ADTRAN

TOTAL ACCESS 600 SERIES
System Manual

Total Access 600R

Total Access 604

Total Access 608

Total Access 612

Total Access 616

Total Access 624

61200624L1-1B
June 2004

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

Total Access® is a registered trademark of ADTRAN, Inc.

To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

About this Manual

This manual provides a complete description of the Total Access 6XX system and system software. The purpose of this manual is to provide the technician, system administrator, and manager with general and specific information related to the planning, installation, operation, and maintenance of the Total Access 6XX. This manual is arranged so that needed information can be quickly and easily found.

901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000

© 2004 ADTRAN, Inc.
All Rights Reserved.
Printed in U.S.A.

Revision History

Document Revision	Date	Description of Changes
A	October 2002	Initial Release
B	May 2004	Updated to include menu changes for firmware release.

Conventions

NOTE	*Notes provide additional useful information.*

CAUTION	*Cautions signify information that could prevent service interruption.*

WARNING	*Warnings provide information that could prevent damage to the equipment or endangerment to human life.*

Safety Instructions

When using your telephone equipment, please follow these basic safety precautions to reduce the risk of fire, electrical shock, or personal injury:

1. Do not use this product near water, such as a bathtub, wash bowl, kitchen sink, laundry tub, in a wet basement, or near a swimming pool.

2. Avoid using a telephone (other than a cordless-type) during an electrical storm. There is a remote risk of shock from lightning.

3. Do not use the telephone to report a gas leak in the vicinity of the leak.

4. Use only the power cord, power supply, and/or batteries indicated in the manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for special disposal instructions.

Save These Important Safety Instructions

© 2004 ADTRAN, Inc.   61200624L1-1B

FCC-Required Information

FCC regulations require that the following information be provided in this manual:

1. This equipment complies with Part 68 of FCC rules and requirements adopted by ACTA. On the equipment housing is a label that contains, among other information, a product identifier in the format US: AAAEQ##TXXXX. If requested, provide this information to the telephone company.

2. If this equipment causes harm to the telephone network, the telephone company may temporarily discontinue service. If possible, advance notification is given; otherwise, notification is given as soon as possible. The telephone company will advise the customer of the right to file a complaint with the FCC.

3. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of this equipment. Advance notification and the opportunity to maintain uninterrupted service are given.

4. 4.If experiencing difficulty with this equipment, please contact ADTRAN for repair and warranty information. The telephone company may require this equipment to be disconnected from the network until the problem is corrected or it is certain the equipment is not malfunctioning.

5. This unit contains no user-serviceable parts.

6. An FCC compliant telephone cord with a modular plug is provided with this equipment. This equipment is designed for connection to the telephone network or premises wiring using an FCC compatible modular jack, which is compliant with Part 68 and requirements adopted by ACTA.

7. The following information may be required when applying to your local telephone company for leased line facilities.

Product Listing	Registration Number	Service Type	REN/SOC	FIC	USOC
TA 600/604/608 Series T1 Products	US:HDCDENAN4213680L1	1.544 Mbps - SF 1.544 Mbps - SF and B8ZS	6.0N	04DU9-BN 04DU9-DN 04DU9-1KN 04DU9-1SN	RJ-48C
TA 612/616/624 Series T1 Products	US: HDCDENAN4213616L1	1.544 Mbps - ESF 1.544 Mbps - ESF and B8ZS			
TA 600 Series SDSL, SHDSL Products	HDCUSA-44560-OT-N	Analog Loop Start/Ground Start	0.1B/9.0F	02LS2 02GS2	RJ-11C
TA 600 Series ADSL Products	US:HDCDL02B4200644L1	Analog Loop Start/Ground Start	0.1B/9.0F	02LS2 02GS2	RJ-11C
		ADSL Service	0.2B/9.0F	02LS2	

8. The REN is useful in determining the quantity of devices you may connect to your telephone line and still have all of those devices ring when your number is called. In most areas, the sum of the RENs of all devices should not exceed five. To be certain of the number of devices you may connect to your line as determined by the REN, call your telephone company to determine the maximum REN for your calling area.

9. This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs. Contact your state public utility commission or corporation commission for information.

Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio frequencies. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

> NOTE   *Shielded cables must be used with this unit to ensure compliance with Class A FCC limits.*

> WARNING   *Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.*

Affidavit Requirements for Connection to Digital Services

• An affidavit is required to be given to the telephone company whenever digital terminal equipment without encoded analog content and billing protection is used to transmit digital signals containing encoded analog content which are intended for eventual conversion into voice band analog signal and transmitted on the network.

• The affidavit shall affirm that either no encoded analog content or billing information is being transmitted or that the output of the device meets Part 68 encoded analog content or billing protection specifications.

• End user/customer will be responsible to file an affidavit with the local exchange carrier when connecting unprotected CPE to a 1.544 Mbps or subrate digital service.

• Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirements for subrate services are waived.

AFFIDAVIT FOR CONNECTION OF CUSTOMER PREMISES EQUIPMENT
TO 1.544 MBPS AND/OR SUBRATE DIGITAL SERVICES

For the work to be performed in the certified territory of _____ (telco name)

State of _____

County of _____

I, _____ (name), _____ (business address),
_____ (telephone number) being duly sworn, state:

(   ) I have responsibility for the operation and maintenance of the terminal equipment to be connected to 1.544 Mbps and/or _____ subrate digital services. The terminal equipment to be connected complies with Part 68 of the FCC rules except for the encoded analog content and billing protection specifications. With respect to encoded analog content and billing protection:

(   ) I attest that all operations associated with the establishment, maintenance, and adjustment of the digital CPE with respect to analog content and encoded billing protection information continuously complies with Part 68 of the FCC Rules and Regulations.

(   ) The digital CPE does not transmit digital signals containing encoded analog content or billing information which is intended to be decoded within the telecommunications network.

(   ) The encoded analog content and billing protection is factory set and is not under the control of the customer.

I attest that the operator(s)/maintainer(s) of the digital CPE responsible for the establishment, maintenance, and adjustment of the encoded analog content and billing information has (have) been trained to perform these functions by successfully having completed one of the following (check appropriate blocks):

(   )   A.   A training course provided by the manufacturer/grantee of the equipment used to encode analog signals; or

(   )   B.   A training course provided by the customer or authorized representative, using training materials and instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or

(   )   C.   An independent training course (e.g., trade school or technical institution) recognized by the manufacturer/grantee of the equipment used to encode analog signals; or

(   )   D.   In lieu of the preceding training requirements, the operator(s)/maintainer(s) is (are) under the control of a supervisor trained in accordance with _____ (circle one) above.

I agree to provide _____ (telco's name) with proper documentation to demonstrate compliance with the information as provided in the preceding paragraph, if so requested.

_____Signature
_____Title
_____ Date

Transcribed and sworn to before me

This _____ day of _____, _____

_____
Notary Public

My commission expires:

_____

Industry Canada Compliance Information

> **NOTE**
> *The Industry Canada Certification label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. The Department of Commerce does not guarantee the equipment will operate to the user's satisfaction.*

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic waterpipe system, if present, are connected together. This precaution may be particularly important in rural areas.

> **WARNING**
> *Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or an electrician, as appropriate.*

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the equipment that the total of the LNs of all devices does not exceed 100.

The ringer equivalence number (REN) assigned to each terminal adapter is used to determine the total number of devices that may be connected to each circuit. The sum of the RENs from all devices in the circuit should not exceed a total of 5.0.

Canadian Emissions Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioelectriques applicables aux appareils numériques de Class A prescrites dans la norme sur le materiel brouilleur: "Appareils Numériques," NMB-003 edictee par le ministre des Communications.

Product Warranty

ADTRAN will repair and return this product within the warranty period if it does not meet its published specifications or fails while in service. Warranty information can be found at www.adtran.com/warranty.

Product Registration

Registering your product helps ensure complete customer satisfaction. Please take time to register your products on line at www.adtran.com. Click *Service and Support* on the top of the page, and then click *Product Registration* under *Support.*

Customer Service, Product Support Information, and Training

ADTRAN will replace or repair this product within the warranty period if it does not meet its published specifications or fails while in service. Warranty information can be found at www.adtran.com/warranty.

A return material authorization (RMA) is required prior to returning equipment to ADTRAN. For service, RMA requests, training, or more information, use the contact information given below.

Repair and Return

If you determine that a repair is needed, please contact our Customer and Product Service (CAPS) department to have an RMA number issued. CAPS should also be contacted to obtain information regarding equipment currently in house or possible fees associated with repair.

> CaPS Department   (256) 963-8722

Identify the RMA number clearly on the package (below address), and return to the following address:

> ADTRAN Customer and Product Service
> 901 Explorer Blvd. (East Tower)
> Huntsville, Alabama 35806
>
> RMA # _____

Pre-Sales Inquiries and Applications Support

Your reseller should serve as the first point of contact for support. If additional pre-sales support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, latest product documentation, application briefs, case studies, and a link to submit a question to an Applications Engineer. All of this, and more, is available at:

> http://support.adtran.com

When needed, further pre-sales assistance is available by calling our Applications Engineering Department.

> Applications Engineering   (800) 615-1176

Post-Sale Support

Your reseller should serve as the first point of contact for support. If additional support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, updated firmware releases, latest product documentation, service request ticket generation and trouble-shooting tools. All of this, and more, is available at:

http://support.adtran.com

When needed, further post-sales assistance is available by calling our Technical Support Center. Please have your unit serial number available when you call.

Technical Support   (888) 4ADTRAN

Installation and Maintenance Support

The ADTRAN Custom Extended Services (ACES) program offers multiple types and levels of installation and maintenance services which allow you to choose the kind of assistance you need. This support is available at:

http://www.adtran.com/aces

For questions, call the ACES Help Desk.

ACES Help Desk   (888) 874-ACES (2237)

Training

The Enterprise Network (EN) Technical Training Department offers training on our most popular products. These courses include overviews on product features and functions while covering applications of ADTRAN's product lines. ADTRAN provides a variety of training options, including customized training and courses taught at our facilities or at your site. For more information about training, please contact your Territory Manager or the Enterprise Training Coordinator.

Training Phone	(800) 615-1176, ext. 7500
Training Fax	(256) 963-6700
Training Email	training@adtran.com

Table of Contents

                                   61200624L1-1B

SYSTEM DESCRIPTION

This section provides an overview of the Total Access 600 Series system.

CONTENTS

1.   SYSTEM OVERVIEW

The Total Access 600 Series contains Integrated Access Devices (IAD) designed for cost-effective deployment of voice and data services at the customer premises. The Total Access 600 Series benefits integrated communications providers (such as CLECs, ILECs, and ISPs) who require a customer premises device with integrated voice and data functions, and provides a viable migration path from TDM to packet-based technology. These IADs support applications such as VoDSL and VoATM.

The Total Access 600 Series features remote management, built-in IP router, and an optional DSX-1 interface (factory installed only). An optional battery backup is also available for many of the models. The units include a Nx56/64 V.35 interface, 10/100BaseT interface, FXS ports, and network interfaces (T1, ADSL, SDSL, and SHDSL). The last two digits of the product name indicate the number of on-board FXS ports. The Total Access 604 contains four FXS ports, the Total Access 608 contains eight FXS ports, etc. The units can provision, test, and provide status for any of the voice and data interfaces. All connections are made via the rear panel.

This line of IADs includes both the ATM and TDM versions of the Total Access 604/608/612/616/624 and Total Access 600R systems. Until now, the Total Access TDM units have been running firmware version A.03.XX. Recently, A.04.XX has been released to support the TDM Total Access IADs. The development of A.04.XX code is a significant step in the evolution of the Total Access product line, as it allows all Total Access family members to share the same base code. This means that features and fixes are more easily implemented and are propagated across the product line. The User Interface Guide section of this manual represents the A.04 firmware changes. There are two possible upgrade paths: (1) Upgrading from A.03 to A.04 directly and; (2) Upgrading from A.03 to A.03.92 (Transition Build) to A.04.

> **NOTE**
>
> *Upgrading from A.03 to A.03.92 (Transition Build) to A.04 will save the unit's configuration. Upgrading from A.03 to A.04 directly (or from A.04 to A.03 directly) will erase the unit's configuration. See DLP-14, A.03 to A.04 Firmware Upgrade, for more details.*

> **WARNING**
>
> *Units manufactured after October 2002 will not be compatible with some older versions of Total Access 612, 616, and 624 software. Refer to the following information if an older version of software is to be loaded into the unit. For TDM applications, please use software revision A.03.58 or later. For ATM applications, software revision D.01.30 or later is required. Using incompatible software will cause the unit to malfunction. For more information or technical assistance, please call ADTRAN Technical Support at 888-4ADTRAN. Please have the unit serial number available when contacting Technical Support.*

2.   FEATURES AND BENEFITS

The following list gives Total Access 600 Series features and benefits. Some features are model-dependent.

Configuration and Management
- VT100 Emulation
- SNMP Management
- Telnet
- Six levels of password protection and privileges for Telnet access
- Support for VoDSL gateway management systems and firmware download

Software Upgradeable
- Flash memory
- TFTP download
- XMODEM via **CRAFT** port

Network Interfaces
- T1
- ADSL
- SDSL
- SHDSL

Integrated Components
- IP router
- Life-line voice backup (xDSL models only)
- Network connection
- 10/100 BaseT connection
- V.35 Nx56/64 DTE interface
- **CRAFT** port
- Optional DSX-1 port (Factory installed only)

ATM Support
- AAL2 (voice), AAL5 (data, voice)
- 6 PVCs (1 voice, 5 data)
- RFC 1483 (multi protocol over ATM)
- PPPoA (RFC 2364)
- QoS Support: VBR-rt (voice), UBR (data)
- I.610 F5 OAM loopback
- G.165/G.168 echo cancellation, 8 ms echo tail
- Voice Codes: PCM (G.711), 32k ADPCM (G.726)
- Idle channel suppression

Frame Relay Support

- Copper Mountain CE fragmentation support
- Annex A, Annex D, and LMI support (T1)
- FRF.5 and FRF.8 support (V.35)

Analog Ports

- Analog FXS ports per TR-57, 50-Pin Amp (number of ports is unit dependent)
- Supports popular CLASS^{TM} features
- Modes: FXS Loop Start, FXS Ground Start, TR08 Single, TR08 UVG, DP0, Tandem (E&M)
- Assured Dialtone^{TM} Lifeline POTS port (available only xDSL models)
- Balanced ringing, 5 REN per port not to exceed 35 REN
- Fixed ringer – 70 Vrms with 20 VDC offset
- Distance up to 1000 feet

V.35 DTE Interface

- Data Rate: Nx56 or Nx64 kbps (N=1 to 24)
- Electrical and Mechanical: CCITT V.35, 34-pin
- Frame Relay (FRF.5, FRF.8 capable)

Routing Capability

- Ethernet: 10/100BaseT (RJ-45)
- IEEE 802.3 and 802.1D (MAC Bridging)
- IP Support: TCP, RIP V1, RIP V2, UDP, ICMP, ARP, UDP Relay, SYSLOG
- PPP Support: LCP, IPCP, BCP
- DHCP Server to LAN, DHCP from network
- Copper Mountain Compatible
- Frame Relay (Annex A, Annex D, LMI, Static)

Security

- PAP, CHAP, and EAP for PPP
- Radius authentication for Telnet access
- NAT with multi-point to single-point
- Future support of NAT multi-point to multi-point
- Filtering (Pattern, IP, Bridge)
- Password protection

Testing

- Local/Remote loopbacks
- Line and payload loopback tests
- FXO tests (Total Access 624 with FXO only)
- FXS tests

Performance Monitoring
*   Reports: Information stored for last 24 hours in 15 minute increments
*   Performance statistics per TR54016, T1.403, RFC1406
*   Alarm reporting per TR54016, T1.403

3.   IAD SYSTEMS

The Total Access 600 Series supports a variety of WAN technologies. The following list displays the various available systems grouped by network technology.

T1
*   P/N 4200600L1#TDM Total Access 600R T1 TDM
*   P/N 4213600L1#TDM Total Access 600R T1 TDM with DSX-1
*   P/N 4200600L1#ATM Total Access 600R T1 ATM
*   P/N 4213600L1#ATM Total Access 600R T1 ATM with DSX-1
*   P/N 4203640L1#TDM Total Access 604 T1 TDM
*   P/N 4213640L1#TDM Total Access 604 T1 TDM with DSX-1
*   P/N 4203640L1#TDMB Total Access 604 T1 TDM with Battery Backup
*   P/N 4203640L1#ATM Total Access 604 T1 ATM
*   P/N 4213640L1#ATM Total Access 604 T1 ATM with DSX-1
*   P/N 4203640L1#ATMB Total Access 604 T1 ATM with Battery Backup
*   P/N 4203680L1#TDM Total Access 608 T1 TDM
*   P/N 4213680L1#TDM Total Access 608 T1 TDM with DSX-1
*   P/N 4203680L1#TDMB Total Access 608 T1 TDM with Battery Backup
*   P/N 4203680L1#ATM Total Access 608 T1 ATM
*   P/N 4213680L1#ATM Total Access 608 T1 ATM with DSX-1
*   P/N 4203680L1#ATMB Total Access 608 T1 ATM with Battery Backup
*   P/N 4203612L1#TDM Total Access 612 T1 TDM
*   P/N 4213612L1#TDM Total Access 612 T1 TDM with DSX-1
*   P/N 4203612L1#ATM Total Access 612 T1 ATM
*   P/N 4213612L1#ATM Total Access 612 T1 ATM with DSX-1
*   P/N 4203616L1#TDM Total Access 616 T1 TDM
*   P/N 4213616L1#TDM Total Access 616 T1 TDM with DSX-1
*   P/N 4203616L1#ATM Total Access 616 T1 ATM
*   P/N 4213616L1#ATM Total Access 616 T1 ATM with DSX-1
*   P/N 4203624L1#TDM Total Access 624 T1 TDM
*   P/N 4213624L1#TDM Total Access 624 T1 TDM with DSX-1
*   P/N 4203624L3#TDM Total Access 624 T1 TDM with 16 FXS and 8 FXO
*   P/N 4213624L3#TDM Total Access 624 T1 TDM with DSX-1, 16 FXS, and 8 FXO
*   P/N 4203624L1#ATM Total Access 624 T1 ATM
*   P/N 4213624L1#ATM Total Access 624 T1 ATM with DSX-1

ADSL

- P/N 4200644L1 Total Access 604 ADSL
- P/N 4200644L1#ACB Total Access 604 ADSL with Battery Backup
- P/N 4200684L1 Total Access 608 ADSL
- P/N 4200684L1#ACB Total Access 608 ADSL with Battery Backup

SDSL

- P/N 4200642L1 Total Access 604 SDSL
- P/N 4200642L1#ACB Total Access 604 SDSL with Battery Backup
- P/N 4200682L1 Total Access 608 SDSL
- P/N 4200682L1#ACB Total Access 608 SDSL with Battery Backup
- P/N 4200612L2 Total Access 612 SDSL
- P/N 4200616L2 Total Access 616 SDSL
- P/N 4200624L2 Total Access 624 SDSL

SHDSL

- P/N 4200600L3 Total Access 600R SHDSL
- P/N 4200643L1 Total Access 604 SHDSL
- P/N 4200643L1#ACB Total Access 604 SHDSL with Battery Backup
- P/N 4200683L1 Total Access 608 SHDSL
- P/N 4200683L1#ACB Total Access 608 SHDSL with Battery Backup
- P/N 4200612L3 Total Access 612 SHDSL
- P/N 4200616L3 Total Access 616 SHDSL
- P/N 4200624L3 Total Access 624 SHDSL

ENGINEERING GUIDELINES

This section provides equipment dimensions, power requirements, front panel design, rear panel design, LEDs, and at-a-glance specifications.

CONTENTS

FIGURES

TABLES

1.   EQUIPMENT DIMENSIONS

Total Access 600R, Total Access 604/608

The Total Access 600R and Total Access 604/608systems measure 11.25" W, 7.5" D, and 2" H and come equipped for table top or wallmount use.

Total Access 612/616/624

The Total Access 612/616/624 systems measure 17" W, 8.5" D, and 1.75" H and come equipped for table top or wallmount use. These systems may be utilized in 19- or 23-inch racks with the purchase of mounting brackets (19"– P/N 1200627L1 and 23"– P/N 1200627L2).

2.   POWER REQUIREMENTS

The following power requirements apply:

Table 1. AC Power Requirements

System	Maximum Power Consumption	Maximum Current Draw
Total Access 600R	14 W	300mA
Total Access 604	14 W	300 mA
Total Access 608	17 W	300 mA
Total Access 612	28 W	1.3 A
Total Access 616	32 W	1.3 A
Total Access 624	40 W	1.3 A

3.   REVIEWING THE FRONT PANEL DESIGN

Total Access 600R

Figure 2 shows the Total Access 600R front panel.

Figure 1. Total Access 600R Front Panel Layout

Front Panel LEDs

The front panel provides five status LEDs to monitor operation and activity. Table 3 provides LED descriptions for Total Access 600R systems.

Table 2. Total Access 600R Front Panel LEDs

For these LEDs...	This color light...	Indicates that...
LAN TX/RX	Off	there is no data traffic on the LAN.
	Green (blinking)	there is data traffic on the LAN.
LAN LINK	Off	the physical link is down; there is no Ethernet connection.
	Green (solid)	there is link integrity on the LAN (physical link is up).
WAN STAT	Red (solid)	the T1 is in red alarm or T1 sync loss has occurred.
	Yellow (solid)	the T1 is in yellow alarm.
	Green (solid)	the unit is not in alarm.
WAN ERR	Off	the WAN link is up and error-free.
	Red (solid)	severe errors are present on the WAN link.
	Red (flashing)	the T1 is down.
	Yellow (solid)	errors are present on the WAN link.
PWR	Green (solid)	power is supplied to the unit.
	Off	power is not supplied to the unit.

Total Access 604/608

The front panels of the Total Access 604/608 systems are identical. Figure 2 shows the Total Access 608 front panel as a representative of both models.

Figure 2. Total Access 604/608 Front Panel Layout

Front Panel LEDs

The front panel provides eight status LEDs to monitor operation and activity. The LED functionality varies based on product and software load (TDM versus ATM). Table 3 provides LED descriptions for Total Access 604/608 systems employing TDM software, and Table 4 on page 26 lists ATM software LED functionality.

Table 3. Total Access 604/608 TDM Front Panel LEDs

For these LEDs...	This color light...	Indicates that...
TX/RX	Off	there is no data traffic on the LAN.
	Green (blinking)	there is data traffic on the LAN.
LINK	Off	the physical link is down; there is no Ethernet connection.
	Green (solid)	there is link integrity on the LAN (physical link is up).
V.35 RX	Off	no data traffic is being received on the V.35.
	Green (blinking)	data is being received on the V.35.
V.35 TX	Off	no data traffic is being transmitted on the V.35.
	Green (blinking)	data is being transmitted on the V.35.
DATA	Red (solid)	the T1 is in red alarm or T1 sync loss has occurred.
	Yellow (solid)	the T1 is in test.
	Green (solid)	Layer 2 is up.
VOICE	Off	the T1 is down.
	Green (blinking)	the phone is off hook.
	Green (solid)	the T1 is up and the phone is on hook.
BATT	Off	there is no power connected to the system.
	Green (solid)	AC power is operational and battery is functional.
	Red/Green (alternating)	AC power is operational, but the battery is not functional.
	Amber (solid)	AC power has failed and the battery is functional.
	Red/Amber (alternating)	AC power has failed and the battery is not functional.
PWR NET	Green (solid)	Layer 1 is up.
	Green (blinking)	Layer 1 is down.

