer__euraw_enabled (45)
answerProfile__eu_answer__euui_enabled (46)
answerProfile__eu_answer__dce_addr (47)
answerProfile__eu_answer__dte_addr (48)
answerProfile__eu_answer__mru (49)
answerProfile__ip_answer__enabled (50)
answerProfile__ip_answer__vj_header_prediction (51)
answerProfile__ip_answer__assign_address (52)
answerProfile__ip_answer__routing_metric (53)
answerProfile__ipx_answer__enabled (54)
answerProfile__ipx_answer__peer_mode (55)
answerProfile__session_info__call_filter (56)
answerProfile__session_info__data_filter (57)
answerProfile__session_info__filter_persistence (58)
answerProfile__session_info__idle_timer (59)
answerProfile__session_info__ts_idle_mode (60)
answerProfile__session_info__ts_idle_timer (61)
answerProfile__session_info__max_call_duration (62)
answerProfile__x75_answer__enabled (63)
answerProfile__x75_answer__k_frames_outstanding (64)
answerProfile__x75_answer__n2_retransmissions (65)
answerProfile__x75_answer__t1_retran_timer (66)
answerProfile__x75_answer__frame_length (67)
answerProfile__framed_only (68)
answerProfile__action (69)

mibuds3NetworkProfile (5)

The `mibuds3Profile` has the value:
1.3.6.1.4.1.529.23.5

The `mibuds3NetworkProfile` in the `configuration` group contains the following objects:

mibuds3NetworkProfileTable (1)
mibuds3NetworkProfileEntry (1)
uds3NetworkProfile__shelf (1)
uds3NetworkProfile__slot (2)
uds3NetworkProfile__item (3)
uds3NetworkProfile__name (4)
uds3NetworkProfile__physical_address__shelf (5)
uds3NetworkProfile__physical_address__slot (6)
uds3NetworkProfile__physical_address__item_number (7)
uds3NetworkProfile__enabled (8)
uds3NetworkProfile__profile_number (9)
uds3NetworkProfile__line_config__trunk_group (10)
uds3NetworkProfile__line_config__nailed_group (11)
uds3NetworkProfile__line_config__route_port__slot_number__slot_number (12)
uds3NetworkProfile__line_config__route_port__slot_number__shelf_number (13)
uds3NetworkProfile__line_config__route_port__relative_port_number__relative_port_number (14)
uds3NetworkProfile__line_config__activation (15)
uds3NetworkProfile__line_config__call_route_info__shelf (16)
uds3NetworkProfile__line_config__call_route_info__slot (17)
uds3NetworkProfile__line_config__call_route_info__item_number (18)

atmpGroup (24)

The `atmpGroup` group is defined as:

`atmpGroup ::= { enterprise ascend 24 }` with this value:
1.3.6.1.4.1.529.24

It contains the following objects:

atmpAgentMode (1)
atmpAgentType (2)
atmpAgentUDPPort (3)
atmpAgentGreMtu (4)
atmpAgentForceFragmentation (5)
atmpAgentHAIdleLimit (6)
atmpLastErrorGenerated (7)
atmpAgentSentErrorTo (8)
atmpLastErrorRecv (9)
atmpAgentRecvErrorFrom (10)
atmpEnableAtmpTraps (11)
atmpAgentNumberFATunnels (12)
atmpAgentNumberHATunnels (13)
atmpAgentNumberLocalTunnels (14)
atmpAgentTunnelHighWater (15)
atmpTunnelTable (16)
atmpTunnelEntry (1)
atmpTunnelIndex (1)
atmpTunnelId (2)
atmpHAIpAddress (3)
atmpFAIpAddress (4)
atmpTunneledProtocol (5)
atmpTunnelType (6)
atmpTunnelState (7)
atmpMnIpAddress (8)
atmpMnNetmask (9)
atmpMnIpxNetAddress (10)
atmpMnIpxNodeAddress (11)
atmpHNProfileName (12)
atmpHNMaxTunnels (13)
atmpFAPrimaryHAAddress (14)
atmpFASecondaryHAAddress (15)
atmpFASsnStatusIndex (16)
atmpFAUserName (17)
atmpInPkts (18)
atmpInOctets (19)
atmpInErrPkts (20)
atmpOutPkts (21)

Using Administrative Profiles

7

The TAOS unit provides a number of profiles that either monitor administration information or enable the administrator to change the state of a slot, line, or device. (For discussion of profiles not directly related to system administration, for example, profiles related to configuring lines, connections, or calls, see the *APX 8000/MAX TNT WAN, Routing, and Tunneling Configuration Guide* or the hardware installation guide for your unit.)

Following are the TAOS unit's administrative profiles:

Profile	**Description**
Admin-State-Perm-If	SNMP Permanent Interface Admin State
Admin-State-Phys-If	SNMP Physical Interface Admin State
Base	System version and enabled features
Call-Info	Active call information
Device-State	Device Operational State
DS3-ATM-Stat	DS3-ATM status
Error	Fatal Error Log
LAN-Modem	LAN modem disable state
Log	System event logging configuration

Profile	Description
Slot-Info	Slot information
Slot-State	Slot Operational State
Slot-Type	Slot Type profile
SNMP	SNMP profiles
System	System-level parameters
T1-Stat	T1 and E1 line status
T3-Stat	T3 line status
Timedate	Current system time and date
Trap	SNMP trap destinations
User	Administrative user accounts

For information about the parameters contained within each of these profiles, see the *APX 8000/MAX TNT Reference*.

An administrative profile uses the same set of commands as does any configuration profile in the TAOS unit. For example:

```
admin> read t1-stat { 1 5 1}
T1-STAT/{ shelf-1 slot-5 1 } read

admin> list
physical-address* = { shelf-1 slot-5 1 }
line-state = active
channel-state = [ nailed-up nailed-up nailed-up nailed-up
nailed-up nailed-up n+
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 = True
network-loopback = False
```

How the TAOS unit creates administrative profiles

The TAOS unit allocates SNMP interfaces when a card comes up for the first time. For example, the initial installation of a T1 card creates eight SNMP interfaces, one for each T1 line. Admin-State profiles are stored in NVRAM to keep state information over system resets, so a physical device keeps the same SNMP interface number across system reset or power failures.

Each physical interface in the system has an associated Admin-State-Phys-If profile and each nailed connection, such as a Frame Relay connection or a nailed PPP connection, has an

associated Admin-State-Perm-If profile. These profiles store the object's desired state and SNMP interface number.

At system startup, the TAOS unit reads the Admin-State profiles. If the addressed device is not present in the system and has been replaced by a device of another type, the TAOS unit deletes that profile and creates a new one, with a new SNMP interface number. The next time the system is reset or power cycles, the old device's SNMP interface number becomes available for reassignment. This means that pulling a slot card does not free up interface numbers. When you reinstall the slot card, the same interface number is assigned. Also, pulling a slot card and replacing it with a slot card of another type does not free up the old interface numbers until the next power cycle or system reset.

For example, each T1 line has an Admin-State-Phys-If profile, and each of the 48 modems on a modem card has a profile. To read the Admin-State-Phys-If profile for the first T1 line in Slot 2, use the Read and List commands, as in the following example:

```
admin>read admin-state-phys-if {1 2 1}
ADMIN-STATE-PHYS-IF/{ shelf-1 slot-2 1 } read

admin>list

[in ADMIN-STATE-PHYS-IF/{ shelf-1 slot-2 1 }]
device-address* = { shelf-1 slot-2 1 }
slot-type = 8t1-card
snmp-interface = 34
modem-table-index = 0
desired-state = admin-state-up
desired-trap-state = trap-state-enabled
```

Using the Telnet Access Control List (TACL) profile

To enable you to permit Telnet access to the TAOS unit only from specific IP addresses, the TAOS system supports a new Telnet Access Control List (TACL) profile. You must have System authorization to create, read, or modify the profile.