Table 4. Total Access 6XX ATM Front Panel LEDs

For these LEDs...	This color light...	Indicates that...
TX/RX	Off	there is no data traffic on the LAN.
	Green (blinking)	there is data traffic on the LAN.
LINK	Off	the physical link is down; no Ethernet connection.
	Green (solid)	there is link integrity on the LAN; the physical link is up.
V.35 RX	Off	no data traffic is being received on the V.35.
	Green (blinking)	data is being received on the V.35.
V.35 TX	Off	no data traffic is being transmitted on the V.35.
	Green (blinking)	data is being transmitted on the V.35.
DATA	Red (solid)	Layer 2 is down.
	Green (solid)	Layer 2 is up.
VOICE	Red (solid)	the T1 is non-operational.
	Green (blinking)	the phone is off hook.
VOICE **(if Gateway is Jetstream)**	Red (solid)	gateway link is down.
	Green (solid)	gateway link is up.
VOICE **(if Gateway is Coppercom or LES-CAS)**	Red (solid)	Layer 2 is down.
	Green (solid)	Layer 2 is up.
VOICE **(if Gateway is Tollbridge)**	Red (solid)	gateway status is inactive.
	Green (solid)	gateway status is active.
VOICE **(if no Gateway)**	Yellow (blinking)	the phone is off hook.
	Off	the phone is on hook.
BATT	Off	there is no power connected to the system.
	Green (solid)	AC power is operational and battery is functional.
	Red/Green (alternating)	AC power is operational, but the battery is not functional.
	Amber (solid)	AC power has failed and the battery is functional.
	Red/Amber (alternating)	AC power has failed and the battery is not functional.
PWR NET	Green (solid)	Layer 1 is up.
	Green (blinking slowly)	unit was unable to train – Layer 1 is down.
	Green (blinking rapidly)	Layer 1 is training (SDSL and SHDSL only).

Total Access 612/616/624

The front panels of the Total Access 612/616/624 systems are identical. Figure 3 shows the Total Access 612 front panel as a representative of all models.
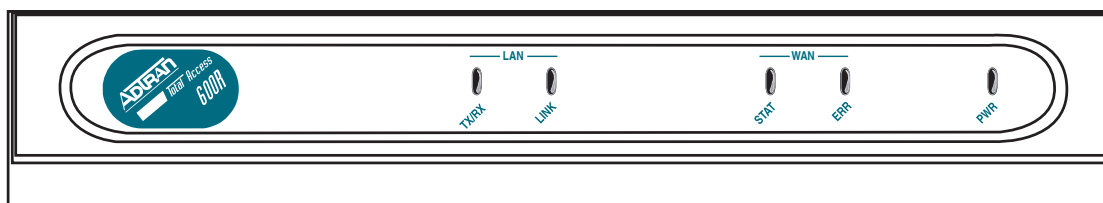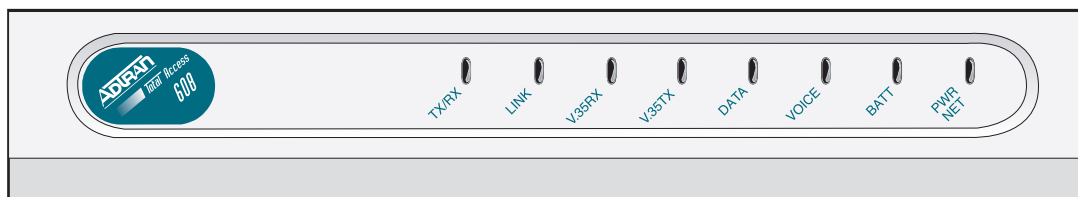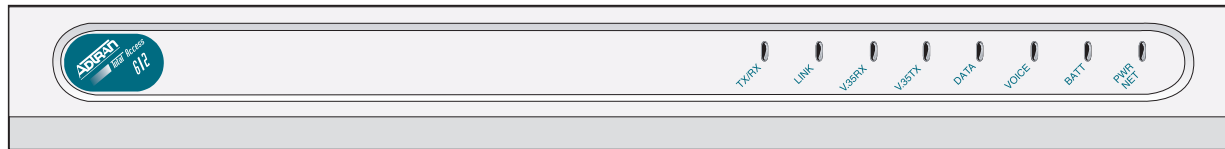

Figure 3. Total Access 612/616/624 Front Panel Layout

Front Panel LEDs

The front panel provides eight status LEDs to monitor operation and activity. The LED functionality varies based on product and software load (TDM versus ATM). Table 5 provides LED descriptions for Total Access 612/616/624 systems employing TDM software, and Table 4 on page 26 lists ATM software LED functionality.

Table 5. Total Access 612/616/624 TDM Front Panel LEDs

For these LEDs...	This color light...	Indicates that...
TX/RX	Off	there is no data traffic on the LAN.
	Green (blinking)	there is data traffic on the LAN.
LINK	Off	the physical link is down; no Ethernet connection.
	Green (solid)	there is link integrity on the LAN; the physical link is up.
V.35 RX	Off	no data traffic is being received on the V.35.
	Green (blinking)	data is being received on the V.35.
V.35 TX	Off	no data traffic is being transmitted on the V.35.
	Green (blinking)	data is being transmitted on the V.35.
DATA	Red (solid)	the T1 is in red alarm or T1 sync loss has occurred.
	Yellow (solid)	the T1 is in test.
	Green (solid)	Layer 2 is up.
VOICE	Red (solid)	the T1 is down.
	Green (blinking)	the phone is off hook.
	Green (solid)	the T1 is operational and the phone is on hook.

Table 5. Total Access 612/616/624 TDM Front Panel LEDs *(Continued)*

For these LEDs...	This color light...	Indicates that...
BATT	Off	there is no power connected to the system.
	Green (solid)	AC power is operational and battery is functional.
	Red/Green (alternating)	AC power is operational, but the battery is not functional.
	Amber (solid)	AC power has failed and the battery is functional.
	Red/Amber (alternating)	AC power has failed and the battery is not functional.
PWR NET	Green (solid)	Layer 1 is up.
	Green (blinking)	Layer 1 is down.

4.   REVIEWING THE REAR PANEL DESIGN

The Total Access 600R provides a **NTWK** connection (via an RJ-48 connector), a **CRAFT** interface (via an RJ-49 connector), a **10/100BASET** interface (via an RJ-48 connector), and an **AC PWR** connection (via a 3-prong detachable power cord). In addition, systems can include the optional **DSX-1** interface (via an RJ-48 connector). The Total Access 600R rear panel differs from the rest of the family in that it does not have a **VOICE** connection (50-pin amphenol connector). Figure 4 illustrates a standard Total Access 600R rear panel.
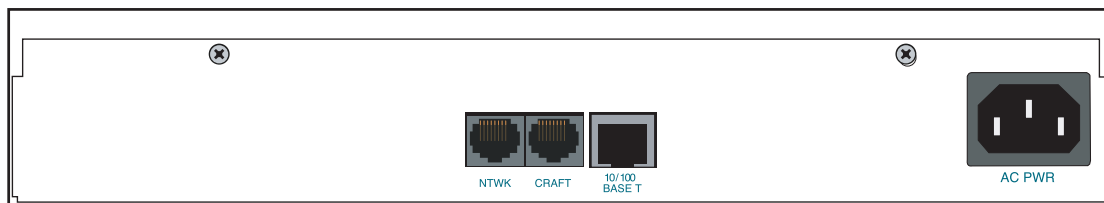
Figure 4. Total Access 600R Rear Panel

All other Total Access 600 Series systems contain the following rear panel interfaces regardless of the model: **VOICE** connection (via a 50-pin female amphenol connector), a **NTWK** connection (via an RJ-48 connector), a **CRAFT** interface (via an RJ-48 connector), a **10/100BASET** interface (via an RJ-48 connector), a **V.35** connection (via a 34-pin Winchester-style connector), a **BATT** connection (via a 3-pin modular plug), and an **AC PWR** connection (via a 3-prong detachable power cord). In addition, systems can include either a **LIFE LINE** analog interface (via an RJ-48 connector) or an optional **DSX-1** interface (via an RJ-48 connector). Figure 5 on page 29 illustrates a standard Total Access 604/608, and Figure 6 and Figure 7 on page 29 illustrate the Total Access 604/608 rear panels with the **LIFE LINE** analog and **DSX-1** interfaces, respectively. Figures 8 through 10 on page 29 illustrate the Total Access 612/616/624 rear panels.
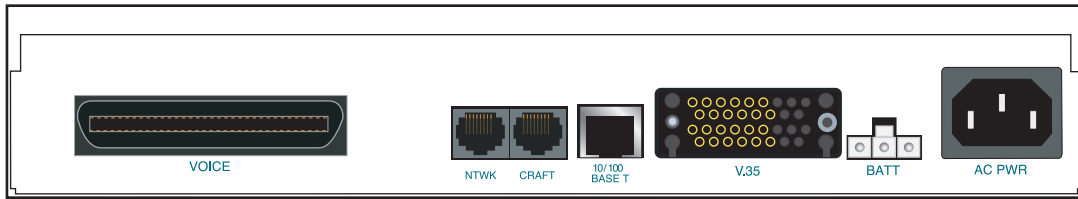
Figure 5. Total Access 604/608 Rear Panel
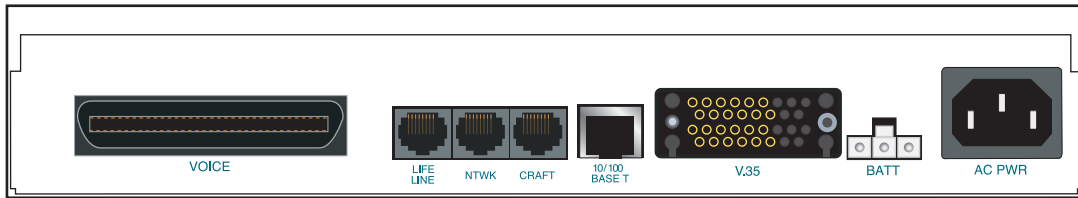
Figure 6. Total Access 604/608 Rear Panel with Optional Life Line POTS
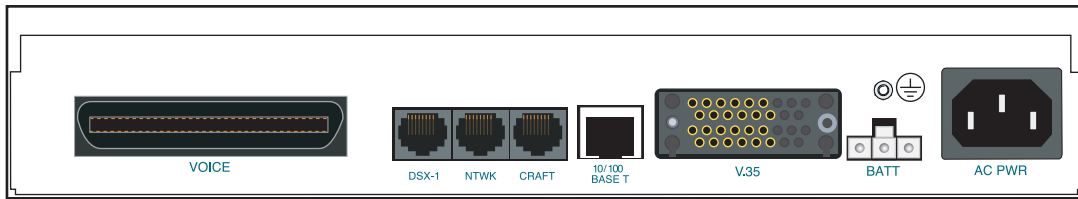
Figure 7. Total Access 604/608 Rear Panel with Optional DSX-1 Interface
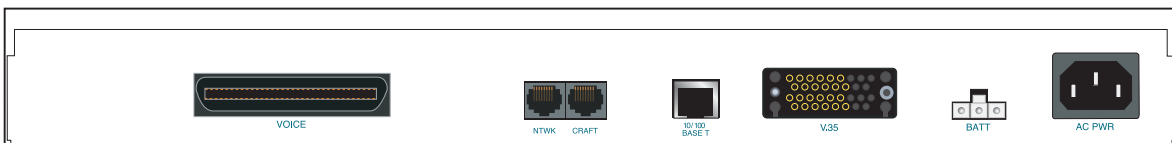
Figure 8. Total Access 612/616/624 Rear Panel
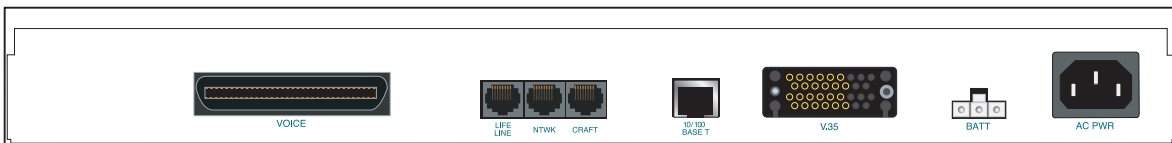
Figure 9. Total Access 612/616/624 Rear Panel with Optional Life Line POTS
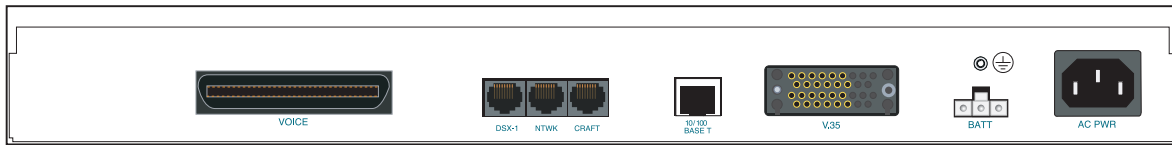
Figure 10. Total Access 612/616/624 Rear Panel with Optional DSX-1 Interface

VOICE Connection

A single 50-pin female amphenol connector provides the interconnect wiring for the analog FXS and FXO (available as an option only on the Total Access 624) circuits. Figure 11 shows the **VOICE** connector pinout.
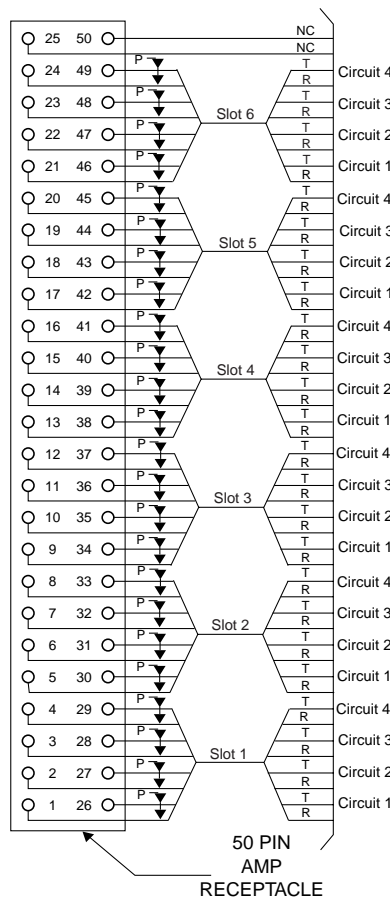
Figure 11. VOICE Connector Pin Assignments

NTWK Connection

The Total Access 600 Series **NTWK** connection is provided via an RJ-48 connector regardless of the network technology (T1, ADSL, SDSL, etc.). Table 6 shows the **NTWK** connection pinout (identical across all technologies).

Table 6. NTWK Connection Pinout

PIN	NAME	DESCRIPTION
1	RX RING	Receive data from the network
2	RX TIP	Receive data from the network
3, 6-8	————	Unused
4	TX RING	Transmit data toward the network
5	TX TIP	Transmit data toward the network

CRAFT Port

The **CRAFT** port (EIA-232) on the rear panel connects to a computer or modem and provides the following functions:

- Accepts EIA-232 input from a PC or a modem for controlling the Total Access 600 Series.
- Baud rate is user-configurable.
- Acts as input for either VT100 or PC control.
- Acts as an interface for flash memory software downloads using XMODEM.

Table 7 shows the **CRAFT** port pinout.

Table 7. CRAFT Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground – connected to unit chassis
2	RTS	Request to send – flow control
3	RXDATA	Receive data
4	DTR	Data terminal ready
5	TXDATA	Transmit data
6	CD	Carrier detect
7	————	Unused
8	CTS	Clear to send - flow control

A DB-9 to RJ-48 adapter is needed to connect a PC or VT100 terminal to the **CRAFT** port. This adapter is not part of the Total Access 600 Series shipment. You may obtain a free adapter (P/N 3196ADPT001) by contacting ADTRAN Technical Support or by adding the adapter to the system order. You can also build your own adapter by purchasing unassembled adapter kits from Black Box or Datacomm Warehouse (or other equivalent companies). The adapter pinout is shown in Table 8.

Table 8. DB-9 to RJ-48 Adapter Pinout

DB-9	RJ-48	DESCRIPTION
2	5	Transmit Data
3	3	Receive Data
5	1	Ground

Table 8. DB-9 to RJ-48 Adapter Pinout *(Continued)*

DB-9	RJ-48	DESCRIPTION
Note: All other pins are unused.		

10/100BaseT Connection

The **10/100BASET** port (RJ-48C) provides a 10/100BaseT Ethernet LAN connection for IP Routing, TFTP, SNMP, and Telnet connections. Table 9 shows the 10/100BaseT pinout.

Table 9. Ethernet Pinout

PIN	NAME	DESCRIPTION
1	TX1	Transmit Positive
2	TX2	Transmit Negative
3	RX1	Receive Positive
4, 5	———	Unused
6	RX2	Receive Negative
7, 8	———	Unused

V.35 Connection

The Total Access 600 Series system provides a single V.35 Winchester-style connection on the rear of the unit (as defined in Table 10).

Table 10. V.35 Winchester Pinout

PIN/CCIT	DESCRIPTION	PIN/CCIT	DESCRIPTION
A/101	Protective ground (PG)	V/115	RX clock (RC-A) to DTE
B/102	Signal ground (SG)	X/115	RX clock (RC-B) to DTE
C/105	Request to send (RTS) from DTE	P/103	Transmitted data (TD-A) from DTE
D/106	Clear to send (CTS) to DTE	S/103	Transmitted data (TD-B) to DTE
E/107	Data set ready (DSR) to DTE	Y/114	TX clock (TC-A) to DTE
E/109	Data carrier detect	AA/114	TX clock (TC-B) to DTE
H/—	Data terminal ready (DTR) from DTE	U/113	External TX clock (ETC-A) from DTE
J/—	Ring indicator (RI)	W/113	External TX clock (ETC-B) from DTE
R/104	Received data (RD-A) to DTE	NN/—	Test mode (TM) to DTE
T/104	Received data (RD-B) to DTE		

Battery Backup Connection

An optional battery backup system is available for the Total Access 604/608 (P/N 1200641L1) and the Total Access 612/616/624 (P/N 1175044L1, 1175044L2, or 1175044L4). For more details on the battery backup system installation and operation, refer to the documentation available for your specific battery backup unit.

AC Power Connection

Each unit includes an auto ranging 90-250 VAC, 50/60 Hz power supply with a 3-prong removable cable. Connect the power supply to a standard 120 VAC, 60 Hz electrical outlet for proper operation.

Life Line Analog Connection

> **NOTE**
> *The **LIFE LINE** analog connection is only available on Total Access 600 Series xDSL models.*

The **LIFE LINE** analog connection provides assured voice for port 1. If the unit loses power or goes into alarm, the network voice service is inhibited and the on-board relay opens. The first port of the voice connector is provided with analog voice from the **LIFE LINE** analog connection. A regular POTS line must be plugged into the **LIFE LINE** port. Table 11 provides the **LIFE LINE** port pinout.

Table 11. LIFE LINE Connection Pinout

PIN	DESCRIPTION
1,2	Unused
3	Life Line Ring
4	Life Line Tip
5,6	Unused

DSX-1 Interface

> **NOTE**
> *The **DSX-1** interface is optional and must be requested at the time of order placement. Total Access 600 Series systems without the DSX-1 interface are not field-upgradeable to add DSX-1 access.*

Table 12 provides the DSX-1 port pinout.

Table 12. DSX-1 Connection Pinout

PIN	NAME	DESCRIPTION
1	TX RING	Transmit data toward the network (RING)
2	TX TIP	Transmit data toward the network (TIP)
3, 6-8	———	Unused
4	RX RING	Receive data from the network (RING)
5	RX TIP	Receive data from the network (TIP)

5.   AT-A-GLANCE SPECIFICATIONS

Table 13 lists the unit specifications.

Table 13. Specifications

Application	Feature	Specification
T1 Network Interface		
	Physical Interface	RJ-48C
	Line Rate	1.544 Mbps +/- 75 bps
	Framing	D4 (SF)/ESF AT&T 54016 ANSI T1.403
	Line Code	AMI/B8ZS
ADSL Network Interface (ITU G.992.1)		
	Throughput	Up to 8 Mbps downstream Up to 1 Mbps upstream
	Interoperability	Interoperate with G.992.1 compliant DSLAMs
G.SHDSL Network Interface (ITU G.991.2)		
	Line Rate	192 kbps to 2.3 Mbps
SDSL Network Interface (2B1Q Conexant-based)		
	Line Rate	160 kbps to 2.3 Mbps
	Training	Conexant Autobaud capable
ATM Support		
	Voice Codes	PCM (G.711) 32K ADPCM (G.726)
	PVC Capability	6 PVCs (1 voice, 5 data)
	Echo Cancellation	G.165/G.168 Echo Cancellation, 8 ms echo tail
	QoS Support	VBR-rt (voice) UBR (data)
	Specifications	AAL2 (voice) AAL5 (data, voice) RFC 1483 (multiprotocol over ATM) RFC 2364 (PPPoA)
Frame Relay Support		
	Specifications	FRF.5 FRF.8

Table 13. Specifications *(Continued)*

Application	Feature	Specification
Analog Ports		
	Number of FXS Ports	4 ports for Total Access 604 8 ports for Total Access 608 12 ports for Total Access 612 16 ports for Total Access 616 24 ports for Total Access 624
	Modes	FXS Loop Start FXS Ground Start TR08 Single TR08 UVG DP0 Tandem (E&M)
	Ringing	Balanced ringing, 5 REN per port not to exceed 35 REN
	Ring Voltage	Fixed 70 VACrms with 20 VDC offset
Routing (Ethernet)		
	Specifications	IEEE 802.3
	IP Support	TCP, RIP V1, RIP V2, UDP, ICMP, ARP, UDP Relay, SYSLOG
	PPP Support	LCP, IPCP, BCP
	DHCP	DHCP Server to LAN DHCP from network
Management		
	CRAFT Interface	EIA 232, Physical RJ-48C
	Ethernet 10/100BaseT Interface	SNMP V1 support • 604/608 ATM units running D.01.36 firmware or previous • 612/616/624 ATM units running D.01.30 firmware or previous SNMP V2 support • TDM units running A.04 firmware or later Full menu-driven Telnet access Software download via TFTP Support for VoDSL gateway management systems and firmware download

NETWORK TURNUP PROCEDURE

This section provides shipment contents list, grounding instructions, mounting options, and specifics of supplying power to the unit.

CONTENTS

FIGURES

1.   INTRODUCTION

This section discusses Total Access 600 Series installation.

2.   TOOLS REQUIRED

The tools required for wallmount installation of the unit are:

- Four #8 x 3/4 inch pan-head wood screws
- Drill and drill bit set
- Flat head screwdriver (medium)
- Two Phillips head screwdrivers (small/medium)
- Wire-wrap gun (optional)
- 25-pair male amphenol cable (customer connection)
- Selected punch-down block and tool

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*During installation, power should be the last connection made.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

3.   UNPACK AND INSPECT THE SYSTEM

Each unit is shipped in its own cardboard shipping carton. Open each carton carefully and avoid deep penetration into the carton with sharp objects.

After unpacking the unit, inspect it for possible shipping damage. If the equipment has been damaged in transit, immediately file a claim with the carrier, and then contact ADTRAN Customer Service (see *Customer Service, Product Support Information, and Training* in the front of this manual).

Contents of ADTRAN Shipments

Your ADTRAN shipment includes the following items:

*   The Total Access 6XX unit with attached wallmount brackets
*   The Total Access 600 Series System CD – ADTRAN P/N 3253052
*   Hardware revision notice card – ADTRAN P/N 61200624L1-17
*   Mounting instructions – ADTRAN P/N 61200624L1-19
*   RJ-45 to RJ-45 8-pin cable (6 ft) –ADTRAN P/N 3127004
*   Cable tie (for securing attached cables) – ADTRAN P/N 3292032
*   Four rubber feet (for table top installations) – ADTRAN P/N 3270BF003
*   3-prong, detachable power cord – ADTRAN P/N 3127009

> **NOTE**
>
> *Customer must supply Ethernet cable and the RJ-48 to DB-9 adapter and DB-9 serial cable for configuration via the VT100* **CRAFT** *interface.*

4.   GROUNDING INSTRUCTIONS

To following paragraphs provide grounding instruction information from the Underwriters' Laboratory UL60950 Standard for Safety of Information Technology Equipment Including Electrical Business Equipment, with revisions dated March 15, 2002.

An equipment grounding conductor that is not smaller in size than the ungrounded branch-circuit supply conductors is to be installed as part of the circuit that supplies the product or system. Bare, covered, or insulated grounding conductors are acceptable. Individually covered or insulated equipment grounding conductors shall have a continuous outer finish that is either green, or green with one or more yellow stripes. The equipment grounding conductor is to be connected to ground at the service equipment.

The attachment-plug receptacles in the vicinity of the product or system are all to be of a grounding type, and the equipment grounding conductors serving these receptacles are to be connected to earth ground at the service equipment.

A supplementary equipment grounding conductor shall be installed between the product or system and ground that is in addition to the equipment grounding conductor in the power supply cord.

The supplementary equipment grounding conductor shall not be smaller in size than the ungrounded branch-circuit supply conductors. The supplementary equipment grounding conductor shall be connected to the product at the terminal provided, and shall be connected to ground in a manner that will retain the ground connection when the product is unplugged from the receptacle. The connection to ground of the supplementary equipment grounding conductor shall be in compliance with the rules for terminating bonding jumpers at Part K or Article 250 of the National Electrical Code, ANSI/NFPA 70. Termination of the supplementary equipment grounding conductor is permitted to be made to building steel, to a metal electrical raceway system, or to any grounded item that is permanently and reliably connected to the electrical service equipment ground.

The supplemental grounding conductor shall be connected to the equipment using a number 8 ring terminal and should be fastened to the grounding lug provided on the rear panel of the equipment. The ring terminal should be installed using the appropriate crimping tool (AMP P/N 59250 T-EAD Crimping Tool or equivalent).

5.   MOUNTING OPTIONS

All units may be wallmounted or installed in a table-top application. In addition, the Total Access 612/616/624 units are available for 19- or 23-inch rackmount installations. Wallmount brackets are included with the unit and are already attached. For a rackmount installation, optional rackmount brackets must be purchased (19" – P/N 1200627L1, 23" – P/N 1200627L2).

> 🤚
> **CAUTION**
> *Be careful not to upset the stability of the equipment mounting rack when installing this product.*

Wallmounting the Unit

Tools Needed

The unit mounts and connects with standard fasteners and hand tools:

- Four #8 x 3/4-inch pan-head wood screws
- Drill and drill bit set
- Flat head screwdriver (medium)
- Two Phillips head screwdrivers (small/medium)
- Wire-wrap gun (optional)
- 25-pair male amphenol cable (customer connection)
- Selected punch-down block and tool

Follow these steps to wallmount the unit:

	Wallmount Installation
Step	**Action**
1.	Decide on a location for the unit. Keep in mind that the unit needs to be mounted at or below eye-level so that the LEDs are viewable. *IMPORTANT! Mount the chassis with LEDs facing to the side or down as shown in Figure 1 on page 39 (not facing up).* Refer to Figure 2 on page 39 for a wallmount illustration.
2.	Prepare the mounting surface by attaching a board (typically plywood, 3/4" to 1" thick) to a wall stud. *IMPORTANT! Mounting to a stud ensures stability. Using sheetrock anchors may not provide sufficient long-term stability.*
3.	Have someone else hold the unit in position as you install two #6 to #10 (1 1/2" or greater in length) wood screws through the unit's brackets and into the mounted board.
4.	Proceed to the steps given in *Supplying Power to the Unit* on page 40.

Acceptable Orientation — Wallmount
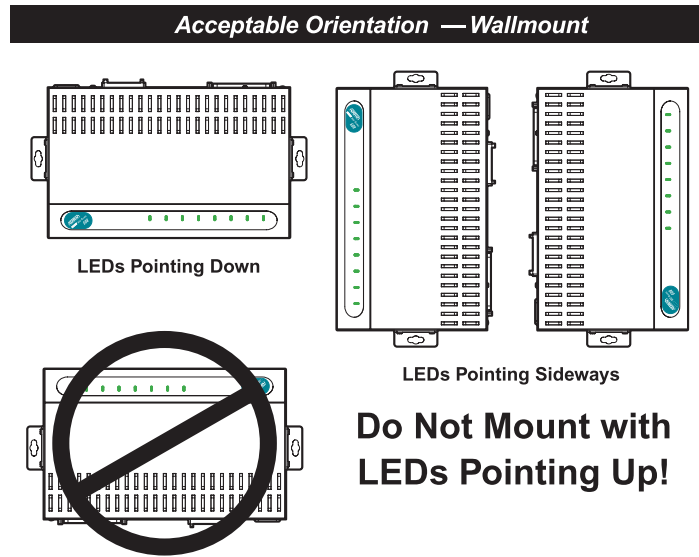
Figure 1. Wallmount Orientation
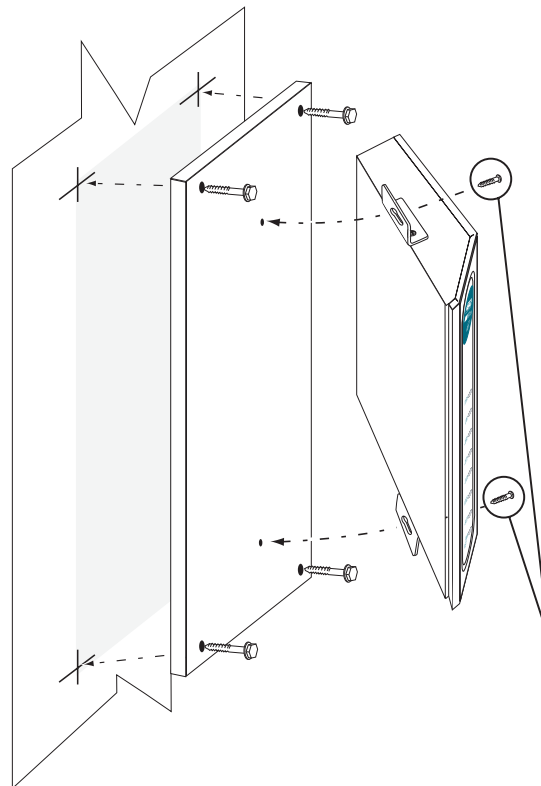
Note: The Total Access 600 Series units come equipped with wall mount brackets preinstalled.

Figure 2. Wallmounting the Unit

Rackmounting the Total Access 612/616/624

Tools Needed

The Total Access 612/616/624 mount and connect with standard fasteners and hand tools:

- Rackmount brackets (19"–P/N 1200627L1 or 23"–P/N 1200627L2)
- Flat head screwdriver (medium)
- Two Phillips head screwdrivers (small/medium)
- Wire-wrap gun (optional)
- 25-pair male amphenol cable (customer connection)
- Selected punch-down block and tool

Follow these steps to rackmount the Total Access 612/616/624:

Rackmount Installation	
Step	**Action**
1.	Remove the wallmount brackets. (The Total Access 612/616/624 ships with wallmount brackets attached.) Attach the mounting brackets to the side of the unit. To avoid damaging the unit, use only the screws included in the mounting bracket shipment when attaching mounting ears to the chassis.
2.	Position the Total Access 612/616/624 in a stationary equipment rack. This unit takes up 1 RU of space. To allow proper grounding, scrape the paint from the rack around the mounting holes where the Total Access 612/616/624 will be positioned.
3.	Have someone else hold the unit in position as you install two mounting bolts through the unit's brackets and into the equipment rack using a #2 Phillip's screwdriver.
4.	Proceed to the steps given in *Supplying Power to the Unit*.

6. SUPPLYING POWER TO THE UNIT

The Total Access 600 Series is not offered in DC powered versions. However, optional DC battery backup systems are available for the Total Access 604/608 (P/N 1200641L1) and Total Access 612/616/624 (P/N 1175044L1, 2, or 4) systems.

AC Powered Systems

The AC powered unit comes equipped with a 3-prong, detachable power cord for connecting to a properly grounded power receptacle. As shipped, the unit is set to factory default conditions. After installing the unit it is ready for power-up. To apply power to the unit, ensure that it is properly connected to an appropriate power source.

CAUTION	• *This unit shall be installed in accordance with Article 400 and 364.8 of the NEC NFPA 70 when installed outside of a Restricted Access Location (i.e., central office, behind a locked door, service personnel only area).* • *Power to the Total Access 600 Series AC system must be from a grounded 90-130 VAC, 50/60 Hz source.* • *Verify the power receptacle uses double-pole, neutral fusing.* • *Maximum recommended ambient operating temperature is 45 ℃.*

USER INTERFACE GUIDE

This section of ADTRAN's Total Access 600 Series System Manual is designed for use by network administrators and others who will configure and provision the system. It contains information about navigating the VT100 user interface, configuration information, and menu descriptions.

CONTENTS

FIGURES

TABLES

1.   NAVIGATING THE TERMINAL MENU

To access the terminal menus and management features of the Total Access 6XX, connect the unit to a VT100 terminal (or VT100 terminal emulator) via the **CRAFT** interface on the rear panel. Configure the terminal settings for 9600 data rate, no parity, 8 data bits, 1 stop bit, and no flow control.

After connecting to the unit and beginning a terminal session, a login screen appears. There is no default password for the Total Access 6XX; press **<ENTER>** to access the terminal menus. (Refer to DLP-2, *Logging in to the System* for detailed instructions.)

Terminal Menu Window

After logging in, all menu items and data fields are displayed in the terminal menu window (see Figure 1), through which you have complete control of the unit.
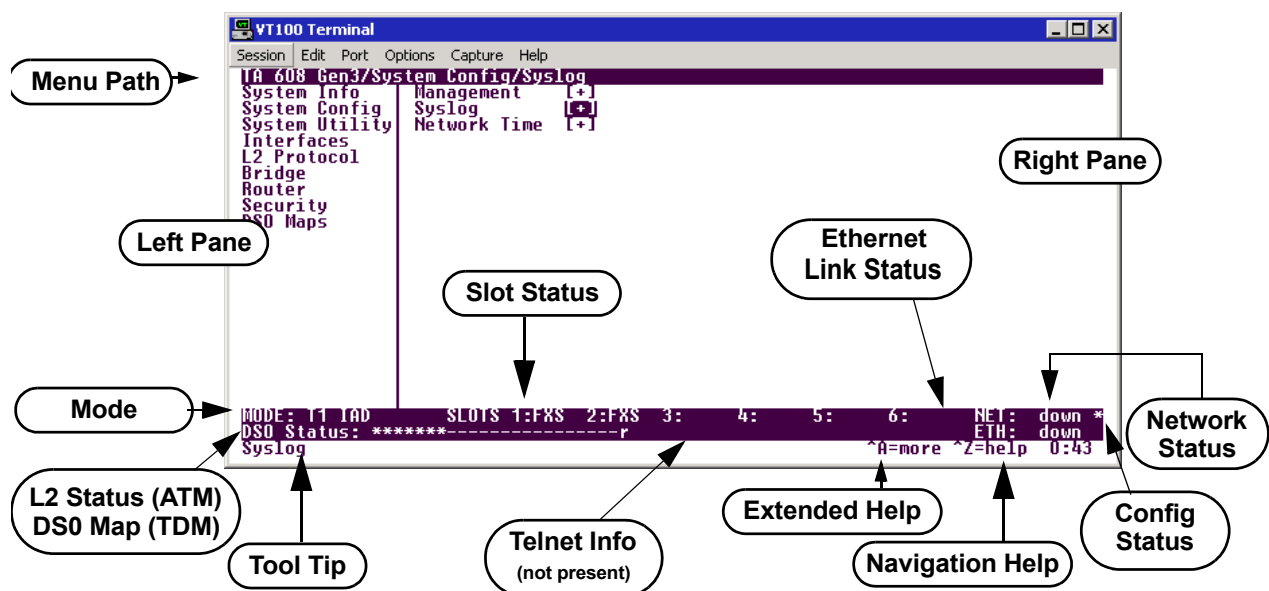
Figure 1. Top-Level Terminal Menu Window

Menu Path

The first line of the terminal menu window (the menu path) shows the session's current position (path) in the menu structure. For example, Figure 1 shows the top-level menu with the cursor on the **SYSTEM CONFIG** submenu; therefore, the menu path reads **TA6XX IAD/SYSTEM CONFIG**.

Window Panes

When you first start a terminal menu session, the terminal menu window is divided into left and right panes. The left pane shows the list of available submenus, while the right pane shows the contents of the currently selected submenu.

You can view the terminal windows in two ways: with fields and submenus displaying horizontally across the right pane, or with fields and submenus displaying vertically down the right pane. Viewing submenus vertically rather than horizontally allows you to see information at a glance rather than scrolling horizontally across the window. To change the view, move your cursor to an index number and press **<ENTER>**. Figure 2 on page 44 shows this alternate view. Fields and submenu names may vary slightly in this view.
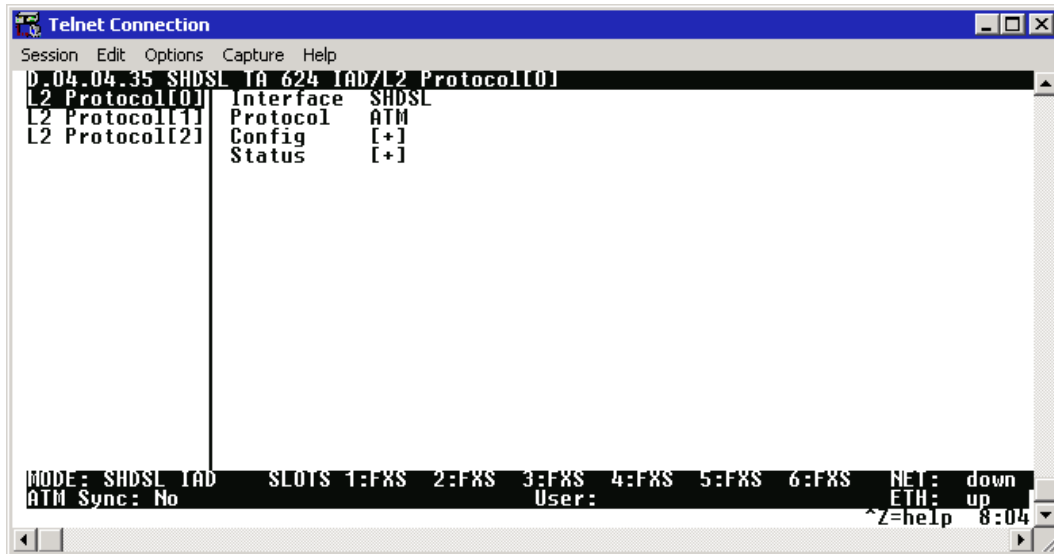
Figure 2. Alternate Menu View

Window Pane Navigation
Use the following chart to assist you in moving between and within the two window panes.

To do this...	Press this key...
Move from left pane to right pane	Tab Enter Right arrow
Move from right pane to left pane	Tab Escape Left arrow Backspace
Move within each pane	Up arrow Down arrow Left arrow Right arrow

Right Window Pane Notation
The right window pane shows the contents of the currently selected menu. These contents include both submenu items and data fields. Some submenus contain additional submenus and some data fields contain additional data fields. The following chart explains the notation used to identify these additional items.

This notation...	Means that...
[+]	more items are available when selected.
[DATA]	more items are available when selected.
<+>	an action is to be taken, such as activating a test.
Highlighted menu item	you can enter data in this field.
Underlined field	the field contains read-only information.

Additional Terminal Menu Window Features

• Mode – displays the network interface mode of the unit (for example, T1 IAD, SHDSL IAD, SDSL IAD, ADSL IAD)

• L2 Status – displays the current status of the L2 protocol (ATM sync is either up or down) – ATM Only

• DS0 Mapping – displays the current mapping of DS0s in the system. DS0s mapped to the router display **r**, unmapped DS0s display **–**, and all other DS0s display *****.

• Tool Tip – provides a brief description of the currently selected mode.

• Slot Status – displays type of module installed in each slot. No entry will appear for slots not containing a module.

• Telnet Info – displays the user name when connected via Telnet. This information is not displayed when connecting to the system via the **CRAFT** interface.

• Ethernet Link Status – displays the current status of the integrated Ethernet interface (located on the rear of the chassis).

• Extended Help – displays information about selected commands <CTRL+A>.

• Navigation Help – lists characters used for navigating the terminal menu and session management <CTRL+Z>.

• Config Status – displays ***** when current configuration contains changes that have not been saved to flash memory. Save changes by backing out to the main menu, or press <CTRL + W> to force a manual save.

Navigating using the Keyboard Keys

You can use various keystrokes to move through the terminal menu, to manage a terminal menu session, and to configure the system. Press <CTRL+Z > to activate a pop-up screen listing the navigation keystrokes.

Moving through the Menus

To do this...	Press this key...
Return to the home screen	H

Jump between two menu items
    Press <J> while the cursor is located on a menu item, and you jump back to the main screen.
    Go to another menu item, press <J>, and you jump back to the screen that was displayed the first time you pressed <J>.
    Press <J> anytime you want to jump between these items.
	J

Select items	Arrows
Edit a selected menu item	Enter
Cancel an edit	Escape
Close pop-up help screen	Escape
Move between the left and right panes	Tab Arrows
Move to the top of a screen	A

To do this...	Press this key...
Move to the bottom of a screen	Z
Ascend one menu level	Backspace
Jump to terminal mode	CTRL+T
Jump to NAT menu	CTRL+N

Session Management Keystrokes

To do this...	Press this key...
Log out of a session	CTRL+L
Refresh the screen To save time, only the portion of the screen that has changed is refreshed. This option should only be necessary if the display picks up incorrect characters caused by disconnecting and reconnecting the terminal session.	CTRL+R

Configuration Keystrokes

To do this...	Press this key...
Restore factory default settings This setting restores the factory defaults based on the location of the cursor. If the cursor is on an interface line (in the **INTERFACES** menu), then only the selected interface is updated to factory defaults.	F

Copy selected items to the clipboard
The amount of information you can copy depends on the cursor location when you press <C>:
    If the cursor is over an editable field, only that item is copied.
    If the cursor is over the index number of a list, then all of the items in the row of the list are copied. For example, if the cursor is over the selection # field in the **INTERFACES** screen, all of the information associated with the interface is copied.
	C

Paste the item stored in the clipboard, if the information is compatible You must confirm all pastes — except those to a single editable field.	P
Increment the value of certain types of fields by one when you paste information into those fields	>
Decrement the value of certain types of fields by one when you paste information into those fields	<
Save the current configuration immediately to flash memory	CTRL+W
Insert a new list item For example, add a new item to the **TELNET USER** connection list by pressing <I> while the cursor is over the index number.	I

To do this...	Press this key...
Delete a list item **For example, delete an item from the TELNET USER connection list by pressing <D>** while the index number is active.	D

Getting Help

The bottom line of the terminal menu window contains context-sensitive help information. When the cursor is positioned over a set of configuration items, a help message displays (when available) providing a description of the item. When more detailed help is available for a particular item, **^A** displays at the bottom of the window. At this point, pressing <CTRL+A> displays a pop-up help screen with information about the item.

Press <CTRL+Z> to activate a help screen that displays the available keystrokes you can use to navigate the main menu system. Press <Exit> to remove these help screens.

2.   MAIN MENU AND SYSTEM CONTROL

Selecting the Appropriate Menu

The main menu system is the access point to all other operations. Each menu item has several functions and submenus that identify and provide access to specific operations and parameters. Use the following chart to help select the appropriate menu.

To do this...	Go to this menu...
Review and monitor general system information for the Total Access 6XX	**SYSTEM INFO**
Set up the operational configuration for the Total Access 6XX	**SYSTEM CONFIG**
Upgrade firmware, perform config transfers, ping, and access terminal mode	**SYSTEM UTILITY**
Review and configure settings for all interfaces (including installed modules)	**INTERFACES**
Configures the Layer 2 protocol for the various interfaces (T1, Ethernet, etc.) and provides all applicable L2 status information	**L2 PROTOCOL**
Configure the bridging parameters and view applicable bridging statistics	**BRIDGE**
Define, configure, and monitor all Total Access 6XX Router functions	**ROUTER**
Configure security filters for L2 traffic and define RADIUS server parameters	**SECURITY**
Map data and voice ports (from integrated interfaces as well as installed modules) to network time slots	**DS0 MAPS**

Security Levels

> **NOTE** *Password security levels only apply to Telnet connections. Connecting to the system through the rear **CRAFT** interface automatically provides maximum rights.*

To edit main menu system items, you must have a password and the appropriate security level. Table 1 describes the security levels.

Table 1. Password Security Level

Security Level	Description
Full	Permission to edit every menu item, including creating and editing passwords - **maximum rights**
Support	Access to all commands except passwords
Config	Access to all commands except passwords, flash/firmware download, configuration transfers, authentication methods, terminal mode, and unit reset
Router	Read/write access to all Router menu items
Voice	Read/write access to all Voice menu items
Status	Read-only permission for all menu items - **minimum rights**

3.   MENU DESCRIPTIONS

The remainder of this section describes Total Access 6XX menu and submenu options.

> **NOTE** *To help you follow the terminal menu hierarchy, the following notations are used:*
>
> **MENUS > SUBMENUS > SUB-SUBMENUS**

SYSTEM INFO

The **SYSTEM INFO** menu provides basic information about the unit as well as data fields for editing information. Figure 3 displays the submenus that are available when you select this menu item.
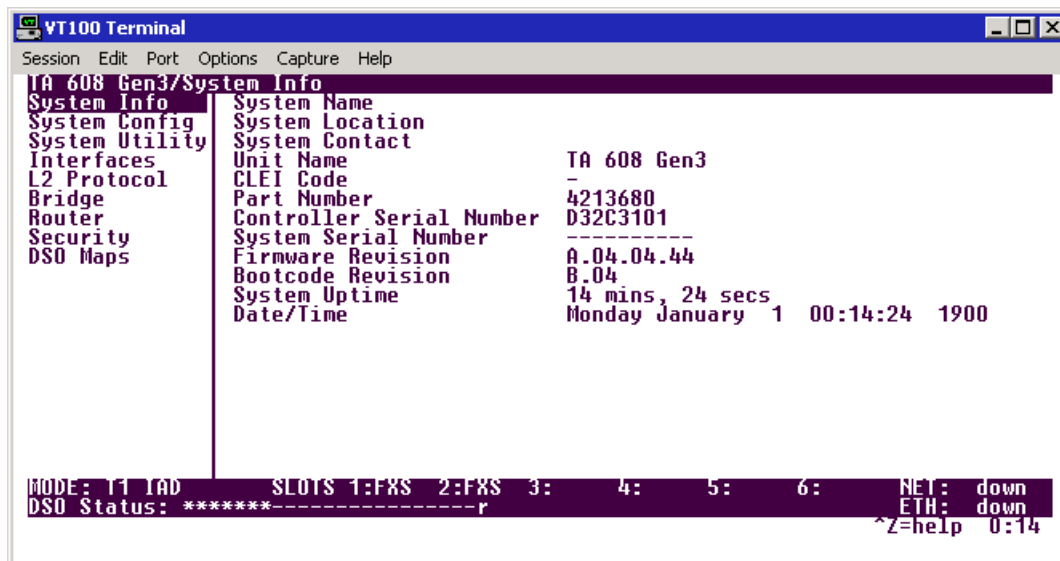
Figure 3. System Info Menu

SYSTEM INFO > SYSTEM NAME

Provides a user-configurable text string for the name of the unit. This name can help you distinguish between different installations. You can enter up to 127 alpha-numeric characters in this field, including spaces and special characters (such as an underscore). This name will appear on the top line of all screens.

SYSTEM INFO > SYSTEM LOCATION

Provides a user-configurable text string for the location of the unit. This field is to help you keep track of the actual physical location of the unit. You can enter up to 127 alphanumeric characters in this field, including spaces and special characters (such as an underscore).

SYSTEM INFO > SYSTEM CONTACT

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or E-mail address of a person responsible for the unit. You can enter up to 127 alpha-numeric characters in this field, including spaces and special characters (such as an underscore).

SYSTEM INFO > UNIT NAME

(Read only) Displays a product-specific name for the unit (such as TA 616, TA 604, etc).

SYSTEM INFO > CLEI CODE

(Read only) Displays the registered CLEI code for the unit.

SYSTEM INFO > PART NUMBER

(Read only) Displays the ADTRAN-specific part number for the unit.

SYSTEM INFO > CONTROLLER SERIAL NUMBER

(Read only) Displays the ADTRAN-specific part number for the chassis hardware. The serial number of the unit will automatically display in this field. This serial number matches the serial number located on the bottom of the unit's chassis.