You can configure up to 20 entries in the TACL profile. Each entry can specify a host address (with a /32 subnet mask) or a subnet address. Specifying a subnet address allows access from any of the addresses in the subnet range.

The TACL profile contains the following parameters, shown here with default values:

```
[in TACL]
enable-permit = no

[in TACL:permit-list[1]]
valid-entry = no
source-address = 0.0.0.0/0
source-address-mask = 0.0.0.0
```

Parameter	Specifies
Enable-Permit	Enable/disable control over Telnet access to the unit on the basis of the Permit-List settings in the TACL profile. If set to `no` (the default), the Permit-List settings have no effect. If set to `yes`, only the IP addresses specified in the Permit-Lists are allowed to telnet into the TAOS command-line interface. Setting Enable-Permit to `yes` has no effect if no Permit-Lists have been specified.
Valid-Entry	Enable/disable the Permit-List entry.
Source-Address	Source IP address of a host or subnet to be allowed Telnet access to the TAOS unit. The specified subnet mask determines whether the entry is valid for a single host or a subnet. If you specify the subnet mask as part of the Source-Address value, the Source-Address-Mask value is set automatically to the corresponding dotted decimal value.
Source-Address-Mask	The subnet mask to be applied to the Source-Address value before enabling a host Telnet access to the unit. You can set the value directly in dotted decimal format or by including a subnet as part of the Source-Address value.

For example, the following commands create a TACL profile that enables Telnet access from 30 host addresses from 10.27.34.1 to 10.27.34.31:

```
admin> new tacl
TACL read

admin> set enable-permit = yes

admin> set permit-list 1 valid-entry = yes

admin> set permit-list 1 source-address-mask = 10.27.34.1/27

admin> list permit-list 1
[in TACL:permit-list[1] (changed)]
valid-entry = yes
source-address = 10.27.34.1/27
source-address-mask = 255.255.255.224

admin> write
TACL written
```

Using the Admin-State-Perm-If profile

The Admin-State-Perm-If profile holds information about the TAOS unit's nailed interfaces. The system creates a profile for an active nailed interface and assigns it an interface index. For example:

```
admin> dir admin-state-perm
    21  08/28/1998 13:21:37  frswan1
    21  08/28/1998 13:21:37  frswan6
    27  08/28/1998 13:22:11  radius-frt1.1
    30  09/02/1998 15:38:07  apx-e1-ds3a-uds3
    30  09/02/1998 17:31:42  apx-e1-ds3a-ds3a
```

The Admin-State-Perm-If profile contains the following parameters (shown here with sample values):

```
[in ADMIN-STATE-PERM-IF/frswan1]
station* = frswan1
snmp-interface = 19
desired-state = admin-state-up
desired-trap-state = trap-state-enabled
inet-profile-type = 1
```

Parameter	Specifies
Station	Name of a nailed profile (PPP or Frame Relay), which may be a local Connection profile or a RADIUS profile.
SNMP-Interface	Interface table index assigned to the nailed interface whose state is stored in this profile.The system assigns a numeric value.
Desired-State	Desired administrative state of the addressed device. The system sets it to Admin-State-Down if an operator downs the device, or to Admin-State-Up if an operator attempts to bring up the device in normal operations mode. An operator can change the admin state by using SNMP SET commands, or the Slot or If-Admin commands.
Desired-Trap-Sate	Desired link up/down enable state of the interface.The system sets it to Trap-State-Enabled if an operator specifies that linkUp/linkDown traps should be generated for the interface, or to Trap-State-Disabled if an operator specifies that linkUp/linkDown traps should not be generated for the interface.
Inet-Profile-Type	If the nailed profile is a local profile (0) or a RADIUS profile (1).

Using the Admin-State-Phys-If profile

The Admin-State-Phys-If profile holds information about the system's physical interfaces. For example:

```
admin> dir  admin-state-phys
    17  08/06/1998 17:03:57  { shelf-1 slot-13 1 }
    17  08/06/1998 17:03:57  { shelf-1 slot-13 2 }
    17  08/06/1998 17:03:57  { shelf-1 slot-13 3 }
    17  08/06/1998 17:03:57  { shelf-1 slot-13 4 }
    17  08/06/1998 17:03:57  { shelf-1 slot-13 5 }
    17  08/06/1998 17:03:57  { shelf-1 slot-13 6 }
```

The system creates a profile for each of its physical interfaces. The Admin-State-Phys-If profile contains the following parameters (shown here with sample values):

```
[in ADMIN-STATE-PHYS-IF/{ shelf-1 slot-13 1 }]
device-address* = { shelf-1 slot-13 1 }
slot-type = hdlc2-card
snmp-interface = 0
modem-table-index = 0
desired-state = admin-state-up
desired-trap-state = trap-state-enabled
```

Parameter	Specifies
Device-Address	Physical slot address within the system.
Slot-Type	Type of card at that address.
SNMP-Interface	Interface table index assigned to the device whose state is stored in this profile.The system assigns a numeric value, which does not change as long as the interface is present in the system. If the card is removed and its profiles deleted (for example, by using a Slot –r command), the index number is freed for future use.
Modem-Table-Index	Modem table index assigned to the device whose state is stored in this profile. The system assigns a numeric value. The value is 0 for devices that are not modems.
Desired-State	Desired administrative state of the addressed device. The system sets it to Admin-State-Down if an operator downs the device, or to Admin-State-Up if an operator attempts to bring up the device in normal operations mode. An operator can change the admin state by using SNMP SET commands, or the Slot or If-Admin commands.
Desired-Trap-Sate	Desired link up/down enable state of the interface.The system sets it to Trap-State-Enabled if an operator specifies that linkUp/linkDown traps should be generated for the interface, or to Trap-State-Disabled if an operator specifies that linkUp/linkDown traps should not be generated for the interface.

Using the Device-State profile

Every host interface or network interface (such as a T1 or E1 channel) on the TAOS unit has a Device-State profile, which stores the current state of the device and allows you to change it. For example, each eight port T1 card has 192 Device-State profiles (one for each T1 channel). Similarly, each modem card has 48 Device-State profiles (one for each modem).

To open one of the profiles, proceed as in the following example:

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

```
up-status = idle-up-status
reqd-state = up-reqd-state
```

In the output, the Device-State parameter shows the current operational state of the device, which can be down, up, or none. (None indicates that the device does not exist.)

The Up-Status parameter is ignored unless the device is up (Device-State=Up-Dev-State). If the device is up, Up-Status shows the status of the device, which can be idle, reserved (will not be used until all idle devices of the same type are in use), or assigned (in use).

The Reqd-State parameter indicates the required operational state of the device, which can be up or down. Changing this value initiates a state change for the device. The change is complete when Device-State changes to match Reqd-State. This setting is not persistent across system resets or power cycles. At system startup, the TAOS unit reinitializes the required state to match the actual state of the card.

Using the Device-Summary profile

The read-only Device-Summary profiles record the status and availability of the modem and HDLC resources on the TAOS unit. This profile is not stored in NVRAM, so it is not persistent across system resets or power cycles.

To view the modem resources on a TAOS unit, proceed in the following example:

```
admin> read device-summary modem
DEVICE-SUMMARY/modem read
admin> list
[in DEVICE-SUMMARY/modem]
device-class* = modem
total-count = 48
operational-count = 48
disabled-count = 0
```

The parameters in the Device-Summary profiles are described below:

Parameter	Description
Device-Class	The type of device. Values can be any of the following: • Modem • Unknown
Total-Count	Total number of devices in the specified class.
Operational-Count	Total number of devices in the specified class that are in the Up operational and Up administrative states.
Disabed-Count	Total number of devices in the specified class that are in the Down operational or Down administrative state.