SYSTEM INFO > SYSTEM SERIAL NUMBER

(Read only) Displays the serial number for the entire system configuration including specific network interface, FXS specifics, and specialized software, as well as the base chassis. This serial number must be programmed at ADTRAN and will display dashes (----) for any unit manufactured prior to this serial number addition.

SYSTEM INFO > FIRMWARE REVISION

(Read only) Displays the current firmware revision level of the unit.

SYSTEM INFO > BOOTCODE REVISION

(Read only) Displays the current bootcode revision.

SYSTEM INFO > SYSTEM UPTIME

Displays the length of time the unit has been running. Each time you reset the system, this value resets to 0 days, 0 hours, 0 min and 0 secs.

SYSTEM INFO > DATE/TIME

Displays the current date and time, including seconds. To edit this field, place the cursor on the field and press **<ENTER>**. Then, enter the time in a 24-hour format (such as 23:00:00 for 11:00 pm), and the date in mm-dd-yyyy format (for example, 05-23-2004). Press **<ENTER>** when you are finished to accept the change.

> **NOTE**
>
> *The System Date and Time will reset to 12:00 January 1, 1990 after a system power loss. If accurate system date and time information is crucial, consider using a time server to prevent the clock reset.*

SYSTEM CONFIG

Set up the unit's operational configuration from the **SYSTEM CONFIG** menu. Figure 4 shows the items included in this menu.
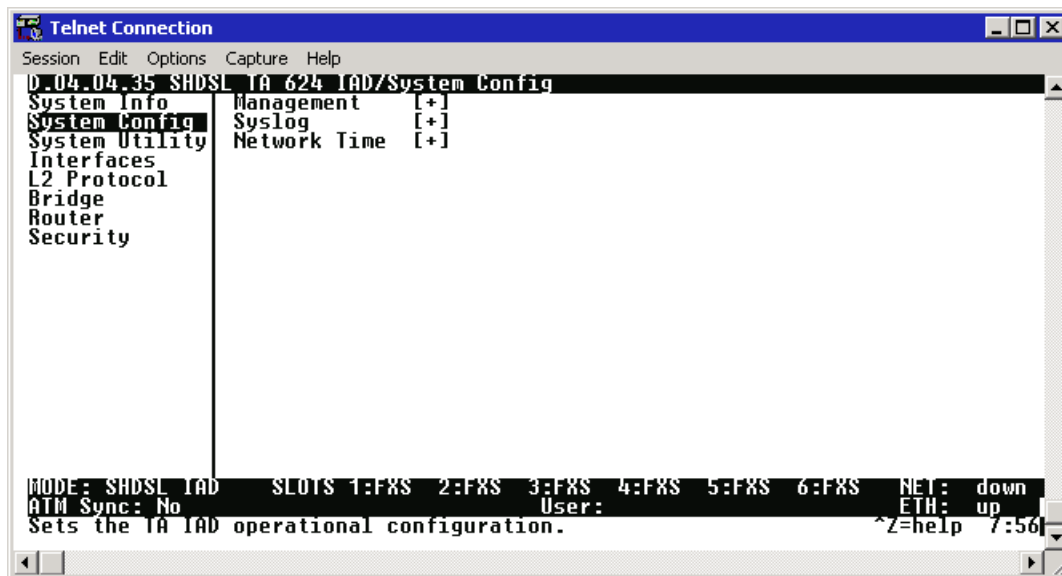
Figure 4. System Config Menu

SYSTEM CONFIG > MANAGEMENT

Set up the **CRAFT** port, **TELNET ACCESS**, **SNMP MANAGEMENT**, and **FDL MANAGEMENT** from this menu.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT

Set up the **CRAFT** port parameters from this menu. The unit's VT100 **CRAFT** port can be accessed via an RJ-48 connector located on the rear of the unit.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PASSWORD PROTECT

When **PASSWORD PROTECT** is set to **NO**, the **CRAFT** port is not password protected. When set to **YES** (def), the unit will prompt for a password upon startup.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PASSWORD

Enter the user-defined password (up to 30 alphanumeric characters including spaces and special characters) to protect the **CRAFT** port. By default, no password is entered. Table 2 on page 52 provides instructions for changing the password.

> *Connecting directly to the* **CRAFT** *port provides full access to all menus. Enable the password on the* **CRAFT** *port to protect against unauthorized access.*

Table 2. Instructions for Changing Passwords

Step	Action
1	Select the **PASSWORD** field—a new **PASSWORD** field displays.
2	Type the new password in the **ENTER** field.
3	Type the new password again in the **CONFIRM** field.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > IDLE TIME

This option defines the amount of time in minutes user may stay connected without any activity on the **CRAFT** port before the user is automatically logged out of the system. A value of **0** disables this inactivity timer function enabling users to stay connected until manually logged out. The value range is **0** (def) to **255** (minutes).

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > BAUD RATE

This is the asynchronous rate that the **CRAFT** port will run. The possible values are **300**, **1200**, **2400**, **4800**, **9600**, **19200**, **38400**, **57600**, and **115200**. The default value is **9600**. The unit and the VT100 terminal or PC with terminal emulation software must be set for the same baud rate.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > DATA BITS

The number of data bits that the **CRAFT** port sends in a frame. The possible values are **7** or **8** (def) bits. The unit and the VT100 terminal or PC with terminal emulation software must be set for the same number of data bits.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PARITY

This is the asynchronous parity that the **CRAFT** port will run. The possible values are **NONE** (def), **ODD**, or **EVEN**. The unit and the VT100 terminal or PC with terminal emulation software must have the same parity setting.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > STOP BITS

This is the number of stop bits used for the **CRAFT** port. The possible values are **1** (def), **1.5** or **2**. The unit and the VT100 terminal or PC with terminal emulation software must have the same number of specified stop bits.

SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS

Activate the Telnet access and set up the various Telnet parameters from this menu. The Total Access 6XX supports up to five simultaneous Telnet sessions.

> **NOTE**
> *The Total Access 6XX ships with default Telnet Access parameters of: guest (user), password (password). Change this password during the initial configuration to protect your unit.*

SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > ACCESS

Sets ACCESS to ON or OFF to allow or block telnet access to the unit. The factory default value for this parameter is ON.

SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > AUTHEN METHOD

Set up the Telnet authentication method from this menu. The choices are LOCAL PASSWORD, RADIUS, LOCAL/RADIUS, and RADIUS/LOCAL. LOCAL/RADIUS indicates that the unit will try Local Password Authentication first, and if that fails, it will try Radius Authentication. RADIUS/LOCAL indicates that the unit will try Radius authentication first, and if that fails, it will try Local Password authentication. The default is LOCAL PASSWORD.

SYSTEM CONFIG > MANAGEMENT > TELNET PORT

Defines the TCP port number used when establishing a Telnet session. Normal Telnet port is **23**. Enter a customized port number if desired. Make certain the Telnet program you use is configured for the same port number (if using a customized port number).

SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > USER LIST

Add Telnet users and control the Telnet access conditions through this menu.

#

Display the index number of the Telnet users. Up to four users can be configured for access to the unit. Each user can be assigned a security level and idle time.

NAME

The name is a text string of the user name for this session. The factory default is UNASSIGNED in the NAME field.You must enter a username in this field (up to 15 characters) because the Telnet entry is not activated until it is assigned a valid username. Editing the UNASSIGNED default to be blank is allowed for a single Telnet entry; duplicate usernames are not allowed. During an active Telnet session the NAME is displayed in the Telnet Information field located at the bottom of the menu screen.

PASSWORD

When the authenticating method is LOCAL PASSWORD, or LOCAL/RADIUS, this text string is used for the password. You can enter up to 30 characters in this field. The factory default is no entry in this field.

IDLE TIME (MINS)

This sets the amount of time in minutes you can be idle before you are automatically logged off. The factory default is **10 MINUTES**. The range is **1 TO 255 MINUTES**.

LEVEL

This is the security level granted to the user. Table 3 on page 54 gives a brief description of each level. The factory default is FULL.

Table 3. Telnet Security Levels

Security Level	Description
Full	The user has all access to view and configure all menus (same as logging in to the **CRAFT** port)
Support	The user has read only access to view the **SYSTEM INFO** menu. The user has privileges to view and change everything under the **SYSTEM CONFIG** menu except for the **CRAFT** port settings, Telnet access lists, and the SNMP management communities. The user has full access to the **SYSTEM UTILITY** menu, including the ability to upgrade firmware and reset the unit. The user has full access to the **INTERFACES, L2 PROTOCOL, BRIDGE, ROUTER,** and **DS0** menus. The user does not have the ability to set **RADIUS SERVER** settings under the **SECURITY** menu.
Config	The same privileges as support, except that the user does not have privileges to download firmware or configuration from the **SYSTEM UTILITY** menu. The user additionally does not have the privilege to reset the unit remotely, or enter the terminal menu.
Router	The user has read only privileges for the **SYSTEM INFO** menu. There is no access to the **SYSTEM CONFIG** menu. The user has **PING** and **TRACEROUTE** access from the **SYSTEM UTILITY** menu. The user is limited to Ethernet configuration and status from the **INTERFACES** menu. The user has full access to the **BRIDGE** and **ROUTER** menus. Access is limited to filters only from the **SECURITY** menu.
Voice	The user has read only privileges for the **SYSTEM INFO** menu. The user has access to the **PING** and **TRACEROUTE** utilities from the **SYSTEM UTILITIES** menu. The user has full access to the FXS module from the **INTERFACES** menu.
Status	The user has read access of all menus except for the following: **SYSTEM CONFIG/CRAFT PORT, SYSTEM CONFIG/TELNET ACCESS, SYSTEM CONFIG/SNMP MANAGEMENT,** and **SECURITY/ RADIUS SERVER**. The user does not have access to **UPGRADE FIRMWARE, UPGRADE CONFIG, PING,** or **TRACEROUTE** menus. The user cannot reset the unit or enter terminal mode.

SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > ACTIVE SESSIONS

Provides a list of all Telnet sessions currently active on the system.

#

Displays the index number of the Telnet user.

NAME

Displays the assigned user name.

PORT

Displays the TCP port used for this Telnet session.

TIME TO LIVE

Displays the amount of time (in minutes) before this Telnet session is terminated, if the user remains idle.

SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > IP ACCESS LIST

Set up the list of allowed Telnet connections by specifying the IP address of the systems used to control the unit.

NETWORK ADDRESS

Enter network addresses from which Telnet access to the unit is allowed. When a remote unit requests Telnet access to the unit, if the access list is empty or the remote's IP address matches a list entry, remote access is granted. A network address of 0.0.0.0 with corresponding netmask 255.255.255.255 blocks all host Telnet access.

The factory default is **0.0.0.0.** (with a **0.0.0.0** subnet **MASK**), which allows all users Telnet access.

MASK

The mask is used to determine which bits of the **NETWORK ADDRESS** are significant. A "0" bit means "don't care." A "1" bit means that the corresponding address bits in the incoming IP packet must match the address bit in the defined **NETWORK ADDRESS**. The netmask of 255.255.255.255 defines a single IP as the only allowed IP address from the specified network. A **NETWORK ADDRESS** defined as 192.22.1.0 with a **NETMASK** of 255.255.255.0 allows all units on the 192.22.1.0 network Telnet access to the unit. The default value is **0.0.0.0** (with a default **NETWORK ADDRESS** of **0.0.0.0**), which allows all users Telnet access.

SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT

Activate the SNMP management and configure the SNMP communities and traps from this menu.

SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > ACCESS

When set to **OFF**, SNMP access is denied. When set to **ON**, the unit will respond to SNMP managers based on the configuration of the **COMMUNITIES** fields. The factory default is **ON**.

SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > TRAP DELAY

When enabled, the Total Access 600 Series inserts a delay before transmitting a created trap for the SNMP session.

SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > COMMUNITIES

Set up the SNMP communities parameters from this menu.

#

Displays the index number of the SNMP Communities. This list is used to set up to 8 SNMP communities that the unit will allow.

NAME

This is the text string used to identify the SNMP community. The factory default is no entry in the name parameter.

PRIVILEGE

The access for this manager can be assigned three levels. The factory default is **NONE**.

NONE	No access is allowed for this community or manager.
GET	Manager can only read items.
GET/SET	Manager can read and set items.

MANAGER IP

This may be used in conjunction with the Netmask field to define a range of manager IPs. A netmask of 255.255.255.255 defines a single IP as the manager host IP. A **MANAGER IP** defined as 192.22.1.0 with a **NETMASK** of 255.255.255.0 allows all managers on the 192.22.1.0 network access to the SNMP information. The default value is **0.0.0.0**.

NETMASK

The mask is used to determine which bits of the **MANAGER IP** are significant. A "0" bit means "don't care." A "1" bit means that the corresponding address bits in the incoming SNMP packet must match the address bit in the defined **MANAGER IP**. The netmask of 255.255.255.255 defines a single IP as the manager host IP. A **MANAGER IP** defined as 192.22.1.0 with a **NETMASK** of 255.255.255.0 allows all managers on the 192.22.1.0 network access to the SNMP information. The default value is **0.0.0.0**.

SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > TRAPS

Sets up the trap manager name and IP from this menu.

#

Displays the index number in the SNMP traps table. This list allows up to 20 managers to be listed to receive traps.

MANAGER NAME

The text string describing the name of the entry. It is intended for easy reference and has no bearing on the SNMP trap function. You can enter up to 31 characters in this field. The factory default is no entry in the **MANAGER NAME** field.

MANAGER IP

This is the IP address of the manager that is to receive the traps. The factory default is **0.0.0.0**.

SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT

Enables the FDL management and configures mode and IP addresses from this menu.

SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > MODE

This enables the FDL (only in ESF mode) to be used for management. Learning mode can also be enabled so the unit can "learn" its IP configuration from the connected DSLAM to be used for its FDL management. Once it learns this information from, for example a Total Access 4303, the configuration items populate. The factory default is **ON**.

SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > LINK IP ADDRESS

This is the local IP address used for FDL management. The FDL uses a separate IP network for communication, distinct from the customer data that is configured under the **ROUTER** menus. The factory default is **0.0.0.0**.

SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > IP NETMASK

This is the subnet mask defining the IP network used for FDL management. The factory default is **0.0.0.0**.

SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > FAR-END IP ADDRESS

This is the far-end IP address used for the FDL management. The FDL is a separate IP network from the customer data that is configured under the **ROUTER** menus. The **FAR-END IP ADDRESS** is generally the management IP from the DSLAM. The factory default is **0.0.0.0**.

SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > LEARN ADDRESS

When set to **ON**, the destination address on each received packet is assumed to be the FDL interface address. A 255.255.255.254 netmask is used, which determines the far-side address as well (since there can be only two addresses on a subnet with that netmask). When set to **OFF,** the user must input the IP address assigned to the FDL interface. Default is **ON**.

SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > ACCEPT ALL SNMP

When set to **ON**, SNMP gets/sets received over the FDL link are always accepted regardless of the community table. When set to **OFF,** the community table is searched for valid manager IP addresses and the SNMP traffic is rejected if a match is not found. Default is **ON**.

SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > MTU

(Maximum Transmit Unit) Defines the largest packet size sent over the FDL. All packets greater in size than the MTU are fragmented.

SYSTEM CONFIG > SYSLOG

Configure the unit Syslog client for use with a Syslog server (supplied with ADTRAN Utilities or available on most Unix platforms) from this menu.

> **NOTE** *For additional information, reference RFC3164: The BSD Syslog Protocol.*

SYSTEM CONFIG > SYSLOG > SYSLOG IP

IP address of the syslog daemon to which log message should be sent. The values must be dotted decimal notation.

SYSTEM CONFIG > SYSLOG > SYSLOG FORMAT

The **SYSLOG FORMAT** is the format of log messages. "**ADTRAN**" uses a format that is compatible with ADTRAN Utilities and forces the Syslog Facility to LOCAL0. **UNIX** uses the traditional Unix format and reports at the configured facility level.

> **NOTE**   *ADTRAN Utilities may malfunction if messages are received in the Unix format.*

SYSTEM CONFIG > SYSLOG > SYSLOG FACILITY

The choices are: **LOCAL0**, **LOCAL1**, **LOCAL2**, **LOCAL3**, **LOCAL4**, **LOCAL5**, **LOCAL6**, **LOCAL7**. **SYSLOG FACILITY** is the facility level for all messages forwarded from the unit to the syslog server. This allows all messages received from the IAD to be filtered by facility level. See *RFC3164: The BSD Syslog Protocol*.

> **NOTE**   *This does not have to correspond to the facility level shown in the terminal mode option. See SYSLOG using Terminal Mode on page 59.*

The remaining Syslog parameters have the following level choices:

    FATAL (Highest priority)
    ALERT
    CRITICAL
    ERROR
    WARNING
    NOTICE
    INFO
    DEBUG (Lowest priority)

Every log message generated by the IAD has a reporting level priority. If the message priority is lower than the configured priority for the destination log, the message is not forwarded to the syslog daemon. See *RFC3164: The BSD Syslog Protocol*. The lower the log level, the more messages that will be generated. Setting reporting levels to DEBUG may negatively affect the performance of the IAD, including causing the IAD to reset.

> **NOTE**   *ADTRAN recommends using DEBUG for only short periods of time, and for debug purposes only.*

SYSLOG using Terminal Mode

Another option for configuring syslog is using the terminal mode command **log dump <logname>**. The logname must be all CAPS must match the listings below. The command will dump all messages for the indicated log (**ALL LEVEL** shows all log messages) stored in the internal log buffer to the command line display.

SYSTEM CONFIG > SYSLOG > ALL LEVEL

This entry allows setting the default reporting level for all log entries. If **ALL LEVEL** is a lower priority than the individual log entry level, **ALL LEVEL** overrides the individual log reporting level.

SYSTEM CONFIG > SYSLOG > KERNEL LEVEL

Minimum required level for sending KERNEL log messages. Kernel messages provide low-level status information concerning the operation of the unit.

SYSTEM CONFIG > SYSLOG > DHCP LEVEL

Minimum required level for sending DHCP log messages. DHCP log messages provide status information on IP addressing information concerning the DHCP server or clients.

SYSTEM CONFIG > SYSLOG > NTP LEVEL

Minimum required level for sending NTP log messages. Network Time Protocol log messages provide information regarding the network time settings.

SYSTEM CONFIG > SYSLOG > TFTP LEVEL

Minimum required level for sending TFTP log messages. TFTP log messages provide status information concerning firmware upgrades and configuration transfers utilizing the TFTP protocol.

SYSTEM CONFIG > SYSLOG > TELNET LEVEL

Minimum required level for sending TELNET log messages.Telnet log messages provide status information concerning telnet requests and connections to the unit.

SYSTEM CONFIG > SYSLOG > IP LEVEL

Minimum required level for sending IP log messages. IP log messages provide information concerning IP packets that are sent and received to and from the unit.

SYSTEM CONFIG > SYSLOG > PPP LEVEL

Minimum required level for sending PPP log messages. PPP log messages provide status information concerning PPP packets and connections through the system.

SYSTEM CONFIG > SYSLOG > NAT LEVEL

Minimum required level for sending NAT log messages. NAT log messages provide status information concerning Network Address Translation being performed by the system.

SYSTEM CONFIG > SYSLOG > ARP LEVEL

Minimum required level for sending ARP log messages. Address Resolution Protocol log messages provide status information for all ARP requests sent and received by the unit.

SYSTEM CONFIG > SYSLOG > UDP LEVEL

Minimum required level for sending UDP log messages. UDP log messages provide status information concerning UDP packets sent and received by the system.

SYSTEM CONFIG > SYSLOG > NETWRITE LEVEL

This parameter is for ADTRAN internal use only.

SYSTEM CONFIG > SYSLOG > TCP LEVEL

Minimum required level for sending TCP log messages. TCP log messages provide status information concerning TCP packets sent and received by the system.

SYSTEM CONFIG > SYSLOG > COMPSYS LEVEL

This parameter is for ADTRAN internal use only.

SYSTEM CONFIG > SYSLOG > CONSOLE LEVEL

This parameter is for ADTRAN internal use only.

SYSTEM CONFIG > SYSLOG > CFGXFER LEVEL

Minimum required level for sending configuration transfer log messages. Configuration transfer log messages provide status information on all attempted configuration transfers.

SYSTEM CONFIG > SYSLOG > ROUTER LEVEL

Minimum required level for sending router log messages. Router messages may provide status information on routing functions within the unit.

SYSTEM CONFIG > SYSLOG > NONVOL LEVEL

Minimum required level for sending nonvolatile memory log messages. Nonvol messages may provide status information when the flash memory is accessed (to either store or read data).

SYSTEM CONFIG > SYSLOG > NOKIA LEVEL

Minimum required level for sending log messages about communication with the Nokia DSLAM. Messages are only generated for products with an SDSL WAN interface.

SYSTEM CONFIG > SYSLOG > AUTOBAUD LEVEL

Minimum required level for sending log messages about communication with the Lucent Stinger DSLAM. Messages are only generated for products with an SDSL WAN interface.

SYSTEM CONFIG > SYSLOG > TOLLBRG LEVEL

Minimum required level for sending log messages about communication with the Tollbridge Voice Gateway. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > CMCP LEVEL

Minimum required level for sending log messages about communication with the CopperMountain DSLAM. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > SDSL LEVEL

This parameter is for ADTRAN internal use only.

SYSTEM CONFIG > SYSLOG > L1 LEVEL

Minimum required level for sending log messages about WAN physical or Layer 1 connection. Layer 1 messages provide status and alarm information on the state of the physical interface (for example, up or down).

SYSTEM CONFIG > SYSLOG > ETH LEVEL

Minimum required level for sending log messages about Ethernet physical connection. These status messages provide information concerning data packets transmitted and received on the **10/100BASET** interface.

SYSTEM CONFIG > SYSLOG > ICMP LEVEL

Minimum required level for sending ICMP log messages. ICMP log messages provide information for ICMP packets sent and received by the system.

SYSTEM CONFIG > SYSLOG > CONFIG LEVEL

This parameter is for ADTRAN internal use only.

SYSTEM CONFIG > SYSLOG >DS0 LEVEL

Minimum required level for sending log messages about DSO mapping.

SYSTEM CONFIG > SYSLOG > SELFTEST LEVEL

Minimum required level for sending log messages about selftest.

SYSTEM CONFIG > SYSLOG > VOICE LEVEL

Minimum required level for sending log messages about AAL2 voices services.
Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > JETSTREAM LEVEL

Minimum required level for sending log messages about communication with the JetStream Voice Gateway. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > POTS LEVEL

Minimum required level for sending log messages about POTS line cards and services.

SYSTEM CONFIG > SYSLOG > LESCAS LEVEL

Minimum required level for sending messages about communication with LESCAS compatible Voice Gateways. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > ATM LEVEL

Minimum required level for sending ATM log messages. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > COPPERCOM LEVEL

Minimum required level for sending log messages about communication with the CopperCom Voice Gateway. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > VOFR LEVEL

Minimum required level for sending voice-over-frame-relay log messages about communication with the CopperMountain DSLAM. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > XMODEM LEVEL

Minimum required level for sending XMODEM log messages for firmware and configuration transfers.

SYSTEM CONFIG > SYSLOG > EMWEB LEVEL

This parameter is for ADTRAN internal use only.

SYSTEM CONFIG > SYSLOG > FRELAY LEVEL

Minimum required level for sending frame relay log messages. Frame Relay log messages provide information for frame relay packets sent to and from the unit as well as link status information.

SYSTEM CONFIG > SYSLOG > BRIDGE LEVEL

Minimum required level for sending bridge mode log messages. Bridge log messages provide status information for bridging process being performed by the unit.

SYSTEM CONFIG > SYSLOG > MAINT LEVEL

Minimum required level for sending **CRAFT** port log messages. Craft messages provide information concerning the operation of the **CRAFT** interface.

SYSTEM CONFIG > SYSLOG > HDLC LEVEL

Minimum required level for sending low level HDLC log messages. HDLC log messages provide status information concerning HDLC processes performed by the unit (sent and received packets, etc.).

SYSTEM CONFIG > SYSLOG > VOATM LEVEL

Minimum required level for sending Voice-over-ATM log messages. VoATM messages provide status information concerning the FXS (or FXO for Total Access 624 units only) voice signaling occurring over the ATM link.

SYSTEM CONFIG > SYSLOG > PPPOA LEVEL

Minimum required level for sending PPP-over-ATM log messages. PPPoA log messages provide status information concerning PPP packets being sent and received over the ATM link.

SYSTEM CONFIG > SYSLOG > FDL LEVEL

Minimum required level for sending FDL log messages. FDL log messages provide status information concerning the operation of the FDL link.

SYSTEM CONFIG > SYSLOG > FILTER

Minimum required level for sending Filter log messages.

SYSTEM CONFIG > NETWORK TIME

Activate the network time and configure the server type, time zone and various other network time parameters from this menu.

SYSTEM CONFIG > NETWORK TIME > SERVER TYPE

The unit time can be entered manually from the **SYSTEM INFO** menu, or the unit can receive time from an NTP/SNTP server. The **NETWORK TIME** menu includes all parameters relating to how the unit communicates with the time server.

The server type defines the port on which the unit will listen to receive timing information from the time server. The choices are **NT TIME** and **SNTP**. When set to **NT TIME**, the unit will receive time from an NT server running SNTP software on its TIME port. When set to **SNTP**, the unit will receive time directly from an SNTP server. The factory default is **SNTP**.

SYSTEM CONFIG > NETWORK TIME > ACTIVE

This network timing feature can be turned on and off. It determines whether the unit will request and receive time from a time server. The factory default is **NO**.

SYSTEM CONFIG > NETWORK TIME > TIME ZONE

All time zones are based off of Greenwich Mean Time (GMT). The choices are listed below.

- **GMT**
- **GMT -5 (EASTERN)**
- **GMT -6 (CENTRAL)**
- **GMT -7 (MOUNTAIN)**
- **GMT -8 (PACIFIC)**
- **GMT -9 (ALASKA)**
- **GMT -10 (HAWAII)**

The factory default is **GMT-6 (CENTRAL)**.

SYSTEM CONFIG > NETWORK TIME > ADJUST FOR DAYLIGHT SAVING

Since some areas of the world use Daylight Savings Time, the unit is designed to adjust the time on the first Sunday in April and the last Sunday in October accordingly if this option is turned on. The factory default is **YES**.

SYSTEM CONFIG > NETWORK TIME > HOST ADDRESS

This is the IP address of the time server that the unit will request and receive time from. The factory default is no entry in the host address field.

SYSTEM CONFIG > NETWORK TIME > REFRESH

This is the interval of time between each request the unit sends out to the time server. A smaller refresh time guarantees that the unit receives the correct time from the server and corrects possible errors more quickly. This may be more taxing on the machine. A range of refresh times is available for the user to decide which is best for their unit. Choices include **5 MINS, 10 MINS, 15 MINS, 20 MINS, 25 MINS, 30 MINS, 35 MINS, 40 MINS, 45 MINS, 50 MINS, 55 MINS,** and **60 MINS**. The factory default is **60 MINS**.

SYSTEM CONFIG > NETWORK TIME > STATUS

This displays the current status of the time negotiation process. If an error is displayed, check all connections and configurations to try to resolve the problem.

SYSTEM UTILITY

Use the **SYSTEM UTILITY** menu to view and set the system parameters shown in Figure 5.
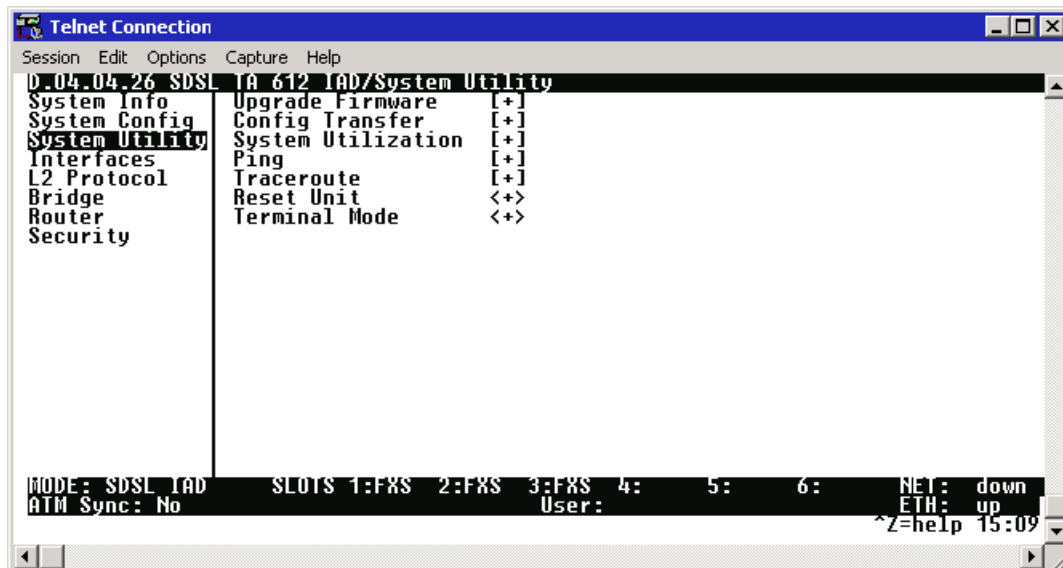
Figure 5. System Utility Menu

SYSTEM UTILITY > UPGRADE FIRMWARE

Select the firmware upgrade method and perform upgrade from this menu.

SYSTEM UTILITY > UPGRADE FIRMWARE > TRANSFER METHOD

The customer can update firmware when unit enhancements are released.

The two methods for upgrading are **XMODEM** and **TFTP**. (See the DLP section of this manual for more information.) **TFTP** requires a TFTP server running on the network. The unit starts a TFTP client function which gets the upgrade code from the TFTP server. Selecting **XMODEM** will load the upgrade code through the **CRAFT** port using any PC terminal emulator with XMODEM capability. The factory default is **TFTP**.

SYSTEM UTILITY > UPGRADE FIRMWARE > TFTP SERVER ADDRESS

This is required when the transfer method is TFTP. It is the IP address or domain name (if DNS is configured) of the TFTP server. The factory default is no entry in the **TFTP SERVER ADDRESS** field.

SYSTEM UTILITY > UPGRADE FIRMWARE > TFTP SERVER FILENAME

This is required when the transfer method is TFTP. It is the case-sensitive file name which contains the upgrade code. The factory default is no entry in the **TFTP SERVER FILENAME** field.

SYSTEM UTILITY > UPGRADE FIRMWARE > TRANSFER STATUS

This appears when TFTP is used. It displays the status of the transfer as it happens. Any error or success message will be displayed here.

SYSTEM UTILITY > UPGRADE FIRMWARE > START TRANSFER

This activator is used when the configurable items in this menu are complete. This will initiate the transfer for either TFTP or XMODEM upgrades.

> **NOTE**
> *Before using **START TRANSFER**, the unit should have a valid IP address, subnet mask, and default gateway (if required). See DLP-3, Setting IP Parameters, for more information.*

SYSTEM UTILITY > UPGRADE FIRMWARE > ABORT TRANSFER

Use this activator to cancel any TFTP transfer in progress.

SYSTEM UTILITY > CONFIG TRANSFER

Select the config transfer method and perform the transfer from this menu. Sends a binary file containing the unit configuration to a PC connected to the **CRAFT** port using XMODEM protocol or to a file on a TFTP server using the TFTP protocol.

CONFIG TRANSFER also lets you save the unit configuration as a backup file, so you can use the same configuration with multiple units. In addition, **CONFIG TRANSFER** can retrieve a configuration file from a TFTP server.

To support these transfers, ADTRAN delivers a TFTP program with the unit called TFTP Server. You can configure any PC running Microsoft Windows with this software, and store a configuration file.

> *Before using **START TRANSFER**, the unit should have a valid IP address, subnet mask, and*
> NOTE *default gateway (if required). See DLP-3, Setting IP Parameters, for more information.*

Only one configuration transfer session (upload or download) can be active at a time. **XMODEM** and **TFTP** are supported.

SYSTEM UTILITY > CONFIG TRANSFER > TRANSFER METHOD

The two methods for transferring a file are **XMODEM** and **TFTP**. (See the DLP section of this manual for more information.) **TFTP** requires a TFTP server running on the network. The unit starts a TFTP client function which gets the configuration file from the TFTP server or saves the existing configuration to the TFTP server. Selecting **XMODEM** will load the configuration file or save the file through the **CRAFT** port using any PC terminal emulator with XMODEM capability. The factory default is **TFTP**.

SYSTEM UTILITY > CONFIG TRANSFER > TFTP SERVER IP ADDRESS

Specifies the IP address of the TFTP server. Get this number from your system administrator. If using the ADTRAN Utilities TFTP server, this number appears in the TFTP server status window. The factory default value is **0.0.0.0**.

SYSTEM UTILITY > CONFIG TRANSFER > TFTP SERVER FILENAME

Defines the name of the configuration file that you transfer to or retrieve from the TFTP server. The default name is **ta_iad.cfg**, but you can edit this name.

SYSTEM UTILITY > CONFIG TRANSFER > CURRENT TRANSFER STATUS

Indicates the current status of the update.

SYSTEM UTILITY > CONFIG TRANSFER > PREVIOUS TRANSFER STATUS

Indicates the status of the previous update.

SYSTEM UTILITY > CONFIG TRANSFER > LOAD AND USE CONFIG

Retrieves the configuration file specified in the **TFTP SERVER FILENAME** field from the server. To start this command, enter **Y** to begin or enter **N** to cancel.

SYSTEM UTILITY > CONFIG TRANSFER > SAVE CONFIG REMOTELY

Saves the configuration file specified in **TFTP SERVER FILENAME** to the server identified in **TFTP SERVER IP ADDRESS**. To start this command, enter **Y** to begin or enter **N** to cancel.

> *Before using this command, you must have identified a valid TFTP server in **TFTP SERVER**
> CAUTION **IP ADDRESS**.*

SYSTEM UTILITY > SYSTEM UTILIZATION

View the CPU utilization stats from this menu.

SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE

Clear the system utilization stats and view the total and current CPU utilization stats from this menu.

SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE > CPU UTILIZATION

Provides maximum CPU utilization percentages for the following intervals:

FROM POWER-UP	Max CPU utilization since the last Total Access 600 Series restart.
LAST SECOND	Max CPU utilization in the last second. This is the most current CPU utilization information.
FROM LAST CLEAR	Max CPU utilization since the last manual clear of the performance statistics using the CLEAR STATS command.

SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE > ISR UTILIZATION

ISRs are interrupt service routines used within the unit for operational tasks. ISR Utilization provides information concerning the amount of time spent completing these processes. ISR Utilization information is only available for 3rd Gen systems and will always show 0 on 2nd Gen units.

FROM LAST CLEAR	ISR utilization since the last manual clear of the performance statistics using the CLEAR STATS command.

NOTE	*ISR information provides useful statistics for ADTRAN's Technical Support group but are not intended for interpretation by the general audience.*

SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE > MAX INTERRUPT DURATION (μS)

Longest time that has been spent processing an interrupt, in microseconds.

SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE > MAX ISR DURATION #1-3 (μS)

Longest times (top 3) spent in an interrupt routine, in microseconds.

SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE > MAX ISR DURATION #1-3 (ID)

Process IDs of the interrupts with the longest processing times (top 3).

SYSTEM UTILITY > SYSTEM UTILIZATION > PERFORMANCE > CLEAR STATS

This activator will clear all the system utilization performance stats.

SYSTEM UTILITY > PING

Activate the ping test and define the ping packet characteristics from this menu.

SYSTEM UTILITY > PING > START/STOP

Activator to start and cancel a ping test.

> 🖉 NOTE   *Only one ping session can be active at a time.*

> 🖉 NOTE   *Diagnostic features such as ping, extended ping, traceroute, extended traceroute, and Telnet client can also be performed via* **TERMINAL MODE** *(see page 69).*

SYSTEM UTILITY > PING > HOST ADDRESS

IP address or domain name (if DNS is configured) of device to receive the ping. The factory default is no entry in the host address field.

SYSTEM UTILITY > PING > SIZE (40-1500)

Total size of the ping to send. Range is **40** to **1500** bytes. The default is **64**.

SYSTEM UTILITY > PING > # OF PACKETS

Total packets to send. Setting this to **0** allows the client to ping continuously.
The default is **5**.

SYSTEM UTILITY > PING > # TRANSMITS

Total packets sent (read only).

SYSTEM UTILITY > PING > # RECEIVES

Total packets received (read only).

SYSTEM UTILITY > PING > % LOSS

Percentage loss based on ping returned from host (read only).

SYSTEM UTILITY > TRACEROUTE

Utility program used to trace a data path to a final destination.

SYSTEM UTILITY > TRACEROUTE > TRACE TARGET

Specifies the IP address of the remote system to trace the routes to.

SYSTEM UTILITY > TRACEROUTE > MAXIMUM HOPS

Specifies the maximum number of router exchanges allowed when traveling to the final destination (specified using the **TRACE TARGET** field) Range is **1** to **30**. Default is **30**.

SYSTEM UTILITY > TRACEROUTE > TIMEOUT (IN SECS)

Specifies the maximum delay (in seconds) given to a host (along a path to the final destination) to respond to the probe datagram sent before considering the packet a failure.

SYSTEM UTILITY > TRACEROUTE > RETRIES

Specifies the number of times the probe datagram is sent to each host (along the path to the final destination).

SYSTEM UTILITY > TRACEROUTE > BEGIN TRACEROUTE

Activates the traceroute process.

SYSTEM UTILITY > RESET UNIT

Selecting this activator will initiate a soft reset of the unit.

SYSTEM UTILITY > TERMINAL MODE

Selecting the terminal mode gives the user a command-line prompt to perform utilities such as pings, traceroutes, resets, firmware updates, configuration, and more. **TERMINAL MODE** can also be accessed by using the shortcut keys <Ctrl+T> from other menu screens. From this command-line prompt, you can:

- Perform a reset with the command "reset"
- Perform a **complete** factory restore with the command "factory_reset"
- Configure the unit. The unit has the ability to download a text file which contains the configuration of the entire unit. This configuration may then be altered in a text editor, and then uploaded to a unit. (See DLP-13, *Saving and Loading Text Configuration using Terminal Command Line*, for further assistance.)
- Debug and troubleshoot. This function would be carried out with the assistance of ADTRAN Technical Support.
- Start and stop the fail-safe timer for the auto-config feature.
- Perform a firmware upgrade via TFTP.

    upgrade_firmware *hostname filename*

- Use the **save** command to write the entire configuration to flash.
- Display the unit's MAC address with the command **mac**.
- Perform a ping or extended ping. Syntax is:

    ping hostname/address [repeat xx] [size xx] [timeout xx] [source xx] [noNat]

Options:

repeat <repeat count>	Number of pings to send (default 5)
size (datagram size)	Range is 40-1500
timeout (seconds)	Timeout in seconds (range 1-10)
source (address or name)	Source address or interface name to use
noNat	Do not NAT the ping packet

Options may be entered in any order and may be truncated.

Valid interface names are eth0, fdl0, ppp0, fr0, fr1, etc.

Example usage: **ping 10.0.0.5 r 10 si 1500 so eth0 n**

This will ping with a repeat count of 10. The datagram size is 1500 bytes, and the source address used in the ping packet will be the Ethernet IP address. The "noNat" option has been specified, so if NAT is enabled, this packet will NOT be translated.

- Perform a traceroute or extended traceroute. Syntax is:

  traceroute hostname/address [hops xx] [timeout xx] [retries xx] [source xx] [noNat]

  Options:

hops <hops count>	Max number of hops (default 30)
timeout <seconds>	Timeout in seconds (default 3)
retries <seconds>	Number of retries per hop (default 3)
source <address or name>	Source address or interface name to use
noNat	Do not NAT the trace packets

  Options may be entered in any order and may be truncated.

  Valid interface names are eth0, fdl0, ppp0, fr0, fr1, etc.

  Example usage: **trace 10.0.0.5 h 20 t 1 r 1 so eth0**

  This will perform a trace to 10.0.0.5 with a max hop count of 20. The timeout for each hop is 1 second, and the retry count per hop is 1. The Ethernet IP will be used as the source address, and the packet WILL go through NAT if NAT is enabled, meaning that the packet will be translated and the source address will be replaced by the NAPT address.

- Use the Telnet client feature to Telnet to a remote host. Syntax is:

  Telnet hostname/address [port xx]

  Default port is 23 (TELNET).

- To exit terminal mode, type **exit** or **!exit**,

  exit - if any configuration have been made, you will be prompted whether or not to save these changes. If no changes were made, the terminal session will exit without the confirm message.

  !exit - exit without saving or applying any configuration changes.

> NOTE
> *Extended ping, extended traceroute, and Telnet client are new features initially available in A.04.02. These functions may be performed simultaneously from multiple user sessions.*

INTERFACES

Use the **INTERFACES** menu to view and configure parameters for the various system interfaces (**T1**, **SHDSL**, **SDSL**, **ADSL**, Ethernet (**ETH**), **V.35**, **FXS**, **FXO**, and **DSX-1**). Figure 6 displays the interfaces menu for an SDSL IAD.

Figure 6. Interfaces Menus

INTERFACES (NETWORK T1)

View the network T1 interface status and configure T1 parameters from this menu. These menus are only applicable to T1 Total Access 600 Series systems.

INTERFACES (T1) > CONFIG

Configure the various T1 parameters and enable/disable loopbacks from this menu.

INTERFACES (T1) > CONFIG > TIMING MODE

Choices are **NETWORK**, **INTERNAL**, and **DSX-1**. Select **NETWORK** when the unit will receive timing from the network. Select **INTERNAL** when the unit will generate the timing. Select **DSX-1** when the system needs to take timing from the T1 connected to the **DSX-1** interface. (The **DSX-1** option is only valid for Total Access 600 Series systems that have the optional **DSX-1** interface.) Default is **NETWORK**.

INTERFACES (T1) > CONFIG > FORMAT

This sets the frame format for the T1 interface. The setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF** or **SF** (D4). Extended Superframe (**ESF**) provides a non-disruptive means of full-time monitoring on the facility datalink (FDL). Default is **ESF**.

INTERFACES (T1) > CONFIG > LINE CODE

This sets the line code for the T1 interface. The setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) and **AMI** (alternate mark inversion). Default is **B8ZS**.

INTERFACES (T1) > CONFIG > EQUALIZATION

Select the line build out for the T1 interface. These are attenuation settings. 0 dB is the strongest signal, and the other settings make the T1 transmit signal weaker. The setting of this field depends on whether the circuit is provisioned for DS1 by the telephone company. The choices are **0 dB**, **-7.5 dB**, **-15 dB**, **-22 dB**. Default is **0 dB**.

INTERFACES (T1) > CONFIG > CSU LPBK

Configures the Total Access 6XX to respond (**ENABLE**) or not respond (**DISABLE**) to a received ANSI Inband CSU loopback pattern. **DISABLE ALL** configures the Total Access 6XX to disregard ALL loopback commands sent inband or over the FDL. Default is **ENABLE**.

INTERFACES (T1) > CONFIG > RX SENSITIVITY

Configures the sensitivity of the T1 receiver for this interface to provide increased sensitivity for long-run T1 applications. Choices are **AUTO** (default), **-36 dB**, and **-10 dB**.

INTERFACES (T1) > STATUS

Displays the T1 status including performance data and alarm histories.

INTERFACES (T1) > STATUS > PERFORMANCE

Displays the T1 performance data.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS

Provides current (15-minute window) status on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for each of the T1 ports as well as historical statistical totals.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > INTERVAL

Identifies the interval (**CURRENT** or **TOTAL**) for the listed performance statistics.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > ES

ES (Errored Second) - For ESF mode, an errored second is defined as a second with one or more Path Code Violations (PCVs), or one or more Out of Frame (OOF) defects, or one or more Controlled Slip events, or a detected AIS (blue alarm) defect. For D4 (SF) mode, the presence of Bipolar Violations (BPVs) also triggers an errored second.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SES

SES (Severely Errored Second) - For ESF mode, an **SES** is a second with 320 or more PCVs, or one or more OOF defects, or a detected AIS defect. For D4 (SF) mode, an **SES** is a second with one or more Framing Error events, or an OOF defect, or at least 1544 Line Code Violations or more.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SEF

SEF (Severely Errored Frame) - An **SEF** condition occurs when 2 out of 6 consecutive frame bits are in error.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > FS

FS (Frame Slip) - A frame slip is defined as one or more frame bit errors in a one-second interval.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > LCV

LCV (Line Code Violation) - A Line Code Violation is defined as a Bipolar Violation (BPV), not including the B8ZS code word if B8ZS is employed. The number displayed is **LCV** events, which is defined as one or more BPVs in a one-second interval.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SLP

SLP (Slip Error Event) - This occurs when a received frame is either repeated or deleted. A **SLP** error indicates a timing problem.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > UAS

UAS (Unavailable Seconds) - When 10 consecutive **SES**s have been logged, the unit is declared in an unavailable state, the 10 **SES**s are cleared, and the Unavailable Seconds count begins to increment starting with 10. The unavailable state is cleared when 10 consecutive non-SES seconds have occurred.

INTERFACES (T1) > STATUS > PERFORMANCE > EXTENDED

Provides statistics for the last 24 hours (in 15 minute windows) on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for each of the T1 ports. Refer to the **CURRENT AND TOTALS** performance information for more details on listed statistics.

INTERFACES (T1) > STATUS > PERFORMANCE > CLEAR CURRENT DATA

Clears all statistics collected in the **CURRENT AND TOTALS** statistics table.

INTERFACES (T1) > STATUS > PERFORMANCE > CLEAR ALL DATA

Clears all statistics collected in the **CURRENT AND TOTALS** and the **EXTENDED** 24 hour statistics tables.

INTERFACES (T1) > STATUS > ALARMS

Displays current alarms and alarm history for T1 interface.

INTERFACES (T1) > STATUS > ALARMS > CURRENT ALARMS

Displays the current alarms on the T1 interface. An asterisk in a field indicates that an alarm is active.

LOS	Loss of Signal. No signal detected on port interface.
RED	Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF). RED alarm most frequently occurs when there is a framing mismatch on the T1 interface.
YELLOW	Remote alarm indicator (RAI) being received on port. A YELLOW alarm indicates that the remote unit is not receiving properly framed information from your unit.
BLUE	Receiving unframed all ones from the port alarm indicator signal (AIS). A BLUE alarm is sent to notify the unit that equipment upstream is disconnected or malfunctioning.

INTERFACES (T1) > STATUS > ALARMS > ALARM HISTORY

Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history. Refer to *Interfaces (T1) > Status > Alarms > Current Alarms* for more details on listed alarm conditions.

INTERFACES (T1) > STATUS > ALARMS > CLEAR HISTORY

Selecting this activator will clear the Alarm History for the T1 interface.

INTERFACES (T1) > STATUS > RX LEVEL

Displays the level (in dB) of the received T1 signal on the interface.

INTERFACES (T1) > TEST

These options are used to initiate local and remote loopback tests and display the test status.

INTERFACES (T1) > TEST > LOC LB

Loopback of the local unit. Choices are **NONE**, **LINE**, and **PAYLOAD**. **LINE** loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **LINE** loopbacks tests right up to the T1 interface of the ADTRAN unit. **PAYLOAD** loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **PAYLOAD** loopbacks not only verify the T1 circuit, but also the internal hardware of the local ADTRAN device. **NONE** disables the loopback test. Default is **NONE**.

INTERFACES (T1) > TEST > REM LB

Sends a loopback command across the network to a remote unit over the FDL, which causes the remote unit initiate a local **LINE** or **PAYLOAD** loopback (whichever is specified). The remote loopback is only available when the T1 is configured for ESF mode.

INTERFACES (T1) > TEST > TEST STATUS

Indicates whether a test is in progress.

INTERFACES (NETWORK SHDSL)

View the network SHDSL interface status and configure SHDSL parameters from this menu. These menus are only applicable to SHDSL Total Access 600 Series systems.

INTERFACES (SHDSL) > CONFIG

Configure the various SHDSL parameters.

INTERFACES (SHDSL) > CONFIG > NTU/LTU MODE

Choices are **NTU** (Network Terminating Unit) or **LTU** (Line Terminating Unit). Select **NTU** when the unit is connected to the SHDSL network device. Select **LTU** when the unit is expected to function as the SHDSL network device. In back-to-back applications, one unit must be set to **NTU** and the other for **LTU**.