Using the Slot-Info profile

The read-only Slot-Info profile stores information about each slot card that has successfully booted. This profile is not stored in NVRAM, so it is not persistent across system resets or power cycles. It is created when the slot card boots, and is deleted when the slot card is removed or when the TAOS unit's system is rebooted. It can be read by SNMP managers.

To view the Slot-Info profile, read and list its contents, as in the following example:

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

admin> list
[in SLOT-INFO/{ shelf-1 slot-1 0 }]
slot-address* = { shelf-1 slot-1 0 }
serial-number = 7470634
software-version = 7.0
software-revision = 4
software-level = b
hardware-level = 0
software-release = 1
```

For information about the parameters in the Slot-Info profiles, see the *APX 8000/MAX TNT Reference* .

Using Slot-State profiles

When you set the required operational state of a slot, the TAOS unit initiates a state change. In terms of settings, Current-State changes to match Reqd-State. This setting is not persistent across system resets or power cycles. At system startup, the TAOS unit reinitializes the required state to match the actual state of the card.

To read a Slot-State profile and display its contents, proceed as in the following example:

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

admin> list
slot-address* = { shelf-1 slot-1 0 }
current-state = oper-state-down
reqd-state = reqd-state-up
```

The slot address is the physical address of the slot, and cannot be set directly. The Current-State value shows the current operational state of the slot, and can be any of the states described below.

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 core.

State	Description
Oper-State-Pend	The slot is no longer down, but is not yet ready for normal operation. This value denotes a transitional state in which additional shelf-to-slot communications are required to make the slot fully operational.
Oper-State-Post	The slot is running a self-test.
Oper-State-None	The slot is empty.

The Reqd-State parameter indicates the required operational state of the slot, which can be up or down. Changing this value initiates a state change for the device. To use the Slot-State profile to change slot states, proceed as in the following example.

To bring a slot down:

```
admin> read slot-state {1 3 6}

SLOT-STATE/{ shelf-1 slot-3 6 } read

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

admin> write
SLOT-STATE/{shelf-1 slot-3 6} written
```

To bring the slot back up:

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

admin> write
SLOT-STATE/{ shelf-1 slot-3 6} written
```

Using DS3-ATM-Stat profiles

To display the status of the DS3-ATM line, read and list the DS3-ATM-Stat profile, as in the following example:

```
admin> read ds3-atm-stat {1 7 1}
DS3-ATM-STAT/{ shelf-1 slot-7 1 } read

admin> list
physical-address*={shelf-1 slot-7 1 }
line-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
```

The Line-State parameter shows the overall state of the line which can be any of the following:

State	Description
Does-Not-Exist	Link is not physically on board.
Disabled	Line disabled.
Loss-of-Signal	Near end has lost signal.
Loss-of-Frame	Near end has lost frame.
Yellow-Alarm	Receiving yellow-alarm from far end.
AIS-Receive	Receiving alarm indication signal
Active	Multipoint established.

The remaining parameters indicate the errors on the DS3 line. (Refer to RFC 1407 for complete description of these errors.)

Parameter	Description
F-Bit-Error-Count	Framing bit errors received since the last TAOS unit reset.
P-Bit-Error-Count	P-bit errors indicate that TAOS unit received a P-bit code on the DS3 M-frame that differs from the locally calculated code.
CP-Bit-Error-Count	For C-Bit-Parity lines indicates that number of parity errors since the last TAOS unit reset.
FEB-Error-Count	Far end block errors received since the last TAOS unit reset.
BPV-Error-Count	Bipolar Violation (BPV) errors may indicate that the line sent consecutive one bits with the same polarity. It could also mean that three or more consecutive zeroes were sent or an incorrect polarity.
Loss-of-Signal	True indicates a loss of signal. False indicates that the carrier is maintaining a connection.
Loss-of-Frame	True indicates a loss of framing. False indicates that the line is up and in frame.
Yellow-Receive	True indicates that the local device has received a Yellow Alarm indication. False specifies that the local device has not received a Yellow Alarm indication.
AIS-Receive	True indicates that the local device has received alarm indication signal. False indicates local device has not received and alarm indication signal.

Using T1-Stat profiles

The T1-Stat profile displays the status of the T1 lines and their channels. Each T1 line has a separate profile. When the T3 card is operational, it creates a T3-Stat profile and twenty-eight T1-Stat profiles, which store the current status of the DS3 and each component DS1.

To display the status of the T1 line, read and list the T1-Stat profile, as in the following example:

```
admin> read t1-stat {1 8 1}
T1-STAT/{ shelf-1 slot-8 1 } read

admin> list
physical-address* = { shelf-1 slot-10 7 }
line-state = disabled
channel-state = [ 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
```

The Line-State parameter shows the overall state of the line which can be any of the following:

State	Description
Does-Not-Exist	Link is not physically on board.
Disabled	Line disabled.
Loss-of-Sync	Red-alarm state, plus or minus.
Yellow-Alarm	Yellow-alarm state.
AIS-Receive	Receiving keep-alive signal
No-D-Channel	D-Channel failure.
Active	Multipoint established.

The channel-state parameter shows the state of each channel. Possible states are:.

State	Description
Unavailable	Not available.
Unused	Not in use.
Out-of-service	Out of service.
Nailed-up	Nailed.

The Error-Count parameter shows an error count for each channel.

For complete descriptions of the parameters in the T1-Stat profile, see to the *APX 8000/MAX TNT Reference.*

Using UDS3-Stat profiles

To display the status of the UDS3 line, read and list the UDS3-Stat profile, as in the following example:

```
admin> read uds3-stat {1 13 1}
UDS3-STAT/{ shelf-1 slot-13 1 } read

admin> list
line-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
```

The Line-State parameter shows the overall state of the line which can be any of the following:

State	Description
Does-Not-Exist	Link is not physically on board.
Disabled	Line disabled.
Loss-of-Signal	Near end has lost signal.
Loss-of-Frame	Near end has lost frame (also known as a red alarm).
Yellow-Alarm	Receiving yellow-alarm from far end.
AIS-Receive	Receiving alarm indication signal
Active	Multipoint established.

The remaining parameters indicate the errors on the DS3 line. (Refer to RFC 1407 for complete description of these errors.)

Parameter	Description
F-Bit-Error-Count	Framing bit errors received since the last TAOS unit reset.
P-Bit-Error-Count	P-bit errors indicate that TAOS unit received a P-bit code on the DS3 M-frame that differs from the locally calculated code.
CP-Bit-Error-Count	For C-Bit-Parity lines indicates that number of parity errors since the last TAOS unit reset.
FEB-Error-Count	Far end block errors received since the last TAOS unit reset.
BPV-Error-Count	Bipolar Violation (BPV) errors may indicate that the line sent consecutive one bits with the same polarity. It could also mean that three or more consecutive zeroes were sent or an incorrect polarity.
Loss-of-Signal	True indicates a loss of signal. False indicates that the carrier is maintaining a connection.
Loss-of-Frame	True indicates a loss of framing (also known as a red alarm). False indicates that the line is up and in frame.

Parameter	Description
Yellow-Receive	True indicates that the local device has received a Yellow Alarm indication. False specifies that the local device has not received a Yellow Alarm indication.
AIS-Receive	True indicates that the local device has received alarm indication signal. False indicates local device has not received and alarm indication signal.

Using the Call-Logging Server profile

You can control to which server the TAOS unit sends its logging information, provided that the Call-Logging profile is properly configured and enabled. Following are the relevant parameters, shown with default settings:

```
[in CALL-LOGGING]
call-log-server-index = host-1
```

Parameter	Description
Call-Log-Server-Index	Which of the configured `call-log-host-`*N* settings are used as the active call-logging server. Valid values are `host-1` (the default), `host-2`, and `host-3`. If the TAOS unit cannot authenticate the specified server, it attempts to use the next configured server.

To enable you to make this choice from an SNMP management station, the `callLoggingCurrentServerFlag` in the `callLoggingServerEntry`, which is in the Ascend call-logging MIB, is a read-write variable. The variable can be set to 1 (active) or 2 (standby). Following is the new definition:

```
callLoggingCurrentServerFlag OBJECT-TYPE
    SYNTAX  INTEGER {
                    active(1),
                    standby(2)
                    }
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION "Value indicates whether this entry is the current
                 Call Logging server or not. The standby(2) is not
                 set-able it is a value to report the standby status
                 of the Call Logging server."
    ::= { callLoggingServerEntry 2 }
```

Getting TAOS Unit Core Dumps

A

What is a core dump?

A TAOS core dump is a snapshot of the TAOS unit's shelf controller or slot card memory. A Lucent representative might ask you to obtain a core dump to help diagnose a problem. To get a core dump from the TAOS unit, you must use the Coredump command on the TAOS unit and the Ascendump utility on a local UNIX workstation.

The Coredump command controls how the TAOS unit generates core dumps. Ascendump controls how the TAOS unit core dumps are written to disk. You can specify that the core dump be collected whenever there is a fatal error, or you can get the core dump at any time from the server running Ascendump or from the TAOS unit itself.

The core-dump server can be connected through any LAN or WAN interface, and may be multiple hops away. The only restriction is that the data path from a crashing shelf or card must pass through shelves or cards that are still alive. The only exception is that a crashing Ethernet card can dump through its own Ethernet port, and a crashing Ethernet card can dump through one of its own Ethernet ports.

The TAOS unit uses UDP to write core dumps over the Ethernet.

Caution: Do not use core dumps unless specifically requested to by a Lucent representative.

Before you begin

Before installing and using the Ascendump utility, make sure you:

- Are familiar with the UNIX shell and know how to change directories, get information about files, use FTP, start processes, check available disk space, and so on.
- Have a local UNIX workstation running Solaris, SUNOS, or BSDI UNIX. (To use core dump on other versions of UNIX, contact technical support.)
- Have a minimum of 16Mb free disk space on the core-dump server. Note, however, that more space might be required under certain circumstances, such as if you are core dumping the core from the 32M DRAM card.
- Have downloaded the appropriate version of Ascendump from the Ascend FTP server (`ftp.ascend.com/pub/Utilities/coredump`).
- Have installed it in the directory from which you want to run it, and have used the `chmod +x` command to make the file executable.

The Ascendump daemon

Ascendump has the following syntax:

ascendump [**-v -r -c -u -p**] [**-n *email-recipient***] [**-s *slot***] [**-d *directory***] [***host***]

Option	Explanation
-v	accept
-r	Reset the TAOS unit after the core dump. This is the default in daemon mode.
-c	Do not reset the box after the core dump. This is the default in client mode.
-p	Print diagnostics to the terminal screen instead of Syslog. By default the server mode uses Syslog and the client mode prints to the terminal.
-s *slot*	Dump the memory of the card in slot number ***slot***. Network traffic will be forwarded through the shelf controller.
-u	Store files uncompressed. By default files are compressed with `gzip`.
-n *email-recipient*	Send an email notification to the specified email recipient. You can use this option more than once to designate multiple recipients. You can also use mail aliases.
-d *directory*	The directory path for writing the core dumps. The default is `/usr/ascendumps`.
host	

Coredump command

The Coredump command's syntax provides the following valid entries:

```
coredump
coredump enable | local | remote [server ]
coredump disable
coredump now
coredump trace
```

Syntax element	Description
coredump	
enable	Enables Coredump. If you do not specify a server, the core-dump server remains unchanged.
local	The most commonly used mode. In Local mode the Ascendump daemon listens for packets from the TAOS unit. The Ascendump daemon operates in server mode, and the TAOS unit core dump facility operates in client mode.
remote	Enables the Ascendump daemon to pull a core dump from the TAOS unit. Remotely initiated core dumps can be a security risk, so they are disabled by default. If you enable remote core dumps, they remain enabled only until the TAOS unit resets. That is, a reset restores the default setting.
server	The host that has the Ascendump daemon installed.
disable	Disables Coredump.
now	Forces an immediate core dump to the machine running the Ascendump daemon. This is useful for testing the core dump process.
trace	Toggles serial debug traces which can be useful to a Lucent representative if a customer is having difficulties.

Core dump naming conventions and file characteristics

The core-dump files use the following naming convention:

hostname-[*shelf, slot*]-*loadname-swversion-YYMMDD-HH:MM.gz*

where:

- *hostname* is the hostname or IP address of the Ascend unit.
- *shelf,slot* is the shelf and slot number of the card that has dumped its core. (This applies only to the TAOS unit.)
- *loadname* is the name of the software load running on the TAOS unit.
- *swversion* is the version of the software load running on the TAOS unit.
- *yymmdd-hh:mm* is a date and time stamp. Each dump file can be four to eight megabytes in size.

For example:

```
tnt10.abc.com-1,3-tntmdm56k-1.3Ap22-980101-13:42.gz
```

When transferring the core-dump files via FTP, use binary mode.

Trigger events

The events that normally trigger a core dump are system or slot-card resets. These usually show up in the fatal error log either as “Fatal Errors” or “Operator Resets.” You cannot specify the types of events that trigger core dumps.

UDP port numbers

The TAOS unit listens for core dumps on the UDP port given by the following formula:

10,000 + (*shelf-number* *100) + *slot-number*

For example, for a card on shelf 1, slot 5, the UDP port for the core dump is 10105. For the shelf controller (slot number 17) on shelf 1, the UDP port for the core dump is 10117. Similarly, the shelf controller on shelf 8 uses UDP port 10817.

Examples

This section uses examples to show how to get core dumps from the TAOS unit.

Enabling Ascendump

To start the Ascendump daemon, proceed as in the following example:

```
% ./ascendump -v -u -d /usr/ascendumps
```

This example runs the daemon in verbose mode and will write the core dumps in uncompressed format to `/usr/ascendumps`.

Enabling core dumps on the TAOS unit

In the following example, the TAOS unit writes the core dump to the host at 172.31.4.34 whenever there is a fatal error:

```
admin> coredump local 172.31.4.34
coreDump: Sending arp request...
core dump server is ‘172.31.4.34 ip=[172.31.4.34/16],
mac=[00:60:83:7d:15:8f]
coredump over UDP is enabled locally only with server
172.31.4.34
```

Pulling a core dump from the TAOS unit

In the following example, the TAOS unit enables the Ascendump daemon to solicit a dump from the TAOS unit. The Ascendump daemon is operating in client mode, and the TAOS unit's core-dump facility is operating in server mode.