INTERFACES (SHDSL) > CONFIG > ANNEX = A/B

Configures the G.shdsl signaling method as either **ANNEX A** or **ANNEX B**. Total Access 600 Series units also support an auto detection signaling method (**ANNEX A&B**) which allows the unit to detect the signaling method on the link and signal accordingly.

INTERFACES (SHDSL) > CONFIG > ITU-T/GSPAN V1.2

Configures the G.shdsl signaling as either standard **ITU-T** or **GLOBESPAN V1.2**.

INTERFACES (SHDSL) > CONFIG > RADSL (AUTO/FIXED)

Configures the SHDSL interface to be either variable rate speeds (**AUTO**) or a fixed rate (**FIXED**). If the system is configured for a fixed rate, the link will only train at the specified rate. The DSLAM setting must match the configured rate when using fixed rates.

INTERFACES (SHDSL) > STATUS

Displays the SHDSL interface status including configuration modes and data rates.

INTERFACES (SHDSL) > STATUS > TRAINING STATE

Indicates the current training state for the SHDSL interface as either trained, currently training, etc.

INTERFACES (SHDSL) > STATUS > NTU/LTU MODE

Displays the current configured mode of operation on the SHDSL link as either NTU or LTU.

INTERFACES (SHDSL) > STATUS > DATA RATE

Displays the negotiated data rate on the SHDSL link.

INTERFACES (SHDSL) > STATUS > FRAME MODE

Displays the framing of the SHDSL link as either framed or unframed.

INTERFACES (SHDSL) > STATUS > G.HS EVENT

Internal ADTRAN use only.

INTERFACES (SHDSL) > STATUS > G.HS STATE

Internal ADTRAN use only.

INTERFACES (SHDSL) > STATUS > ANNEX

Displays the current G.shdsl signaling method as either **ANNEX A** or **ANNEX B**.

INTERFACES (SHDSL) > STATUS > EOC STATS

Displays statistics for information transferred between the Total Access 6XX and the DSLAM over the EOC.

INTERFACES (SHDSL) > STATUS > PERFORMANCE

Displays the current layer one SHDSL information including signal to noise ratio (SNR), errored seconds (ES), severely errored seconds (SES), unavailable seconds (UAS), and code violations.

INTERFACES (NETWORK SDSL)

View the network SDSL interface status and configure SDSL parameters from this menu. These menus are only applicable to SDSL Total Access 600 Series systems.

INTERFACES (SDSL) > CONFIG

Configure the various SDSL parameters from this menu (such as DSLAM type).

INTERFACES (SDSL) > CONFIG > DSLAM

Specify the type of DSLAM the Total Access 6XX SDSL unit is connected to. Choices include: **NOKIA D50**, **LUCENT STINGER**, and **COPPER MOUNTAIN CE150**. DSLAM setup parameters will vary depending on configured DSLAM type.

INTERFACES (SDSL) > CONFIG > DSLAM SETUP

Configure the DSLAM settings from this menu.

INTERFACES (SDSL) > CONFIG > DSLAM SETUP > TRAINING

Specifies the training method for the SDSL link as either **FIXED RATE** (using only the specified rate) or **FAST EOC** (which allows for the fastest negotiated rate).

INTERFACES (SDSL) > CONFIG > DSLAM SETUP > BIT RATE

Configures the fixed data rate used when training the SDSL link. This menu only applies when the Training parameter is specified for **FIXED RATE**. Using a fixed data rate requires the DSLAM to be configured for the same rate as the Total Access 6XX. Choices vary depending on configured DSLAM and range from **144K** to **2320K**.

INTERFACES (SDSL) > STATUS

Displays the SDSL interface status information.

INTERFACES (SDSL) > STATUS > SDSL RATE

Displays the current negotiated SDSL data rate.

INTERFACES (NETWORK ADSL)

View the network ADSL interface status and configure ADSL parameters from this menu. These menus are only applicable to ADSL Total Access 600 Series systems.

INTERFACES (ADSL) > CONFIG

Configure the ADSL parameters from this menu.

INTERFACES (ADSL) > CONFIG > TX ATTEN

Specifies the attenuation required for the ADSL link from **0 dB** to **12 dB**.

INTERFACES (ADSL) > CONFIG > RETRAIN

Forces the Total Access 6XX to retrain the ADSL link.

INTERFACES (ADSL) > STATUS

Displays the ADSL interface status information.

INTERFACES (ADSL) > STATUS > RX RATE

Displays the current receive data rate on the ADSL link.

INTERFACES (ADSL) > STATUS > TX RATE

Displays the current transmit data rate on the ADSL link.

INTERFACES (ADSL) > STATUS > RX LATENCY

Displays the current receive latency on the ADSL link.

INTERFACES (ADSL) > STATUS > TX LATENCY

Displays the current transmit latency on the ADSL link.

INTERFACES (ADSL) > STATUS > SNR (dB)

Displays the current signal to noise ratio on the ADSL link in decibels.

INTERFACES (DSX)

View the integrated DSX interface status and configure T1 parameters from this menu.

INTERFACES (DSX) > CONFIG

Configure the various DSX parameters and enable/disable loopbacks from this menu.

INTERFACES (DSX) > CONFIG > FORMAT

This sets the frame format for the DSX interface. The setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF**, **SF** (D4). Extended Superframe (**ESF**) provides a non-disruptive means of full-time monitoring on the facility datalink (FDL). Default is **ESF**.

INTERFACES (DSX) > CONFIG > LINE CODE

This sets the line code for the DSX interface. The setting must match the line code of the circuit to which the interface is connected. Choices are **B8ZS** (bipolar with 8-zero substitution) and **AMI** (alternate mark inversion). Default is **B8ZS**.

INTERFACES (DSX) > CONFIG > EQUALIZATION

Select the line build out for the DSX1 interface. The choices are **0 dB, 266 FT, 399 FT, 533 FT, 655 FT,** or **-7.5 dB**. Default is **0 dB**. The **7.5 dB** setting is provided for terminal equipment that has trouble recovering a full 0dB level signal (typically one with a DS1 long haul line interface).

INTERFACES (DSX) > CONFIG > CSU LPBK

Configures the Total Access 6XX to respond (**ENABLE**) or not respond (**DISABLE**) to a received ANSI Inband CSU loopback pattern. **DISABLE ALL** configures the Total Access 6XX to disregard ALL loopback commands sent inband or over the FDL. Default is **ENABLE**.

INTERFACES (DSX) > CONFIG > RX SENSITIVITY

Configures the sensitivity of the T1 receiver for this interface to provide increased sensitivity for long-run T1 applications. Choices are **AUTO**, **-36 dB**, and **-10 dB**.

INTERFACES (DSX) > STATUS

Displays the T1 status including performance data and alarm histories.

INTERFACES (DSX) > STATUS > PERFORMANCE

Displays the T1 performance data.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS

Provides current (15-minute window) status on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 as well as historical statistical totals for the integrated DSX port.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > INTERVAL

Identifies the interval (**CURRENT** or **TOTAL**) for the listed performance statistics.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > ES

ES (Errored Second) - For ESF mode, an errored second is defined as a second with one or more Path Code Violations (PCVs), or one or more Out of Frame (OOF) defects, or one or more Controlled Slip events, or a detected AIS (blue alarm) defect. For D4 (SF) mode, the presence of Bipolar Violations (BPVs) also triggers an errored second.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SES

SES (Severely Errored Second) - For ESF mode, an **SES** is a second with 320 or more PCVs, or one or more OOF defects, or a detected AIS defect. For D4 (SF) mode, an **SES** is a second with one or more Framing Error events, or an OOF defect, or at least 1544 Line Code Violations or more.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SEF

SEF (Severely Errored Frame) - An **SEF** condition occurs when 2 out of 6 consecutive frame bits are in error.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > FS

FS (Frame Slip) - A frame slip is defined as one or more frame bit errors in a one-second interval.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > LCV

LCV (Line Code Violation) - A Line Code Violation is defined as a Bipolar Violation (BPV), not including the B8ZS code word if B8ZS is employed. The number displayed is **LCV** events, which is defined as one or more BPVs in a one-second interval.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SLP

SLP (Slip Error Event) - This occurs when a received frame is either repeated or deleted. A **SLP** error indicates a timing problem.

INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > UAS

UAS (Unavailable Seconds) - When 10 consecutive **SES**s have been logged, the unit is declared in an unavailable state, the 10 **SES**s are cleared, and the Unavailable Seconds count begins to increment starting with 10. The unavailable state is cleared when 10 consecutive non-SES seconds have occurred.

INTERFACES (DSX) > STATUS > PERFORMANCE > EXTENDED

Provides statistics for the last 24 hours (in 15 minute windows) on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for each of the T1 ports. Refer to the **CURRENT AND TOTALS** performance information for more details on listed statistics.

INTERFACES (DSX) > STATUS > PERFORMANCE > CLEAR CURRENT DATA

Clears all statistics collected in the **CURRENT AND TOTALS** statistics table.

INTERFACES (DSX) > STATUS > PERFORMANCE > CLEAR ALL DATA

Clears all statistics collected in the **CURRENT AND TOTALS** and the **EXTENDED** 24 hour statistics tables.

INTERFACES (DSX) > STATUS > ALARMS

Displays current alarms and alarm history for the integrated DSX interface.

INTERFACES (DSX) > STATUS > ALARMS > CURRENT ALARMS

Displays the current alarms on the DSX interface. An asterisk in a field indicates that an alarm is active.

LOS	Loss of Signal. No signal detected on port interface.
RED	Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF). RED alarm most frequently occurs when there is a framing mismatch on the T1 interface. RED alarm is also registered when the interface in in LOS.
YELLOW	Remote alarm indicator (RAI) being received on port. A YELLOW alarm indicates that the remote unit is not receiving properly framed information from your unit.
BLUE	Receiving unframed all ones from the port alarm indicator signal (AIS). A BLUE alarm is sent to notify the unit that equipment upstream is disconnected or malfunctioning.

INTERFACES (DSX) > STATUS > ALARMS > ALARM HISTORY

Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history. Refer to *Interfaces (DSX) > Status > Alarms > Current Alarms* for more details on listed alarm conditions.

INTERFACES (DSX) > STATUS > ALARMS > CLEAR HISTORY

Selecting this activator will clear the Alarm History for the integrated DSX interface.

INTERFACES (DSX) > STATUS > RX LEVEL

Displays the level (in dB) of the received T1 signal on the DSX interface.

INTERFACES (DSX) > TEST

These options are used to initiate local and remote loopback tests and display the test status.

INTERFACES (DSX) > TEST > LOC LB

Loopback of the local unit. Choices are **NONE**, **LINE**, and **PAYLOAD**. **LINE** loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **LINE** loopbacks tests right up to the T1 interface of the ADTRAN unit. **PAYLOAD** loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **PAYLOAD** loopbacks not only verify the T1 circuit, but also the internal hardware of the local ADTRAN device. **NONE** disables the loopback test. Default is **NONE**.

INTERFACES (DSX) > TEST > REM LB

Sends a loopback command across the network to a remote unit over the FDL, which causes the remote unit initiate a local **LINE** or **PAYLOAD** loopback (whichever is specified). The remote loopback is only available when the T1 is configured for ESF mode.

INTERFACES (DSX) > TEST > TEST STATUS

Indicates whether a test is in progress.

INTERFACES (ETH)

View the Ethernet interface status and configure the Ethernet parameters from this menu.

INTERFACES (ETH) > CONFIG

Configure the various Ethernet parameters from this menu.

INTERFACES (ETH) > CONFIG > AUTO NEGOTIATION

The Total Access 600 Series has the capability of auto negotiating the rate and duplex of the connected Ethernet link. Additionally, when this parameter is set to **OFF**, the rate and duplex are set manually.

INTERFACES (ETH) > CONFIG > DATE RATE

Defines the Ethernet interface as **100BASET** or **10BASET**. **DATA RATE** configuration is only available when **AUTO NEGOTIATION** is set to **OFF**.

INTERFACES (ETH) > CONFIG > DUPLEX TYPE

Defines operation on the Ethernet interface as **FULL DUPLEX** or **HALF DUPLEX**. **DUPLEX TYPE** configuration is only available when **AUTO NEGOTIATION** is set to **OFF**.

INTERFACES (ETH) > STATUS

Displays the Ethernet status information.

INTERFACES (ETH) > STATUS > MAC ADDRESS

(Read only) Displays the unique MAC address programmed at ADTRAN.

INTERFACES (ETH) > STATUS > DATA LINK

Displays the current status of the Ethernet link as either **UP** or **DOWN**. If there is an active Ethernet link, the status displays **UP**.

INTERFACES (V35)

View the V.35 interface status and configure the V.35 parameters from this menu.

INTERFACES (V35) > CONFIG

Configure the DTE leads from this menu.

INTERFACES (V35) > CONFIG > CTS

Sets the control characteristic of the clear-to-send lead. Choices are **NORMAL** (follows RTS) or **FORCE ON.** Default is **NORMAL.**

INTERFACES (V35) > CONFIG > DCD

Sets the control characteristic of the carrier detect lead. Choices are **NORMAL** (follows valid signal on the network interface) or **FORCE ON.** Default is **NORMAL.**

INTERFACES (V35) > CONFIG > DSR

Sets the control characteristic of the data set ready lead. Choices are **NORMAL** (follows DTR) or **FORCE ON**. Default is **NORMAL.**

INTERFACES (V35) > STATUS

View the status of the DTE leads from this menu.

INTERFACES (V35) > STATUS > RTS

View the status of Request to Send (RTS) lead. Possibilities are **OFF** or **ON**.

INTERFACES (V35) > STATUS > DTR

View the status of the Data Terminal Read (DTR) lead. Possibilities are **OFF** and **ON**.

INTERFACES (V35) > TEST

These options are used to loopback tests.

INTERFACES (V35) > TEST > LOOPBACK

Enables a local loopback of the V.35 interface. All data received on the V.35 interface is transmitted back out the interface.

INTERFACES (FXS)

View the FXS interface status and configure the FXS parameters from this menu.

INTERFACES (FXS) > CONFIG

Configure the FXS mode, line impedance and Tandem parameters from this menu.

INTERFACES (FXS) > CONFIG > PORT

Indicates the port of the FXS module.

INTERFACES (FXS) > CONFIG > MODE

Choices are given below. Default is **LOOP START.**

> NOTE *This mode must match the network configuration and/or how each port is being used. Each port on the FXS Module is independent and should be set accordingly.*

LOOP START	Sets the port to use FXS loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.
GROUND START	Sets the port to use FXS ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.
TR08 SINGLE	Sets the port to use Single Party Channel Unit signaling on the T-span (as defined by TR-TSY-000008) and loop start supervision on the analog 2-wire interface.Only available when using a T1 network interface.
TR08 UVG	Sets the port to use Universal Voice Grade signaling on the T-span (as defined by TR-TSY-000008) and either loop start or ground start supervision on the analog 2-wire interface. Only available when using a T1 network interface.
DPO	Sets the port to use Dial Pulse signaling to originate dialed numbers. Only available when using a T1 network interface.
TANDEM (E&M)	Sets the port to use E&M signaling on the T-span and either loop start or ground start supervision on the analog 2-wire interface. See the **TANDEM** submenus for more information. Only available when using a T1 network interface.

INTERFACES (FXS) > CONFIG > TX (dB)

Sets the TX direction level points. This signal will change the volume of the voice. TX (dB) is the signal that is transmitted out the T1, with 0 dB being the strongest. If the volume is too loud across the T1, this number should be increased. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **6.0 dB**.

INTERFACES (FXS) > CONFIG > RX (dB)

Sets the RX direction level points. This signal will change the volume of the voice. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **3.0 dB**. The maximum signal is **0.0 dB**.

INTERFACES (FXS) > CONFIG > SVC MODE

Indicates whether the module is **IN SERVICE** or **OUT OF SVC**. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 MAPS** menu. Default is **IN SERVICE.**

INTERFACES (FXS) > CONFIG > LINE Z

Sets the line impedance. Choices are **600 OHMS, 900 OHMS, 600 OHMS + 2.16µF, 900 OHMS + 2.16µF,** and **AUTO**. The line impedance of each port is based on the size of the network. Default is **600 OHMS**.

INTERFACES (FXS) > CONFIG > MSG IND

This is better referred to as On-Hook Message Waiting. When this is set to **ENABLE,** talk path is always open, even in On-Hook conditions, in order for these FSK message tones to pass through. Default is **DISABLE**. Enabling on-hook message waiting will allow message lamp usage but will cause a lower on-hook voltage. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID.

INTERFACES (FXS) > CONFIG > BATT MODE

Configures the on-hook battery voltage. For most IAD installs, the FXS loop is short with 6 to 7 V present on tip / ring. To reduce power dissipated during off-hook conditions, the battery is lowered for short loop lengths. When set to **AUTO SWITCH**, the IAD uses a higher on-hook battery voltage (48-52 V). When off-hook, it automatically switches to low battery (24-26 V) to minimize power dissipation. When set to **LOW BATTERY** mode, the higher battery is not used and the voltage is a constant 26 V even while on-hook. The tip/ring voltage is reduced to 26 V when using the **LOW BATTERY** mode.

INTERFACES (FXS) > CONFIG > FWD DISC TIMER

Specifies the interval of battery removal during a forward disconnect state. Choices are **FOLLOW SWITCH** (default), **500MS**, **750MS**, **1000MS**, and **2000MS**.   When using ATM mode, there is an additional choice of **IGNORE SWITCH**. If the timer is set to **FOLLOW SWITCH**, the Total Access 6XX will follow the switch at all times; this is normal operation. If a time period has been selected, the Total Access 6XX will remove battery for the specified time period OR as long as the switch requests battery removal, whichever is longer. For example, if the timer expires but the switch continues to request battery removal, the Total Access 6XX will follow the switch and continue to remove battery. For ATM mode, if the timer is set to **IGNORE SWITCH**, the IAD will never remove battery.

INTERFACES (FXS) > CONFIG > TANDEM

Sets the port to use E&M signaling on the T-Span and either loop start or ground start supervision on the analog 2-wire interface. To access submenus for this item, use the arrow keys to scroll to the **TANDEM** column for the corresponding module, and then press **<ENTER>**.

INTERFACES (FXS) > CONFIG > TANDEM > CONVERSION MODE

Sets the port to either **LOOP START** or **GROUND START** mode. Default is **LOOP START**.

INTERFACES (FXS) > CONFIG > TANDEM > SUPERVISION

Sets the supervision method used to either **IMMEDIATE** or **WINK**. Default is **IMMEDIATE**.

INTERFACES (FXS) > CONFIG > TANDEM > DIAL TONE

Used to enable or disable the on-board dial tone generation. Dial Tone is supplied for 5 sec; then it drops. It cannot be broken when dialing digits. Default is **DISABLE**.

INTERFACES (FXS) > CONFIG > TANDEM > RING BACK TONE

Used to enable or disable the option of generating ring back tone towards the T-span. Default is **DISABLE**.

INTERFACES (FXS) > CONFIG > TANDEM ANSWER SUPERVISION

Causes the polarity of tip and ring to be reversed when the far-end answers. Can be **ENABLED** or **DISABLED**. Default is **DISABLE**.

INTERFACES (FXS) > CONFIG > TANDEM > DNIS OPTIONS

This parameter is used in conjunction with **DNIS DELAY**. Choices are **DISABLE**, **ENABLE**, and **ENABLE W/ NO ANSWER WINK**. Default is **DISABLE**.

INTERFACES (FXS) > CONFIG > TANDEM > DNIS DELAY

Sets the amount of time the voice module waits after it receives a wink before forwarding a DNIS digit if **DNIS OPTIONS** is set to **ENABLE**. Choices are **0.5 SEC**, **1.0 SEC**, **2.0 SEC**, **2.5 SEC**, **3.0 SEC**, and **5.0 SEC**. Default is **3.0 SEC**.

INTERFACES (FXS) > CONFIG > TANDEM > FWD DISC DELAY

In Tandem mode, **FWD DISC DELAY** defines the time battery is actually removed/reversed once the forward disconnect is received. Choices are **250 MSEC**, **500 MSEC**, **750 MSEC**, **1 SEC**, and **2 SEC**. Default is **1 SEC**.

INTERFACES (FXS) > CONFIG > TANDEM > FWD DISC BATTERY

In Tandem mode, selects whether battery is to be removed or reversed during forward disconnect. Choices are **REMOVE** and **REVERSE**. Default is **REMOVE**.

INTERFACES (FXS) > STATUS

Displays the status of the FXS signal bits.

INTERFACES (FXS) > STATUS > PORT

Displays the port number.

INTERFACES (FXS) > STATUS > TA SIG

This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXS) > STATUS > TB SIG

This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXS) > STATUS > RA SIG

This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXS) > STATUS > RB SIG

This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXS) > TEST

Activate tests and monitor test status on a per port basis from this menu.

INTERFACES (FXS) > TEST > PORT

Displays the port number.

INTERFACES (FXS) > TEST > TEST

Choices are given below. Default is **NONE**.

NONE	Indicates that no test is currently active.
DIGITAL NETWORK LPBK	Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit's transmit time slot.
NETWORK ON HOOK TEST	Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.
NETWORK OFF HOOK TEST	Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced off-hook while this test is active.
CUSTOMER RING TEST	The customer ring test will activate the unit's ring relay in a 2-on /4-off cadence, providing ringing to the customer loop.

INTERFACES (FXS) > TEST > TEST STATUS

This option indicates whether a test is in progress.

INTERFACES (FXO)

View the FXO interface status and configure the FXO parameters from this menu.

> **NOTE** *FXO interfaces are only available with Total Access 624 systems.*

INTERFACES (FXO) > CONFIG

Configure the FXO mode, line impedance, and Tandem parameters from this menu.

INTERFACES (FXO) > CONFIG > PORT

Indicates the port of the FXO module.

INTERFACES (FXO) > CONFIG > MODE

Choices are given below. Default is **LOOP START.**

> **NOTE** *This mode must match the network configuration and/or how each port is being used. Each port on the FXO Module is independent and should be set accordingly.*

LOOP START	Sets the port to use FXO loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.
GROUND START	Sets the port to use FXO ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.
DPT	Sets the port to use Dial Pulse signaling to terminate dialed numbers.
MODIFIED DPT	Sets the port to use DPT signaling on the interface. In DPT mode, digits are transmitted out the FXO interface to the user equipment. DPT mode is one-way operation for outbound calls towards user equipment on the 2-wire side.

INTERFACES (FXO) > CONFIG > TX (dB)

Sets the TX direction level points. This signal will change the volume of the voice. TX (dB) is the signal that is transmitted out the T1, with 0 dB being the strongest. If the volume is too loud across the T1, this number should be increased. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **0.0 dB**.

INTERFACES (FXO) > CONFIG > RX (dB)

Sets the RX direction level points. This signal will change the volume of the voice for the signal being transmitted by the Total Access 6XX out the interface. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **0.0 dB**.

INTERFACES (FXO) > CONFIG > SVC MODE

Indicates whether the module is **IN SERVICE** or **OUT OF SVC**. This does not indicate whether the port has been mapped.

INTERFACES (FXO) > STATUS

Displays the status of the FXO signal bits.

INTERFACES (FXO) > STATUS > PORT

Displays the port number.

INTERFACES (FXO) > STATUS > TA SIG

This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXO) > STATUS > TB SIG

This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXO) > STATUS > RA SIG

This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXO) > STATUS > RB SIG

This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXO) > TEST

Activate tests and monitor test status on a per port basis from this menu.

INTERFACES (FXO) > TEST > PORT

Displays the port number.

INTERFACES (FXO) > TEST > TEST

Choices are given below. Default is **NONE**.

NONE	Indicates that no test is currently active.
DIGITAL NETWORK LPBK	Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit's transmit time slot.
NETWORK ON HOOK TEST	Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.
NETWORK OFF HOOK TEST	Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced off-hook while this test is active.

INTERFACES (FXO) > TEST > TEST STATUS

This option indicates whether a test is in progress.

L2 PROTOCOL (TDM FIRMWARE)

Use the L2 protocol menu to select the L2 protocol, configure the protocol specific parameters and view the status as shown in Figure 7. The following menus are for Total Access 600 Series systems using TDM firmware.
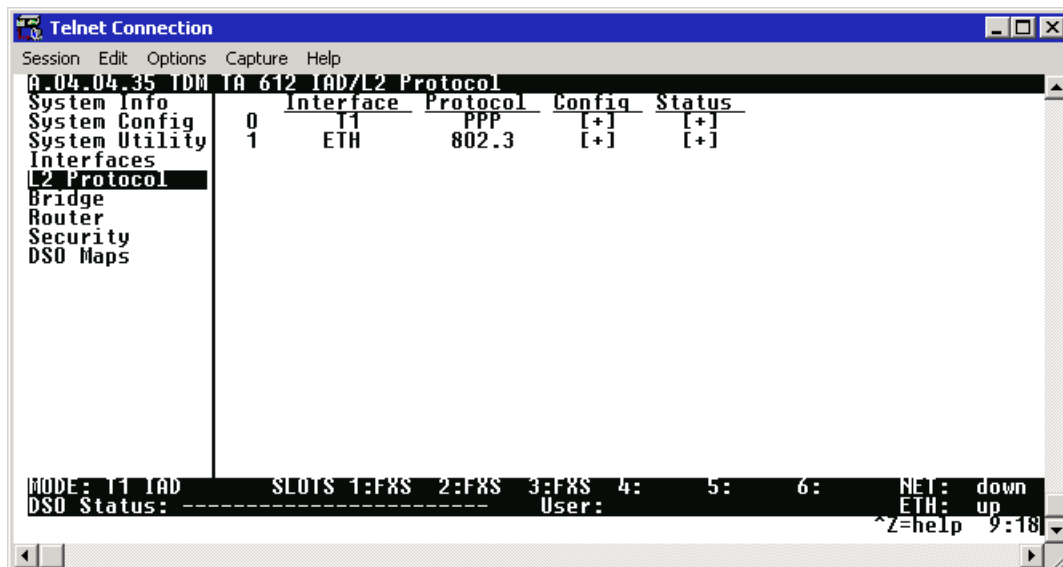
Figure 7. L2 Protocol (T1 TDM) Menu

For convenience, the following heading notations identify the type of firmware and L2 protocol configured in the Total Access 600 Series system:

L2 Protocol (TDM – T1 – PPP)

Firmware type. (For example, TDM or ATM.)

Interface type. (For example, T1, Ethernet, V.35, etc.)

Configured Layer 2 protocol. (For example, PPP, FRE, Auto, etc.)
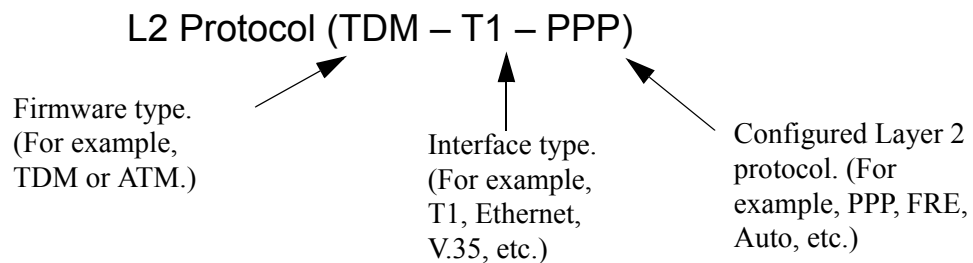
L2 PROTOCOL (TDM FIRMWARE) – T1 INTERFACE

Configure the L2 Protocol parameters and view the status of the Network T1 interface using items from this menu.

L2 PROTOCOL (TDM – T1) > PROTOCOL

Configure the L2 protocol mode. Choices are **PPP**, **FRE**, **HDLC**, and **AUTO** (def). Selecting **PPP** configures the interface for Point-to-Point Protocol signaling on Layer 2. Selecting **FRE** configures the interface for frame relay signaling on Layer 2. Selecting **HDLC** configures the interface for generic High-Level Data Link Control signaling on Layer 2. Selecting **AUTO** enables the Auto-config feature.

L2 PROTOCOL (TDM – T1) > PROTOCOL > PPP

Point-to-Point Protocol (PPP) is an 8-bit serial protocol which allows a PC to connect as a TCP/IP host to a network through an asynchronous port. PPP is used for connection from a PC to an Internet Service Provider (ISP) for Internet access. PPP works over synchronous and asynchronous circuits. Router-to-router and host-to-network connections can be made via PPP. PPP includes error detections which Serial Line Internet Protocol (SLIP) and other protocols do not.

L2 PROTOCOL (TDM – T1) > PROTOCOL > FRE

Frame Relay is a switched data link layer protocol that handles multiple virtual circuits using High-Level Data Link Control (HDLC) encapsulation. Frame Relay uses statistical multiplexing as opposed to time-division-multiplexing to multiplex many logical connections over a single physical link. It contains a cyclical redundancy check (CRC) for detecting bad data, but leaves the error correction algorithms to be performed by higher protocol layers. Similarly, Frame Relay uses simple congestion notification. This notification in turn can alert higher-layer protocols to exercise flow control. These characteristics allow Frame Relay to provide a more flexible and efficient use of bandwidth.

L2 PROTOCOL (TDM – T1) > PROTOCOL > HDLC

HDLC (High-level Data Link Control) is a group of protocols or rules for transmitting data between two network points (point-to-point transmission). HDLC provides a low overhead system for transmitting data over Layer 2. IP packets are encapsulated into frames with an HDLC start and end flag. Generic HDLC protocol should be used when connecting with remote equipment using proprietary HDLC encapsulation methods.

L2 PROTOCOL (TDM – T1) > PROTOCOL > AUTO

Setting the **L2 PROTOCOL** to **AUTO** allows the unit to automatically detect the **L2 PROTOCOL** from the network.

> **NOTE**   *The **L2 PROTOCOL** must be set to **AUTO** in order to use the Auto-config feature.*

L2 PROTOCOL (TDM FIRMWARE) – T1 INTERFACE > PPP

Configure the **L2 PROTOCOL** parameters and view the status of the T1 interface using PPP protocol from this menu.

L2 PROTOCOL (T1 TDM–T1–PPP) > CONFIG

Configure the **L2 PROTOCOL** parameters for the T1 interface using PPP protocol.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > MODE

Select the **L2 PROTOCOL** mode. Choices are **ROUTE IP**, **BRIDGE ALL**, and **ROUTE IP/BRIDGE OTHER**. The default is **ROUTE IP**.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > AUTHENTICATION

The **AUTHENTICATION** menu contains the required parameters for the authentication of the PPP peer and for being authenticated by the PPP peer. Authentication is applied between the unit and the PPP peer as described in the Authentication submenus.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > AUTHENTICATION > TX METHOD

This parameter specifies how the unit is to be authenticated by the PPP peer. There are four possible selections. Default is **NONE**.

NONE	The connection will not allow the PPP peer to authenticate it
PAP, CHAP, OR EAP	The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** or **PAP**.
CHAP OR EAP	The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** but not **PAP**.
EAP ONLY	The unit will only allow EAP to be negotiated. If the PPP peer is not capable of doing EAP, then the connection will not succeed.
PAP ONLY	The unit will only allow **PAP** to be negotiated. If the PPP peer is not capable of doing **PAP**, then the connection will not succeed.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > PPP

Configure the PPP specific parameters such as **MAX CONFIG**, **MAX TIMER**, **MAX FAILURE**, and **FORCE PEER IP ADDRESS** from this menu.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > PPP > MAX CONFIG

This value is the number of unanswered configuration-requests that should be transmitted before resetting PPP negotiations. The possible values are **5**, **10**, **15** and **20** (def).

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > PPP > MAX TIMER (SEC)

This value is the numbers of seconds to wait between unanswered configuration-requests. The possible values are **1 SEC**, **2 SECS**, **3 SECS** (def), **5 SECS** and **10 SECS**.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > PPP > MAX FAILURE

Due to the nature of PPP, configuration options may not be agreed upon between two PPP peers. This value is the number of configuration-naks that should occur before an option is configuration-rejected. The possible values are **5** (def), **10**, **15**, and **20**.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > PPP > KEEPALIVE PERIOD

This option allow the user to generate PPP keepalive packets that can be sent one every 1 minute, 2 minutes or every 5 minutes. A value of 0 (def) disables the PPP keepalive packet generating feature.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > PPP > FORCE PEER IP ADDRESS

This option forces the PPP to negotiate the IP address entered instead of allowing the IP address to be assigned by the remote end.

L2 PROTOCOL (TDM–T1–PPP) > CONFIG > PPP > SEND IDENTIFICATION

When enabled, this option enables the Total Access 600 Series to send the system identification code in response to a configure acknowledgement from the peer equipment. For most peer routers this option should be configured as **YES**. If set to **NO**, the Total Access 600 Series will accommodate peer routers that do not correctly respond to the identification code.

L2 PROTOCOL (TDM–T1–PPP) > STATUS

View the **L2 PROTOCOL** status for the T1 interface using the PPP protocol.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > LCP

Link Control Protocol. Reflects the LCP layer active.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > BCP

Shows **UP** if PPP Bridge Control Protocol has negotiated successfully.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > IPCP

Shows **UP** if PPP IP Control Protocol has negotiated successfully.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > UP TIME

Displays how long the PPP session has been connected.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > TX PKTS

Number of packets transmitted on the T1 interface.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > RX PKTS

Number of packets received on the T1 interface.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > TX BYTES

Number of bytes transmitted on the T1 interface.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > RX BYTES

Number of bytes received on the T1 interface.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > CURRENT UTIL (b/s)

Current utilization of the T1 interface bandwidth presented in bits per second.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > CURRENT UTIL (%)

Current utilization of the T1 interface bandwidth presented in percentage format.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > AVERAGE UTIL (b/s)

Average utilization of the T1 interface bandwidth (since the last stats reset) presented in bits per second.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > AVERAGE UTIL (%)

Average utilization of the T1 interface bandwidth (since the last stats reset) presented in percentage format.

L2 PROTOCOL (TDM–T1–PPP) > STATUS > TX PKTS

Number of packets transmitted on the T1 interface

L2 PROTOCOL (TDM–T1–PPP) > STATUS > CLEAR STATS

Clears the PPP stats (returning the counters to 0) for the T1 interface.

L2 PROTOCOL (TDM FIRMWARE) – T1 INTERFACE > FRE PROTOCOL

Configure the **L2 PROTOCOL** parameters and view the status of the T1 interface using Frame Relay protocol from this menu.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG

Configure the **L2 PROTOCOL** parameters for the T1 interface using the Frame Relay protocol.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > MAINTENANCE PROTOCOL

The Frame Relay maintenance protocol is used on the WAN port. The maintenance protocol is used to send link status and virtual circuit information between Frame Relay switches and other devices (such as routers that communicate with them). Possible choices are as follows:

ANNEX D (ANSI)	(Default) This ANSI standard ANSI T1.617-D and is the most commonly used in the United States.
ANNEX A (Q933A)	This is the CCITT European standard, ITU-T Q.933-A.
LMI	This was developed by a vendor consortium and is also known as the "Consortium" management interface specification. It is still used by some carriers in the United States.
STATIC (NO SIG)	This should be selected when there is no Frame Relay switch in the circuit. The DLCIs are assigned in the DLCI Mapping and must be the same for the device it will communicate with.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > POLLING FREQUENCY (5-30)

This parameter is the interval that the unit polls the Frame Relay switch using the maintenance protocol selected. The unit is required to poll the Frame Relay switch periodically to determine whether the link is active. The value is in seconds and ranges from **5** to **30** seconds with a default of **10 SECONDS**.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > DLCI MAPPING

This menu allows each DLCI to be mapped to a particular Frame Relay maintenance protocol. Each protocol parameter can be individually configured for each DLCI. By factory default, the DLCI map is empty.

When empty and a maintenance protocol other than the static is used, the unit will poll the switch to determine which DLCIs are active. If the Total Access 6XX learns a new DLCI not listed in the DLCI Map, an entry is added for that DLCI in the PVC Status table. The learned DLCIs are listed as **INACTIVE** until the user configures them in the DLCI Map.

> **NOTE** *To insert a new profile, press the **I** key when over the **Num** column. A new inserted profile will always be set up with the default parameters. To copy parameters from an old profile to this newly inserted profile, use the copy (**C**) and paste (**P**) keys. Entire configuration trees can be copied with this method.*

> **NOTE** *To delete an unused profile, use the **D** key when the cursor is over the number in the **Num** column. Once deleted, the profile is gone permanently.*

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > DLCI MAPPING > NUM

Displays the index number in the DLCI mapping table.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > DLCI MAPPING > ACTIVE

The default value is **YES**. If set to **NO**, the unit will ignore the virtual circuit with this DLCI.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > DLCI MAPPING INTERFACE

Shows the user the physical and logical port associated with each DLCI. This is a read-only field.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > DLCI MAPPING > DLCI

This DLCI (Data Link Connection Identifier) number identifies the virtual circuit being configured.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > DLCI MAPPING > MODE

The mode identifies how the data will be forwarded. The choices are:

ROUTE IP (def)	All IP data for this DLCI will be routed.
BRIDGE ALL	All data for this DLCI will be bridged.
ROUTE UIP/BRIDGE OTHER	All IP data will be routed. All other data will be bridged.

L2 PROTOCOL (TDM–T1–FRE) > CONFIG > DLCI MAPPING > BECN TIMEOUT (MSEC)

This value is expressed in milliseconds and represents the amount of time the unit will stop transmitting over a PVC which received a packet with the BECN bit set. Range is **50-5000** msec; the default is **50 MILLLISECONDS**.

L2 PROTOCOL (TDM–T1–FRE) > STATUS

View the L2 protocol status for the T1 interface using the Frame Relay protocol.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT

View the Frame Relay statistics on the WAN port.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > PORT INDEX

Integer used for identifying DLCIs on an interface. A single DLCI will always be port index 0. Subsequent DLCIs will have incrementing port indices.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > SIGNAL STATE

Displays "up" when the unit is communicating with the Frame Relay switch; otherwise displays "down".

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > TX FRAMES

Total frames transmitted out the WAN port.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > RX FRAMES

Total frames received from the WAN port.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > TX BYTES

Total bytes transmitted out the WAN port.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > RX BYTES

Total bytes received on the WAN port.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > CURRENT UTIL (b/s)
Current utilization of the T1 interface bandwidth presented in bits per second.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > CURRENT UTIL (%)
Current utilization of the T1 interface bandwidth presented in percentage format.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > AVERAGE UTIL (b/s)
Average utilization of the T1 interface bandwidth (since the last stats reset) presented in bits per second.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > AVERAGE UTIL (%)
Average utilization of the T1 interface bandwidth (since the last stats reset) presented in percentage format.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > FULL STATUS TX FRAMES
Number of full status frames transmitted out the WAN port.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > FULL STATUS RX FRAMES
Number of full status frames received on the WAN port

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > LINK INTEGRITY STATUS TX FRAMES
Number of Link-Integrity (LI) only frames transmitted out the WAN port.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > LINK INTEGRITY STATUS RX FRAMES
Number of LI only frames received on the WAN port.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > DROP UNKNOWN DLCI
Number of frames received that were not associated with any known PVC.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > DROP INVALID DLCI
Number of frames received that had illegal DLCIs.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PORT > CLEAR STATS
Selecting this activator will clear the port Frame Relay Statistics.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S)
View the Frame Relay status on a per PVC basis.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > DLCI
The DLCI number identifies the virtual circuit being monitored.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > STATE

The state of the virtual circuit:

INACTIVE	The circuit exists but has been deactivated by the Frame Relay switch.
ACTIVE	The circuit is fully active.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > TX FRAMES

Number of Frame Relay packets that have been transmitted via this DLCI.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > RX FRAMES

Number of Frame Relay packets that have been received via this DLCI.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > TX BYTES

Number of Frame Relay bytes that have been transmitted via this DLCI.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > RX BYTES

Number of Frame Relay bytes that have been received via this DLCI.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > DE COUNT

Number of packets received on this DLCI with the Discharge Eligible (DE) bit set.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > CR COUNT

Number of packets received on this DLCI with the Command Response (CR) bit set.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > BECN COUNT

Number of packets received on this DLCI with the Backward Explicit Congestion Notification (BECN) bit set.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > FECN COUNT

Number of packets received on this DLCI with the Forward Explicit Congestion Notification (FECN) bit set.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > UNKNOWN FRAME RX

Number of frames that have been received that the unit does not know where to route.

L2 PROTOCOL (TDM–T1–FRE) > STATUS > PVC(S) > CLEAR STATS

Clears all gathered statistics for this interface and returns counters to 0.

L2 PROTOCOL (TDM FIRMWARE) – T1 INTERFACE > HDLC PROTOCOL

View the status of the T1 interface with the **L2 PROTOCOL** set to **HDLC**.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS

View the status of traffic flow and utilization for the T1 interface with an **L2 PROTOCOL** set to **HDLC**.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > TX PKTS

Number of packets transmitted on the T1 interface.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > RX PKTS

Number of packets received on the T1 interface.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > TX BYTES

Number of bytes transmitted on the T1 interface.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > RX BYTES

Number of bytes received on the T1 interface.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > CURRENT UTIL (b/s)

Current utilization of the T1 interface bandwidth presented in bits per second.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > CURRENT UTIL (%)

Current utilization of the T1 interface bandwidth presented in percentage format.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > AVERAGE UTIL (b/s)

Average utilization of the T1 interface bandwidth (since the last stats reset) presented in bits per second.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > AVERAGE UTIL (%)

Average utilization of the T1 interface bandwidth (since the last stats reset) presented in percentage format.

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > TX PKTS

Number of packets transmitted on the T1 interface

L2 PROTOCOL (TDM–T1–HDLC) > STATUS > CLEAR STATS

Clears all the gathered statistics for this interface and returns the counters to 0.

L2 PROTOCOL (TDM FIRMWARE) – T1 INTERFACE > AUTO PROTOCOL

View the status of the T1 interface with the **L2 PROTOCOL** set to **AUTO** (using Auto-config feature).

L2 PROTOCOL (TDM–T1–AUTO) > STATUS

View the status of the auto detect function and traffic flow for the T1 interface with an **L2 PROTOCOL** set to **AUTO**.

L2 PROTOCOL (TDM–T1–AUTO) > STATUS > STATE

This field represents the state of the auto detect/configuration function. The possible state are:

OFF	The T1 interface is down, so the auto-detect/configuration process is currently idle.
DETECTING L2 PROTOCOL	The T1 interface is up and waiting for the first control/signaling packet.
CONFIRMING FR	The T1 interface is up and one FR signaling packet has been received
CONFIRMED FR	The T1 interface is up and two FR signaling packets have been received. It takes two consecutive control/signaling packets of the same type to confirm the detected protocol.
CONFIRMING PPP	The T1 interface is up and one PPP control packet has been received.
CONFIRMED PPP	The T1 interface is up and two PPP control packets have been received. It takes two consecutive control/signaling packets of the same type to confirm the detected protocol.

L2 PROTOCOL (TDM–T1–AUTO) > STATUS > TX PKTS

Number of packets transmitted out of the WAN port.

L2 PROTOCOL (TDM–T1–AUTO) > STATUS > RX PKTS

Number of packets received on WAN port.

L2 PROTOCOL (TDM–T1–AUTO) > STATUS > TX BYTES

Number of bytes transmitted out of the WAN port.

L2 PROTOCOL (TDM–T1–AUTO) > STATUS > RX BYTES

Number of bytes received out of the WAN port.

L2 PROTOCOL (TDM–T1–AUTO) > STATUS > CLEAR STATS

Clears all the gathered statistics for this interface and returns the counters to 0.

L2 PROTOCOL (ATM FIRMWARE)

Use the **L2 PROTOCOL** menu to select the **L2 PROTOCOL**, configure the protocol specific parameters, and view the status as shown in Figure 7. The following menus are for Total Access 600 Series systems using ATM firmware. All Total Access 600 Series ATM systems have the same L2 Protocol menus regardless of network interface type (T1, ADSL, SDSL, SHDSL).
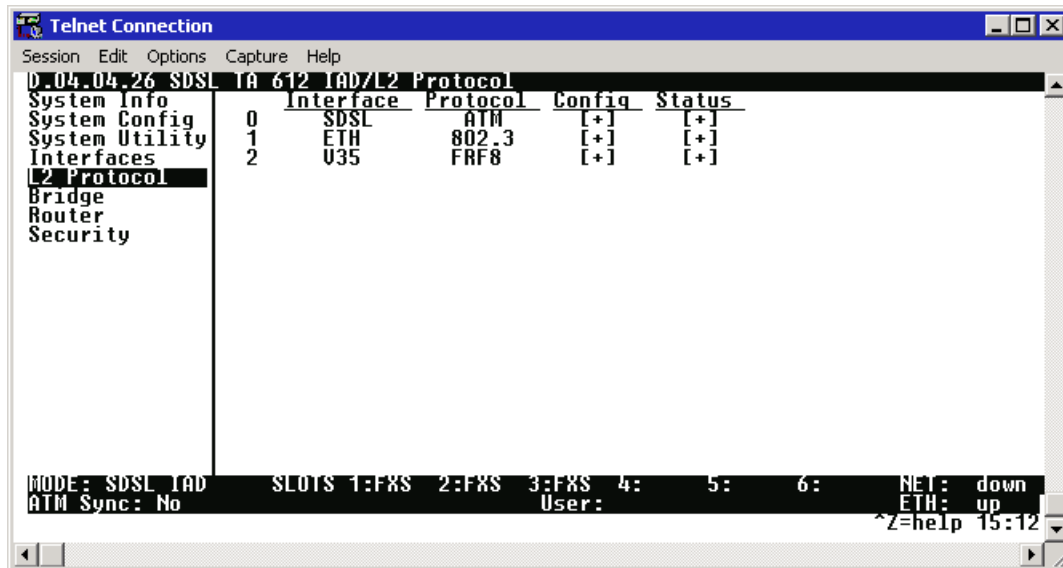
Figure 8. L2 Protocol (SDSL ATM) Menu

For convenience, the following heading notations identify the type of firmware and L2 protocol configured in the Total Access 600 Series system:

L2 Protocol (ATM – NET – ATM)

Firmware type. (For example, TDM or ATM.)

Interface type. (For example, Network (NET), Ethernet, V.35, etc.)

Configured Layer 2 protocol. (For example, ATM or CuMTN.)
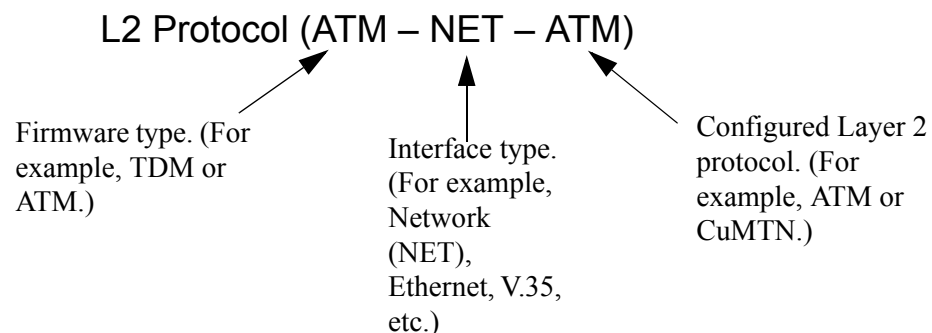
L2 PROTOCOL (ATM FIRMWARE) – NETWORK (NET) INTERFACE

Configure the **L2 PROTOCOL** parameters for these menus are identical regardless of network interface. Therefore, the interface is denoted by **NET**.

L2 PROTOCOL (ATM – NET) > PROTOCOL

Configure the **L2 PROTOCOL** mode. Choices are **ATM** and **CUMTN** (def). Selecting **ATM** configures the interface for Asynchronous Transfer Mode signaling on Layer 2. Selecting **CUMTN** configures the interface for Copper Mountain frame relay signaling on Layer 2.

L2 PROTOCOL (ATM – NET) > PROTOCOL > ATM

Asynchronous Transfer Mode allocates bandwidth on demand, automatically adjusting the network capacity to meet the system needs. Fixed-length cells (53 octet) require lower processing overhead and allow higher transmission speeds than traditional packet switching methods. ATM uses five octet headers in each fifty-three octet cell to match cells with specific virtual channels to which they belong.