```
admin> coredump remote
```

Once remote core dumps are enabled on the TAOS unit, an administrator can "pull" a core dump as in the following example:

```
% ascendump -d /usr/ascendumps tnt10
```

where `/usr/ascendumps` is the directory on the Ascendump server and `tnt10` is the name of the TAOS unit from which to get the core dump.

Initiating an immediate core dump

In the next example, an administrator forces an immediate core dump:

```
admin> coredump now
```

Getting core dumps from slot cards

You can configure the Ascendump daemon to request a core dump from a particular TAOS unit's slot. In the following example the modem card in slot 4 of the TAOS named `tnt10` will write to the Ascendump server when it crashes:

1. After opening a session with the card, execute Coredump with the remote option:

   ```
   modem-4> coredump remote
   ```

2. Start the Ascendump daemon in slot mode:

   ```
   % ./ascendump -v -u -s 4 -d /usr/ascendump
   ```

Disabling core dumps

To disable core dumps on the TAOS :

```
admin> coredump disable
coredump over UDP is disabled
```

Fatal error log and core dumps

The fatal-error log lists the pseudouser `coredump` as the responsible user when the shelf controller resets after a core dump. For example:

```
OPERATOR RESET:  Index:  99  Revision: 1.3Ap8  Shelf 1 (tntsr)
        Date: 09/12/1997.       Time: 15:52:43
        Reset from unknown, user profile coredump.
```

Troubleshooting core dumps

Take the following steps if you have difficulty setting up the TAOS unit core dumps:

1. If you have previously installed Ascendump in `inetd.conf`, temporarily disable it now, by commenting out the Ascendump line, then, logged in as root, send the `SIGHUP` command to `inetd`.
2. Change to a writable directory, and enter **`ascendump -p -v -d`**
   - **`-v`** is verbose mode, which prints progress reports as the core dump proceeds, keeps the daemon in the foreground, and handles dumps serially, all of which make debugging easier.
   - **`-p`** prints diagnostics to `stderr` instead of through Syslog (whose output on most systems goes to `/var/adm/messages`).
   - **`-d`** puts the dump files in the current directory.

   Performing initial tests in this manner saves time by making failures immediately diagnosable.
3. On the TAOS , enable core dumps to the server machine that is running Ascendump.
4. Look for old debug profiles by entering, **`dir debug`** from the shelf controller.

   The only reason to have a debug profile on a card other than the shelf controller is to override the settings for the shelf controller. Unless you want to do that, you should define a single debug profile for the shelf controller and delete all other debug profiles.
5. Test slot-card dumps by opening a session with a slot card. You should perform a test dump first on the T1 or E1 card, if present, because these cards have smaller memories, and are quick to reboot.
6. From the session on the card, enter **`coredump`** to check the status of core dump. The resulting output should report that core dump is enabled and that dumps will be directed to the server you specified in step 3.
7. Force a core dump with the following command:

   `coredump now`

   Ascendump should print something like this:

```
$ ascendump -p -v -d

ascendump: Dumping compressed DRAM image to ‘./tnt10.abc.com-1,11-
tnt8t1-1.3Ae0-971022-11:17.gz’
Section ‘.data’: dumping 2048 pages from address 0x80000000
.......1 Mb.......2 Mb
```

Occasionally, core dump fails because `gzip` is not installed or not in the user’s path. If this is the case, you should download `gzip-1.2.4.tar.gz` from any GNU FTP mirror site, then compile and install it, or use the `-u` (uncompressed) option in the Ascendump command line.

If you still have unexplained failures, run `tcpdump` or `snoop` or a packet sniffer on the Ethernet segment attached to the TAOS that is in the route to the dump server. Do the same on the Ethernet segment attached to the dump server in the route to the TAOS .

Coredump uses UDP, so filter UDP packets. If there’s too much UDP traffic, you might want to filter on port-number ranges as well. For information about the UDP port core dump uses, see “UDP port numbers” on page A-4.

Proceed to testing more cards by opening CLI channels to them and using the `coredump now` command. Finish by testing Coredump from the shelf controller.

Once you have established that core dump works, reinstate your `inetd.conf` entry, if present, or add one if necessary. Be sure that the entry points to the same Ascendump binary that you just tested.

Here is a sample `inetd.conf` entry:

```
ascendump dgram udp nowait root /usr/local/bin/ascendump ascendump -n
dump-notify
```

The `-n dump-notify` argument tells Ascendump to send email to the email alias `dump-notify` whenever a core dump is captured.

Log Messages on the TAOS Unit

B

The TAOS unit logs fatal and warning error messages to the fatal error log. If the system crashes before creating a log entry, it prints a stack trace to the console serial port. System-status messages, however, go to the Syslog host (if enabled) and the Status log.

Fatal and warning error messages

Each time the TAOS unit reboots, it logs a fatal error message to the fatal error log. The fatal error log also notes Warnings, which indicate situations that did not cause the TAOS unit to reset. Development engineers use Warnings for troubleshooting purposes. When a Warning occurs, the TAOS unit has detected an error condition and has recovered from it. Available flash space limits the number of entries in the fatal error log, and entries rotate on a First-in, First-out (FIFO) basis. You can clear the log by using the Clr-History command.

Format of fatal and warning error messages

Fatal and warning messages have the format shown in the following example:

```
WARNING:  Index: 171  Revision: 8.0.2 Slot 9/2 (csm3v)
Date: 12/22/1999.       Time: 20:57:59
Location: e0020b54 e006f568 e005d6b8 e005fd90 e005e4dc e00770a8
```

The first line indicates the type of error (fatal or warning), the index number of the error, the software revision number, the shelf and slot on which the error occurred,

The second line shows the date and time of the error.

The third line displays the top six program counter addresses from the execution stack active at the time of the crash.

Definitions of fatal errors

Following are definitions, by index number, of the fatal errors that the TAOS unit can report. If you experience a fatal error, contact Lucent Technical Support.

Index	Definition
1	Assert invoked during program execution. An Assert has been placed in the code. This problem can be either hardware related or software related.
2	Out of memory during memory allocation This is an out-of-memory condition, sometimes termed a memory leak.
4	Switch type bad
5	LIF error
6	LCD error
7	ISAC (BRI) timeout BRI physical layer timeout.
8	Processor exception A processor-exception error caused the reset.
9	Invalid task switch (EXEC)
10	No mail descriptor (EXEC) This reset occurs if the TAOS unit tries to allocate a mail message when there are none left. The cause is usually a memory leak.
11	No mail buffer memory (EXEC)
12	No task to run (EXEC)
13	No timer memory (EXEC)
14	No timer pool (EXEC)
15	Wait called while in critical section (EXEC)
16	DSP not responding
17	DSP protocol error
18	DSP internal error
19	DSP loss of sync
20	DSP unused
21	DDD not responding
22	DDD protocol error
23	X25 buffer error
24	X25 init error
25	X25 stack error

Index	Definition
27	Memory allocation of zero length
28	Memory allocation of negative length
29	Task infinite loop The reset was the result of a software loop.
30	Too large memory copy
31	Magic sequence missing (MEMCPY)
32	Wrong magic sequence (MEMCPY)
33	Bad start address (MEMCPY)
34	IDEC timeout
35	EXEC restricted
36	Stack overflow
37	DRAM card error Indicates that a DRAM card of unknown size is inserted in the DRAM slot or that the DRAM card failed POST. Applies to the Pipeline 220 only.
40	Protection fault
99	Operator reset This reset is logged immediately before the TAOS unit goes down. Instead of a standard stack backtrace, the message includes the active security-profile index. 0 (zero) indicates an unknown security profile. On the TAOS unit, the Default profile is number 1, and the Full Access profile is number 9.
100	System up As a complement to entry 99, this entry is logged as the TAOS unit is coming up. For a normal, manual reset, you should see a fatal error 99 followed by a fatal error 100.

Definitions of warning messages

Warnings are not the results of reset conditions. Most are detected problems from which the TAOS unit typically recovers fully. Following are the definitions, by index number, of the warnings the TAOS unit can report. Warning messages, by themselves, are not necessarily cause for concern. They are used by development engineers to determine the cause of fatal errors. Contact Lucent technical support if warning messages are accompanied by fatal errors.

Index	Definition
101	Buffer already in use
102	Buffer belongs to wrong pool
103	Buffer belongs to wrong heap

Index	Definition
104	Buffer not previously allocated
	This warning can be logged under different conditions. For example, double freeing of memory and low-memory conditions can both generate a warning 104.
105	Buffer bad memory allocation
106	Buffer belongs to bogus pool
107	Buffer belongs to bogus heap
	Memory management code (or other modules) detected that the buffer header of what should have been a free buffer was corrupted by the previous overwrite.
108	Buffer negative length memory allocation
	A negative length request was made to the memory allocation code.
109	Buffer zero length memory allocation
	This warning is similar to Warning 108, except that a zero length request is made to the memory allocation code.
110	Error in buffer boundary
111	Error buffer too big
	Indicates that a software routine has tried to allocate a block of memory greater than 64Kbytes.
112	Error buffer null
113	Error buffer segment count zero
114	Error buffer trailer magic
115	Error in buffer trailer
116	Error in buffer trailer length
117	Error in buffer trailer user magic
118	Error buffer write after free
119	Error buffer not in use
120	Error buffer magic in memory copy
121	Error next buffer magic in memory copy
130	PPP async buffer in use
	Indicates a PPP error.
140	Error no timers
145	LCD memory allocation failure
	Indicates that a memory-copy routine was called, but the source buffer was much larger than expected.
150	Error memory copy too large
151	Error memory copy magic missing

Index	Definition
152	Error memory copy wrong magic
153	Error memory copy bad start address
154	WAN buffer leak Indicates an error in the WAN drivers.
160	Error in terminal-server state Indicates an error in the WAN drivers.
161	Error in terminal server semaphore
165	Error in telnet free driver
170	STAC timeout Indicates a hardware error in the STAC compression chip.
171	STAC data not owned Error in the STAC compression chip.
175	EXEC failure Indicates that there is insufficient memory to start a new task.
176	EXEC restricted
177	EXEC no mailbox
178	EXEC no resources
179	Unexpected error
180	Channel map stuck Caused by a missing channel on a T1/PRI line.
181	Channel display stuck
182	New call without disconnect request Indicates that a Disconnect message to the Central Office (CO) was not sent. The problem can be caused by conditions on the TAOS unit or at the CO. When the TAOS unit encounters the condition, it assumes the CO is correct, and answers the call.
183	New call without disconnect response
184	Disconnect request dropped
185	Spyder buffer error
186	Spyder descriptor error
190	TCP send buffer too big
191	TCP sequence gap
192	TCP too much data
193	TCP write attempt too large
194	TCP options bad

Index	Definition
195	Modem message parsing failed
301	TACACS Plus pointer inconsistency
302	TACACS Plus index inconsistency
303	TACACS Plus TCP inconsistency
304	TACACS Plus TCP out-of-range socket
305	TACACS Plus socket mismatch
306	TACACS Plus unexpected authentication state
381	Error in filter list
382	Error no count in filter list
383	Error mismatch count filter list
550	No Ethernet transmit buffer
1001	Waiting for Ethernet controller
1002	Ethernet ACK command failed
1003	Ethernet reset invoked
1006	Ethernet controller unavailable (wait fail)
1010	Bad Ethernet transmit interrupt
1011	Ethernet transmit not completed

Fatal crash information on console

If the TAOS unit crashes without being able to write to the fatal error log, it prints a stack trace to the console serial port at the bit rate defined in the Serial profile. The trace reports the following information:

`FE: N, Load: loadname, Version: version`
`Stack trace: 0xaddr-0 0xaddr-1 0xaddr-2 0xaddr-3 0xaddr-4 0xaddr-5`

The first line indicates the number of the error and the software revision number.

The second line displays the top six program counter addresses from the execution stack active at the time of the crash.

Syslog messages

Syslog offloads to a host computer, known as the Syslog host. The Host parameter in the Log profile specifies the Syslog host, which saves the system status messages in a log file.

See the UNIX man pages about `logger(1)`, `syslog(3)`, `syslog.conf(5)`, and `syslogd(8)` for details of the `syslog` daemon. The Syslog function requires UDP port 514.

The TAOS unit can report the following session data about various errors logged via Syslog:

Data	Description
`[shelf/slot/line/channel]`	Physical channel identifier.
`[MBID xxx]`	Session identifier.
`[name]`	The authenticated name.
`[ calling -> called ]`	The calling number or the called number, or both.
`Progress code`	A TAOS unit-specific code indicating the progress of the call. (For a list of progress codes, see the *APX 8000/MAX TNT Reference*.)
`Disconnect code`	A TAOS unit-specific code indicating the reason the call was disconnected. (For a list of disconnect codes, see the *APX 8000/MAX TNT Reference*.)

For a given session identifier, multiple physical channel identifiers are possible. For example, one identifier might be for a T1 lineThis is shown in the sample log below, in which messages include the MBID, DNIS, and CLID in brackets. In this example, slot 1/2 is an 8T1 card, and slot 1/3 is a 48-modem card.

```
...: [1/2/1/2] [MBID 1; 9995551212 -> 7898] Incoming Call
...: [1/3/1/0] [MBID 1; 9995551212 -> 7898] Assigned to port
...: [1/2/1/2] [MBID 1; 9995551212 -> 7898] Call Connected
...: [1/3/1/0] [MBID 1] [johnc-pc] LAN session up: <johnc-pc>
...: [1/3/1/0] [MBID 1] [johnc-pc] LAN session down: <johnc-pc>
...: [1/3/1/0] [MBID 1; 9995551212 -> 7898] Call Terminated
...: [1/3/1/0] [MBID 1] [johnc-pc] : STOP: 'johnc-pc'; cause 45.;
progress 60.; host 10.1.26.2
```

End of call information

If the Call-Info parameter is set to End-of-Call, the TAOS unit reports the following information to Syslog at the end of each authenticated call:

- Station name
- Calling phone number
- Called phone number
- Encapsulation protocol
- Data rate (in bits per second)
- Progress code and 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

The following example of a Syslog message shows the information it provides about the terminated call:

```
"Conn=("cjones-p50" 5106785291->? PPP 56000 60/185) \
Auth=(3 347/12 332/13) \
Sess=(1 643/18 644/19), Terminated"
```

The information also appears in the connection-status window, and is logged as a message at level Info.

If some of the information is not available, that field displays either a question mark (for strings) or a zero (for numerals).

DNIS and CLID information

Syslog messages pertaining to a call display DNIS and CLID information, provided that the information is known. Following is an example that shows the DNIS 7895 in Syslog messages:

```
LOG info, Shelf 1, Controller, Time: 17:48:56--
† shelf 1, slot 1, line 1, channel 6, dnis 7895, Incoming Call, MBID
001

LOG info, Shelf 1, Controller, Time: 17:48:56--
† shelf 1, slot 2, dnis 7895, Assigned to port, MBID 001

LOG info, Shelf 1, Controller, Time: 17:48:57--
† shelf 1, slot 1, line 1, channel 6, dnis 7895, Call Connected, MBID
001

LOG warning, Shelf 1, Controller, Time: 17:49:20--
† shelf 1, slot 1, line 1, channel 6, dnis 7895, Call Disconnected

LOG info, Shelf 1, Controller, Time: 17:49:20--
† shelf 1, slot 2, Call Terminated
```

Syslog messages initiated by a Secure Access Firewall

Depending on the settings specified in Secure Access Manager (SAM), the TAOS unit might generate Syslog packets about packets detected by Secure Access Firewall. By default, SAM specifies generation of a Syslog message about every packet blocked by the firewall. All messages initiated by a firewall are in the following format:

date time router name LUCENT*: interface message*

- *date* is the date the message was logged by syslog.
- *time* is the time the message was logged by syslog.
- *router* is the router this message was sent from.
- *interface* is the name of the interface (`ie0`, `wan0`, and so on), unless a call filter logs the packet as it brings up the link, in which case the word `call` appears.
- The *message* format has a number of fields, one or more of which may be present.

For more information on syslog message fields for Secure Access Firewalls, refer to Table B-1 on page B-9. The message fields appear in the following order:

```
protocol local direction remote length frag log tag
```

Table B-1. Syslog message fields for Secure Access Firewalls

Field	Description
protocol	Can be the four hexadecimal character Ether Type or one of the following network protocol names: ARP, RARP, IPX, Appletalk. For IP protocols, the field contains either the IP protocol number (up to 3 decimal digits) or one of the following names: IP-in-IP, TCP, ICMP, UDP, ESP, AH. In the special case of ICMP, the field also includes the ICMP Code and Type ([Code]/[Type]/icmp).
local	For non-IP packets, `local` is the source Ethernet MAC address of transmitted packets and the destination Ethernet MAC address of received packets. For a nonbridged WAN connection, the two MAC addresses are zeros. For IP protocols, `local` is the IP source address of transmitted packets and the IP destination address of received packets. In the case of TCP or UDP, it also includes the TCP or UDP port number ([IP-address];[port]).
direction	An arrow (<- or ->) indicating the direction in which the packet was traveling (receive and send, respectively).
remote	For non-IP protocols, `remote` has the same format that *`local`* has non-IP packets, but `remote` shows the destination Ethernet MAC address of transmitted packets and the source Ethernet MAC address of received packets. For IP protocols, `remote` has the same format as `local` but shows the IP destination address of transmitted packets and the IP source address of received packets.
length	The length of the packet in octets (8-bit bytes).
frag	Indicates that the packet has a nonzero IP offset or that the IP More-Fragments bit is set in the IP header.
log	Reports one or more messages based upon the packet status or packet header flags. The packet status messages include: • corrupt—the packet is internally inconsistent • unreach—the packet was generated by an “unreach=” rule in the firewall • !pass—the packet was blocked by the data firewall • bringup—the packet matches the call firewall • !bringup—the packet did not match the call firewall • TCP flag bits that will be displayed include syn, fin, rst. • syn is will only be displayed for the initial packet which has the SYN flag and not the ACK flag set.
tag	contains any user defined tags specified in the filter template used by SAM.

The backoff queue error message in the Syslog file

Accounting records are kept until they are acknowledged by the accounting server. Up to 100 unacknowledged records are stored in the backoff queue. If the unit never receives an acknowledgment to an accounting request, it will eventually run out of memory. In order to keep this situation from the occurring, the unit deletes the accounting records and displays this error message in the syslog file:

```
Backoff Q full, discarding user username
```

This error generally occurs for one of the following reasons:

- You enabled RADIUS accounting on the TAOS unit, but not on the RADIUS server.
- The Acct-Port or Acct-Key are incorrect. The Acct-Key must match the value assigned in the RADIUS clients file or the TACACS+ configuration file.
- You are using a PortMaster® server rather than a TAOS unit server.

Flash card error messages

When a Load, Format, or Dircode command fails, the TAOS unit logs the messages described in this section.

Load command messages

Table B-2 lists the error messages that might appear when using the Load command:

Table B-2. Load command error messages

Error message	Description
`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 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.

Format command messages

Table B-3 lists the error messages might appear when using the Format command:

Table B-3. Format command error messages

Error message	Description
`error: flash card N is not present`	No flash card is detected in the specified slot (1 or 2).
`error: flash card N is unavailable`	The flash card in the specified slot is already being formatted, is just coming up, or is in an error condition.
`error: flash card N is write-protected`	The write-protect switch is set on the card in the specified slot (1 or 2).
`error: flash card N is currently in use`	One or more images on the flash card are being read by a slot card in the LOAD state or are being written as part of a code download.

Dircode command messages

Table B-4 lists the error messages might appear when using the Dircode command:

Table B-4. Dircode command error messages

Error message	Description
`Card N is not formatted for use with this system`	The flash card is blank, corrupted, or formatted for another environment, such as DOS. To use this card, you must issue a Format command first.
`Card N is temporarily unavailable`	The flash card is currently coming up or is being formatted.
`Card N is unavailable`	The flash card experienced an error and is inaccessible.Check that the card is inserted properly.

PPP Decoding Primer

C

Many of the diagnostic commands display raw data. This Primer is designed to assist you in decoding PPP, MP, MP+ and BACP negotiations. The negotiations can be logged with the diagnostic commands `PPPDump`, `WANDisplay`, `WANDSess`, `WANNext` or `WANOpen`. For more detailed information than this guide provides, refer to the specific RFCs. A partial list of pertinent RFCs appears at the end of this guide.

Breaking down the raw data

An important concept to keep in mind is that each device negotiates PPP independently, so the options might be identical for each direction of the session.

During PPP negotiation, frame formats in the various protocols are very similar. They share the following characteristics:

- `FF 03` indicating it is a PPP frame.
- A two-byte Protocol Identifier.
- A one-byte Packet Format ID number
- A one-byte ID number.
- A two-byte length.
- Options for the protocol.

Below is a table of the most common protocols you'll see in Lucent diagnostic traces:

Identifier:	**Description:**
`C0 21`	Link Control Protocol (LCP)
`C0 23`	Password Authentication Protocol (PAP)
`C2 23`	Challenge Handshake Authentication Protocol (CHAP)
`80 21`	Internet Protocol (IP)
`80 29`	Appletalk Protocol
`80 2B`	Novell's Internetwork Packet Exchange (IPX)
`80 31`	Bridging PDU

Identifier:	Description:
80 FD	Compression Control Protocol (CCP)

Following are the packet formats:

Packet Format ID	Description
01	Configure Request
02	Configure Acknowledgment
03	Configure Non-Acknowledgment
04	Configure Reject
05	Terminate Request
06	Terminate Acknowledgment
07	Code Reject
08	Protocol Reject
09	Echo Request
0A	Echo Reply
0B	Discard Request

Note: If a packet received from the wan fails the Cyclic Redundancy Check (CRC) the display is similar to the following, where RBAD denotes Received BAD:

```
RBAD-27:: 8712 octets @ 26CFE8
[0000]: fe dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0010]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0020]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0030]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
```

Annotated traces

Use the following traces as guides to help you decode other traces.

LCP Configure Request - MP+, MRU of 1524, MRRU of 1524 and End Point Discriminator using the device's MAC address:

```
XMIT-3:: 29 octets @ 2C2E94
[0000]: ff 03 c0 21 01 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

This is a second LCP Configure Request from the same device. Everything in the packet is identical to the previous packet, except the ID number has incremented from 01 to 02:

```
XMIT-3:: 29 octets @ 2C2E94
[0000]: ff 03 c0 21 01 02 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

LCP Configure Request - CHAP authentication, Magic number

```
RECV-3:: 19 octets @ 2BEB8C
[0000]: ff 03 c0 21 01 60 00 0f 03 05 c2 23 05 05 06 4e
[0010]: 36 c9 05
```

LCP Configure Acknowledgment - This device will authenticate using CHAP. The Magic number is also acknowledged:

```
XMIT-3:: 19 octets @ 2C2E94
[0000]: ff 03 c0 21 02 60 00 0f 03 05 c2 23 05 05 06 4e
[0010]: 36 c9 05
```

LCP Configure Reject - MP+, MRU of 1524, MRRU of 1524 and End Point Discriminator.

This rejection shows two things. It shows that the remote side does not support MP+ or MP, since MP+ and the MRRU were rejected. This will have to be a PPP connection. Also, since the MRU of 1524 was rejected, the default of 1500 is assumed. There needs to be an MRU, so a rejection of a given value only means to use the default value.

At this point, this device will need to retransmit another LCP Configure Request, removing all the rejected options.

```
RECV-3:: 29 octets @ 2BF1A4
[0000]: ff 03 c0 21 04 02 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

LCP Configure Request - Note all values that were previously rejected are no longer in the packet:

```
XMIT-3:: 8 octets @ 2C2E94
[0000]: ff 03 c0 21 01 04 00 04
```

LCP Configure Acknowledgment -

```
RECV-3:: 8 octets @ 2BF7BC
[0000]: ff 03 c0 21 02 04 00 04
```

At this point, since both sides have transmitted LCP Configure Acknowledgments, LCP is up and the negotiation moves to the authentication phase.

This device receives a CHAP challenge from the remote end:

```
RECV-3:: 21 octets @ 2BFDD4
[0000]: ff 03 c2 23 01 01 00 11 04 4e 36 c9 5e 63 6c 63
[0010]: 72 34 30 30 30
```

This device transmits its encrypted user name and password:

```
XMIT-3:: 36 octets @ 2C2E94
[0000]: ff 03 c2 23 02 01 00 20 10 49 b8 e8 54 76 3c 4a
[0010]: 6f 30 16 4e c0 6b 38 ed b9 4c 26 48 5f 53 65 61
[0020]: 74 74 6c 65
```

The remote device sends a CHAP Acknowledgment:

```
RECV-3:: 8 octets @ 2C03EC
[0000]: ff 03 c2 23 03 01 00 04
```

At this point, the negotiation moves from authentication to negotiation of Network Control Protocols (NCPs). The TAOS unit supports Bridging Control Protocol (BCP), IPCP, IPXCP and ATCP.

IPCP Configure Request - Van Jacobsen Header Compression, IP address of 1.1.1.1

```
RECV-3:: 20 octets @ 2C0A04
[0000]: ff 03 80 21 01 e3 00 10 02 06 00 2d 0f 00 03 06
[0010]: 01 01 01 01
```

BCP Configure Request -

```
RECV-3:: 8 octets @ 2C101C
[0000]: ff 03 80 31 01 55 00 04
```

IPCP Configure Request - IP address of 2.2.2.2

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 01 01 00 0a 03 06 02 02 02 02
```

IPCP Configure Reject - Van Jacobsen Header Compression. The remote device should send another IPCP Configure Request and remove the request to do VJ Header Compression:

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 04 e3 00 0a 02 06 00 2d 0f 00
```

BCP - Protocol Reject. This local device is not configured to support bridging.

```
XMIT-3:: 8 octets @ 2C2E94
[0000]: ff 03 80 31 08 55 00 04
```

IPCP Configure Acknowledgment

```
RECV-3:: 14 octets @ 2C1634
[0000]: ff 03 80 21 02 01 00 0a 03 06 01 01 01 01
```

IPCP Configure Request - Note VJ Header Compression is not requested this time.

```
RECV-3:: 14 octets @ 2C1C4C
[0000]: ff 03 80 21 01 e4 00 0a 03 06 02 02 02 02
```

IPCP Configure Acknowledgment

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 02 e4 00 0a 03 06 01 01 01 01
```

At this point, a PPP connection has been successfully negotiated. The caller was successfully authenticated by means of CHAP and IPCP was the only successfully configured NCP. IPX, Appletalk and bridging will not be supported during this session.

Below are two packets used in determining link quality:

LCP Echo request packet

```
RECV-3:: 16 octets @ 2BEB8C
[0000]: ff 03 c0 21 09 01 00 0c 4e 36 c9 05 00 00 00 00
```

LCP Echo Response

```
XMIT-3:: 16 octets @ 2C2E94
[0000]: ff 03 c0 21 0a 01 00 0c 00 00 00 00 00 00 00 00
```

Example of MP+ call negotiation

LCP Configuration Request - MP+, MRU of 1524, MRRU of 1524, End Point Discriminator using the device's MAC address:

```
XMIT-31:: 29 octets @ D803C
[0000]: ff 03 c0 21 01 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 5c d3 71
```

LCP Configure Request - MP+, MRU of 1524, PAP authentication is required. MRRU of 1524, End Point Discriminator using the device's MAC address:

```
RECV-31:: 33 octets @ D4FBC
[0000]: ff 03 c0 21 01 01 00 1d 00 04 00 00 01 04 05 f4
[0010]: 03 04 c0 23 11 04 05 f4 13 09 03 00 c0 7b 53 f0
[0020]: 7a
```

LCP Configuration Acknowledgment -

```
RECV-31:: 29 octets @ D55CC
[0000]: ff 03 c0 21 02 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 5c d3 71
```

LCP Configuration Acknowledgment -

```
XMIT-31:: 33 octets @ D803C
[0000]: ff 03 c0 21 02 01 00 1d 00 04 00 00 01 04 05 f4
[0010]: 03 04 c0 23 11 04 05 f4 13 09 03 00 c0 7b 53 f0
[0020]: 7a
```

At this point, LCP is up. Next is the authentication phase. The local device agreed to authenticate using PAP, so it should transmit its user name and password. Note that it is not encrypted, and user name and password can be decoded very easily:

PAP Authentication Request - User name is shown in hexadecimal and must be converted to ascii. User name is 0x6a 0x73 0x6d 0x69 0x74 0x68 (jsmith) and password is 0x72 0x65 0x64 (red):

```
XMIT-31:: 20 octets @ D803C
[0000]: ff 03 c0 23 01 01 00 10 06 6a 73 6d 69 74 68 03 72
[0010]: 65 64
```

PAP Authentication Acknowledgment -

```
RECV-31:: 9 octets @ D5BDC
[0000]: ff 03 c0 23 02 01 00 05 00
```

Authentication is successful. Final negotiation determines protocols to be supported over the link.

Note: MP+ was negotiated, and both devices begin sending MP+ packets from here. The data portion of the packet is identical to PPP, but there is an 8-byte MP+ header instead of the 2-byte PPP header:

In the following packet, `00 3d` is the designation for a Multilink packet. The next byte designates whether this packet is fragmented. The next three bytes are the sequence number. You'll see them increment by one for each packet sent or received.

Next, the 80 31 01 designates this as a BCP Configure Request:

```
RECV-31:: 20 octets @ D61EC
[0000]: ff 03 00 3d c0 00 00 00 80 31 01 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Request:

```
XMIT-31:: 20 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 00 80 31 01 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Acknowledgment:

```
XMIT-31:: 20 octets @ D864C
[0000]: ff 03 00 3d c0 00 00 01 80 31 02 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Acknowledgment:

```
RECV-31:: 20 octets @ D67FC
[0000]: ff 03 00 3d c0 00 00 01 80 31 02 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP is up and the session begins sending bridged traffic. No routed protocols were negotiated.

The following packets are sent as part of the MP+ protocol. They are sent at one-second intervals. These packets are used by each unit to validate the existence of the link. It gives the devices a secure way to determine whether the link is still up, even if there is no data traffic passing between the devices.

```
RECV-31:: 8 octets @ D5BDC
[0000]: ff 03 00 3d c0 00 00 05
XMIT-31:: 8 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 04
RECV-31:: 8 octets @ D61EC
[0000]: ff 03 00 3d c0 00 00 06
XMIT-31:: 8 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 05
```

The following RFCs provide more detail about the subjects listed in their titles:

Identifier	Title
RFC1378	PPP AppleTalk Control Protocol (ATCP)
RFC1552	PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC1638	PPP Bridging Control Protocol (BCP)
RFC1661	Point-to-Point Protocol (PPP)
RFC1934	Multilink Protocol Plus (MP+)
RFC1962	PPP Compression Control Protocol (CCP)
RFC1974	PPP Stac LZS Compression Protocol
RFC1989	PPP Link Quality Monitoring

Identifier	Title
RFC1990	PPP Multilink Protocol (MP)
RFC1994	PPP Challenge Handshake Authentication Protocol

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W