L2 PROTOCOL (ATM – NET) > PROTOCOL > CUMTN FRE

Copper Mountain Frame Relay (FRE) is a data link layer protocol that uses Frame Relay instead of ATM on the subscriber loop. Frame relay is a switched layer protocol that handles virtual circuits using High-Level Data Link Control (HDLC) encapsulation. Frame Relay uses statistical multiplexing as opposed to time-division-multiplexing many logical connections over a single physical link.

L2 PROTOCOL (ATM FIRMWARE) – NET> ATM

Configure the **L2 PROTOCOL** parameters and view the status of the T1 interface using ATM protocol from this menu.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG

Configure the **L2 PROTOCOL** parameters for the T1 interface using ATM protocol.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > ATM CONFIG

Use the **ATM CONFIG** menu to set the parameters listed below.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > ATM CONFIG > IDLE CELLS

The **IDLE CELLS** format must be configured for either **ATM FORUM (UNASSIGNED)** or **ITU (IDLE)**. Configuring this setting incorrectly for a particular circuit will cause poor performance at the ATM Layer. The default is **ATM FORUM (UNASSIGNED)**.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > ATM CONFIG > DATA SCRAMBLING

DATA SCRAMBLING can be ENABLED or DISABLED for cell traffic. Configuring this setting incorrectly for a particular circuit will cause poor performance at the ATM Layer.

> NOTE *The setting must match the configuration setting of the ATM switch or DSLAM at the other end of the circuit.*

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > ATM CONFIG > HEC COSET

Header Error Control is located in the last (5th) byte of the ATM cell header that checks for cell integrity only. The Coset polynomial is applied to the received HEC for comparison with the HEC generated internally. HEC errors may be detected after synchronization, and any detected bit errors prompt that the cell be dropped. The choice are ENABLED (def) or DISABLED.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG

Configure up to six ATM PVCs from this menu (five data and one voice PVC).

> NOTE *To insert a new PVC, press the I key when over the NUM column. A new inserted PVC will always be set up with the default parameters. To copy parameters from an old PVC to the new PVC, use the copy (C) and paste (P) keys. Entire configuration trees can be copied with this method.*

> NOTE *To delete an unused PVC, use the D key when the cursor is over the number in the NUM column. Once deleted, the PVC is gone permanently.*

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > NUM

Displays the index number for the PVC entry.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > ACTIVE

Activates the ATM PVC. The choices are YES or NO. Default is NO.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > SUB-INTERFACE

This is a read-only field which displays the physical and logical port of the interface using the following nomenclature: [A.B], where A represents the physical port (network interface is 0, Ethernet is 1) and B represents the logical port for the Layer 2 protocol (i.e. PVC for Frame Relay, PPP link, etc.) Each configured logical port is assigned a number corresponding to the order in which they are listed in the L2 Protocol configuration fields.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > VPI

ATM Virtual Path Identifier located in the ATM cell header identifies the virtual path over which this port is running. The range is 0-256. The default is 0.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > VCI

This is the ATM Virtual Channel Identifier that serves as an address for the virtual channel cell transmissions between two devices. The range is **0-65355**. The default setting is **38**.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > CONNECTION

Select the physical and logical method of data transfer over the virtual path. There are three valid connection entries: **ROUTER**, **V35**, and **VOICE**. Select **ROUTER** to connect traffic from this PVC to the Total Access 600 Series integral IP router. Select **V35** to connect traffic from this PVC to a V.35 interface on the system. Select **VOICE** to connect traffic from this PVC to a voice connection (on a DSX-1 or FXS interface).

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > SETUP (ROUTER)

Use these menus to configure the router parameters for this logical connection from the router to the T1 interface. These menus are only applicable when the **CONNECTION** parameter is set to **ROUTER**.

CONNECTION (ROUTER) > SETUP > PROTOCOL

Selects the data-link protocol for the PVC connection between the T1 interface and the router. The choices are: **IP** (def) and **PPP**.

CONNECTION (ROUTER) > SETUP > MODE

Identifies how the data will be transferred through the Total Access 600 Series system. The following choices are available:

ROUTE IP (def) – All IP data for this PVC is routed through the Total Access 600 Series integral router.
BRIDGE ALL – All data for this PVC is bridged through the Total Access 600 Series system.
ROUTE IP/BRIDGE OTHER – All IP data for this PVC is routed through the Total Access 600 Series integral router and all other data is bridged through the system.

CONNECTION (ROUTER) > SETUP > PPP SETUP

Provides PPP configuration parameters for the PVC. These menus are only visible when the **MODE** is set to **PPP**.

AUTHENTICATION

Contains the required parameters for PPP peer authentication and for being authenticated by the PPP peer. Authentication is applied between the unit and the PPP peer as described in the submenus.

TX METHOD

Specifies the method the Total Access 600 Series uses to obtain PPP
authentication from the peer. There are four possible selections:

NONE	The connection will not allow the PPP peer to authenticate it.
PAP, CHAP, OR EAP	The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** or **PAP**.
CHAP OR EAP	The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** but not **PAP**.
EAP ONLY	The unit will only allow **EAP** to be negotiated. If the PPP peer is not capable of doing **EAP**, then the connection will not succeed.
PAP ONLY	The unit will only allow **PAP** to be negotiated. If the PPP peer is not capable of doing **PAP**, then the connection will not succeed.

RX METHOD

Specifies the method the Total Access 600 Series uses to authenticate the PPP
peer. There are four possible selections:

NONE	The connection will not allow the PPP peer to authenticate it.
PAP, CHAP, OR EAP	The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** or **PAP**.
CHAP OR EAP	The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** but not **PAP**.
EAP ONLY	The unit will only allow **EAP** to be negotiated. If the PPP peer is not capable of doing **EAP**, then the connection will not succeed.
PAP ONLY	The unit will only allow **PAP** to be negotiated. If the PPP peer is not capable of doing **PAP**, then the connection will not succeed.

PPP

Configure the PPP specific parameters such as **MAX CONFIG**, **MAX TIMER**, **MAX FAILURE**,
and **FORCE PEER IP ADDRESS** from this menu.

MAX CONFIG

This value is the number of unanswered configuration-requests that should be transmitted before resetting PPP negotiations. the possible values are **5**, **10**, **15**, and **20** (def).

MAX TIMER (SEC)

This value is the number of seconds to wait between unanswered configuration-requests. The possible values are **1 SEC**, **2 SECS**, **3 SECS (DEF)**, **5 SECS**, and **10 SECS**.

MAX FAILURE

Due to the nature of PPP, configuration option may not be agreed upon between two PPP peers. This value is the number of configuration-naks that should occur before an option is configuration-rejected. The possible values are **5 (DEF)**, **10**, **15**, and **20**.

FORCE PEER IP ADDRESS

This option forces the PPP to negotiate the IP address entered instead of allowing another address to be assigned by the remote end. The default is **NO**.

KEEPALIVE PERIOD

This option allows the user to generate PPP keepalive packets that can be sent every **1** minute, **2** minutes, or every **5** minutes. A value of **0 (OFF)** disables the PPP keepalive packet generating feature. The default is **0 (OFF)**.

PPP ENCAPSULATION

This option allows the user to set the encapsulation modes for PPP over ATM. LLC has an encapsulation header in the AAL5 frame indicating it is encapsulating PPP. VC-Mux does not have a header, and is therefor dedicated to using PPP. The choices are **LLC** or **VC-MUX**. The default is **VC-MUX**.

SEND IDENTIFICATION

When enabled, this option enables the Total Access 600 Series to send the system identification code in response to a configure acknowledgement from the peer equipment. For most peer routers this option should be configured as **YES**. If set to **NO**, the Total Access 600 Series will accommodate peer routers that do not correctly respond to the identification code.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > SETUP (V35)

Use these menus to configure the V35 parameters for this logical connection from the T1 interface to the V.35 port. These menus are only applicable when the **CONNECTION** parameter is set to **V35**.

CONNECTION (V35) > SETUP > SETUP

Use these menus to configure the Protocol mapping, DE map, and FECN map for the V.35 PVC connections.

CONNECTION (V35) > SETUP > SETUP > PROTOCOL MAPPING

Network providers have the ability to provision each PVC pair with an encapsulation mode to ensure interoperability between terminal equipment. The choices are **TRANSPARENT** or **TRANSLATION** (def). **TRANSLATION** mode is most common and carries multiple upper layer protocols over Frame Relay and ATM PVCs.

CONNECTION (V35) > SETUP > SETUP > DE MAP

Maps Frame Relay Discard Eligible (DE) bit to the ATM Cell Loss Priority (CLP) bit. The choices are **DE = 0**, **DE = 1**, and **CONVERT** (map DE TO CLP). The factory default setting is **DE = 0**.

CONNECTION (V35) > SETUP > SETUP > FECN MAP

Allows mapping of Frame Relay FECN (Forward Explicit Congestion Notification) bit to ATM EFCI (Explicit Forward Congestion Indicator) bit. The choices are **NO MAP FECN** and **MAP** FECN. The factory default setting is **NO MAP FECN**.

CONNECTION (V35) > SETUP > DLCI MAPPING

Use these menus to configure the DLCI mapping for the PVC from the T1 network interface to the V.35 interface.

CONNECTION (V35) > SETUP > DLCI MAPPING > MAP

Displays the DLCI Map number and is used as an index for multiple listings. The first map entry listed is 1, the next is 2, etc. All map numbers assigned will be sequential.

CONNECTION (V35) > SETUP > DLCI MAPPING > ACTIVE

Enables FR/ATM mapping and data passing between the V.35 FRFx connection and the ATM PVC on the network interface. If set to **NO**, data will not pass from the network to the configured V.35 endpoint. By default, this field is set to **YES** to allow data to pass as soon as the connection is configured.

CONNECTION (V35) > SETUP > SETUP > INTERFACE

The T1 interface is **ATM[0.0]** which represents the T1 physical and logical ports respectively. This is an identifier for the system to document the T1 network end of the logical link between the network port and the V.35 interface.

CONNECTION (V35) > SETUP > SETUP > UNI DLCI

The Total Access 6XX terminates/converts an ATM circuit to a frame relay User to Network Interface (UNI) on the V.35 interface. This DLCI must match the DLCI programmed in the equipment connected to the V.35 interface.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > SETUP (VOICE)

Use these menus to configure the voice parameters for this logical connection from the T1 interface to the DSX-1 of FXS port being used as a voice interface. These menus are only applicable when the CONNECTION parameter is set to VOICE.

CONNECTION (VOICE) > SETUP > CALL CONTROL

The Call Control setting is used to configure the correct Voice Gateway protocol for voice signaling control between the Total Access 6XX and the configured Gateway. The CALL CONTROL setting must be configured correctly before the voice circuits will work correctly. The Total Access 6XX supports JETSTREAM, COPPERCOM, TOLLBRIDGE, and LES-CAS. The default is LES-CAS.

CONNECTION (VOICE) > SETUP > LES PROFILE

This option applies when CALL CONTROL is set to LES-CAS. The choices are ITU PROFILE 1, ATM FORUM PROFILE 9, and ATM FORUM PROFILE 10. The default is ATM FORUM PROFILE 10.

ATM FORUM PROFILE 9 provides ability to support 64 kbps PCM calls. ATM FORUM PROFILE 10 enables support of 64 kbps PCM calls as well as 32 kbps ADPCM calls.

CONNECTION (VOICE) > SETUP > LES-CAS GW SIM

Configures the interface to simulate a LES-CAS gateway. Enable this parameter only when back-to-back IAD testing.

CONNECTION (VOICE) > SETUP >IAD IP ADDRESS

This option applies when CALL CONTROL is set to TOLLBRIDGE. This field is automatically configured with the received IP address from the Tollbridge gateway. If the gateway fails to transmit the IP address this field may be set manually.

L2 PROTOCOL (ATM–NET–ATM) > CONFIG > PVC CONFIG > QOS

Use these menus to configure the Quality of Service parameters for the connection. This menu does not apply to logical connections involving a VOICE port.

QOS > QUALITY OF SERVICE

Quality of Service for ATM Undefined Bit Rate (UBR) and non-real time Variable Bit Rate (VBR) for the data PVC DLCI. This setting depends on the type of network ATM service being provided.

QOS > PEAK CELL RATE

Defines the peak cell rate for the data PVC. This setting is normally used for Undefined Bit Rate (UBR) connections and is calculated using the following equation:

$$\text{Peak Cell Rate} = \text{Bit Rate} / 424$$

The total of all peak cell rates for the ATM network connection must not exceed the line rate. The range for this parameter is **0** to **3623**.

L2 PROTOCOL (ATM–NET–ATM) > STATUS

Displays all available ATM statistics (both overall and PVC-specific).

L2 PROTOCOL (ATM–NET–ATM) > STATUS > ATM STATUS

Displays overall ATM link performance statistics. The following statistics are available:

AP: TX CELLS	Number of cells transmitted over the ATM link.
AP: RX CELLS	Number of cells received over the ATM link.
AP: RX OAM CELLS	Number of Operation, Administration, and Maintenance cells received on the ATM link. OAM cells provide network fault indications, performance information, and data and diagnostic functions.
AP: RECEIVE CELL DISCARDED	Number of cells received that are received and discarded. An incrementing count in this field could indicate a configuration problem with the ATM layer.
AP: RECEIVE CELL ERRORS	Number of cells received that contain a Header Error Control (HEC) error. The HEC is a CRC code located in the last byte of the ATM cell header that's used for checking integrity.
AP: SYNC	Indicates cell delineation at the ATM layer.
AP: OUT OF CELL	Indicates loss of cell delineation at the ATM layer.
AAL5: TRANSMIT FRAMES	Number of ATM Adaptation Layer Type 5 frames transmitted on the ATM link.
AAL5: RECEIVE FRAMES	Number of ATM Adaptation Layer Type 5 frames received on the ATM link.
AAL5: TRANSMIT DISCARDED FRAMES	Number of ATM Adaptation Layer Type 5 transmitted frames that were discarded before transmission.
AAL5: RECEIVE ERRORS	Number of ATM Adaptation Layer Type 5 frames that were received and contained errors.
AAL5: RECEIVE DISCARDED FRAMES	Number of ATM Adaptation Layer Type 5 frames that were received but then discarded.
AAL5: NO ATM FRAMES	Internal ADTRAN use only.
AAL5: NO DATA PACKETS	Internal ADTRAN use only.

L2 PROTOCOL (ATM–NET–ATM) > STATUS > ATM STATUS > CLEAR STATS

Clears all ATM statistics contained in the ATM status field and returns all counters to 0.

L2 PROTOCOL (ATM–NET–ATM) > STATUS > PVC STATUS

View the ATM PVC statistics from this menu.

L2 PROTOCOL (ATM–NET–ATM) > STATUS > PVC STATUS > NUM

Displays the index number in the PVC Status menu.

L2 PROTOCOL (ATM–NET–ATM) > STATUS > PVC STATUS > SUB-INTERFACE

This is a read-only field which displays the physical and logical port of the interface using the following nomenclature: [A.B], where A represents the physical port (network interface is 0, Ethernet is 1) and B represents the logical port for the Layer 2 protocol (i.e. PVC for Frame Relay, PPP link, etc.) Each configured logical port is assigned a number corresponding to the order in which they are listed in the L2 Protocol configuration fields.

L2 PROTOCOL (ATM–NET–ATM) > STATUS > PVC STATUS > AAL STATS

Shows the statistics of ATM Adaptation Layer frames.

MAX PDU SIZE	Maximum Protocol Data Unit size for the ATM AAL5 frame. All data information larger than the PDU must be transmitted in multiple frames.
TX DATA BYTES	Number of AAL5 data bytes transmitted.
TX FRAMES	Number of AAL5 frames transmitted.
TX CELLS (ALL TYPES)	Total number of AAL5 cells transmitted (all types).
TX OAM CELLS	Number of AAL5 Operations, Administration, and Maintenance cells transmitted.
TX RM CELLS	Number of AAL5 Resource Management cells transmitted.
TX EFCI=1 CELLS	Number of AAL5 EFCI=1 cells transmitted.
TX CLPI=1 CELLS	Number of AAL5 CLPI=1 transmitted.
RX DATA BYTES	Number of AAL5 data bytes received.
RX FRAMES	Number of AAL5 frames received
RX USER CELLS	Number of AAL5 user cells received
RX OAM CELLS	Number of AAL5 OAM cells received
RX BAD OAM CELLS	Number of AAL5 Bad OAM cells received
RX RM CELLS	Number of AAL5 RM cells received
RX BAD RM CELLS	Number of AAL5 Bad RM cells received
RX EFCI=1 CELLS	Number of AAL5 EFCI=1 cells received.
RX CLPI=1 CELLS	Number of AAL5 CLPI=1 cells received.
DISCARD RX CELLS	Number of AAL5 RX cells which were discarded.
DISCARD RX FRAMES	Number of AAL5 RX frames which were discarded.
DISCARD TX FRAMES	Number of AAL5 TX frames which were discarded.
TX QUEUE OVERFLOW	Number of cells discarded due to queue overflow.
TX OUT OF CELLS	Number of AAL5 TX Out of Cells.
TX INACTIVE	Number of TX frames discarded while PVC is inactive.
RX INACTIVE	Number of RX frames discarded while PVC is inactive.

CRC ERRORS	Number of AAL5 CRC Errors.
REASSEMBLY TIMEOUTS	Number of AAL5 Reassembly Timeouts.
TOO LONG FRAMES	Number of AAL5 Too Long Frames.
CLEAR COUNTS	Clears all recorded statistics and returns all counters to 0.

L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > PVC STATUS > PROTOCOL STATUS

Use these menus to view the **AAL2 STATS**, **POTS STATS**, and to **CLEAR STATS** for the PVC Protocol.

AAL2 STATS

ATM Adaptation Layer 2 statistics is used to provide error information on voice traffic. This menu displays **RX AAL2 HEC ERRORS**, **RX AAL2 SEQ ERRORS**, **RX VOICE SEQ ERRORS**, **RX VOICE BAD CID**, **RX VOICE BAD UUI**, **RX VOICE EOC CELLS**, and **PEAK CELL RATE**.

RX AAL2 HEC ERRORS

A CRC code (used for data integrity checks) is contained in the last byte of an AAL2 header. A received HEC error could result in dropped packets and poor voice quality.

RX AAL2 SEQ ERRORS

A single bit of the AAL2 header is used as a sequence bit and toggles from 1 to 0 with each successive transmitted cell. If two cells are received back to back with the same sequence bit, a sequence error is denoted.

RX VOICE SEQ ERRORS

Indicates that the Total Access 600 Series received voice packets that were out of sequence according to the voice sequencing bits. The Total Access 600 Series does not drop these packets, but the error is logged because invalid sequence numbers were received.

RX VOICE BAD CID

Indicates that the channel identifier (used for identifying voice calls in the ATM cell) was not valid.

RX VOICE BAD UUI

The User Indication designates the signaling bit pattern for PCM/ADPCM and identifies the packet as Type 1 (voice) or Type 3 (signaling). This error indicates the Total Access 600 Series received an incorrectly formatted UUI.

RX VOICE EOC CELLS

Indicates an EOC cell was received with a voice designation.

POTS STATS

Selecting this menu options will show real-time indication status of each voice port on the Total Access 600 Series. On a per port basis, the user can determine which ports are active/inactive as well as view other statistics like **TXQ**, **INSERTS** and **DROPS INDICATORS**.

> *The Echo Canceller module ADPCM functionality automatically shifts ON/OFF when fax or modem calls are placed. To find out the current status of the Echo Canceller functionality, check the current status of each FXS port. The path of the current status can be found at the following path:* **L2 PROTOCOL > STATUS > PVC STATUS > PROTOCOL STATUS > POTS STATS > CODING TYPE** *(this will display either PCM of ADPCM).*

TXQ

Displays the numbers of cells waiting in the buffer to transmit out the POTS port. Buffering voice cells is used to minimize jitter.

INSERTS

Displays the number of cells the Total Access 600 Series inserted on the analog interface to keep the current voice call connected when the network is idle.

DROPS

Displays the number of voice cells the Total Access 600 Series dropped due to a full buffer. This indicates that the network is sending traffic faster than the Total Access 600 Series is anticipating receiving cells; thus overrunning the jitter buffer. Excess drops could cause a timing mismatch.

CLEAR STATS

Clears all recorded statistics and returns all counters to 0.

L2 PROTOCOL (ATM FIRMWARE) – NETWORK INTERFACE > CUMTN FRE

Configure the **L2 PROTOCOL** parameters and view the status of the network interface using Copper Mountain Frame Relay protocol from this menu.

L2 PROTOCOL (ATM–NET–CUMTN) > CONFIG

Configure the **L2 PROTOCOL** parameters for the network interface using Copper Mountain Frame Relay protocol.

> *To insert a new profile, press the **I** key when over the **NUM** column. A new inserted profile will always be set up with the default parameters. To copy parameters from an old profile to this newly inserted profile, use the copy (**C**) and paste (**P**) keys. Entire configuration trees can be copied with this method.To delete an unused profile, use the **D** key when the cursor is over the number in the **NUM** column. Once deleted, the profile is gone permanently.*

L2 PROTOCOL (ATM–NET–CUMTN) > CONFIG > NUM

Displays the index number in the DLCI config table. The number range is **0-9**.

L2 PROTOCOL (ATM–NET–CUMTN) > CONFIG > ACTIVE

When this parameter is set to **YES** (def), the mapping is used to determine the protocols used. If set to **NO,** the unit will ignore the virtual circuit with this DLCI.

L2 PROTOCOL (ATM–NET–CUMTN) > CONFIG > INTERFACE

Shows the user the physical and logical port associated with each DLCI. This is a read-only field.

L2 PROTOCOL (ATM–NET–CUMTN) > CONFIG > DLCI

The DLCI (Data Link Connection Identifier) number identifies the virtual circuit being configured. The DLCI range is **16-1023**. The default is **16-25** corresponding to the index numbers **0-9** respectfully.

L2 PROTOCOL (ATM–NET–CUMTN) > CONFIG > CONNECTION

Select the physical and logical method of data transfer over the virtual path. There are two valid connection entries: **ROUTER** and **VOICE**. Select **ROUTER** to connect traffic from this PVC to the Total Access 6XX integral IP router. Select **VOICE** to connect traffic from this PVC to a voice connection (normally an FXS interface).

L2 PROTOCOL (ATM–NET–CUMTN) > CONFIG > SETUP

This submenu only appears for **VOICE** connections. Configure the **CALL CONTROL** for voice gateway using this menu.

L2 PROTOCOL (ATM–NET–CUMTN) > CONFIG > SETUP > CALL CONTROL

The **CALL CONTROL** setting is used to configure the correct Voice Gateway protocol for voice signaling control between the Total Access 6XX and the configured Gateway. The Call Control setting must be configured correctly before the voice circuits will work correctly. The Total Access 6XX supports **JETSTREAM**, **COPPERCOM**, **TOLLBRIDGE** and **LES-CAS** (def).

L2 PROTOCOL (ATM–NET–CUMTN) > STATUS

View the status of the Copper Mountain DLCI connections.

L2 PROTOCOL (ATM–NET–CUMTN) > STATUS > NUM

Displays the index number for the Status menu entries.

L2 PROTOCOL (ATM–NET–CUMTN) > STATUS > SUB-INTERFACE

This is a read-only field which displays the physical and logical port of the interface using the following nomenclature: [A.B], where A represents the physical port (network interface is 0, Ethernet is 1) and B represents the logical port for the Layer 2 protocol (i.e. PVC for Frame Relay, PPP link, etc.) Each configured logical port is assigned a number corresponding to the order in which they are listed in the L2 Protocol configuration fields.

L2 PROTOCOL (ATM–NET–CUMTN) > STATUS> DLCI STATE

This is a read-only field that displays the live DLCI state.

L2 PROTOCOL (ATM–NET–CUMTN) > STATUS > PROTOCOL STATUS

This is a read-only field that displays the live protocol status. Menu visible for physical and logical **VOICE** ports only.

L2 PROTOCOL (ATM–NET–CUMTN) > STATUS > PROTOCOL STATUS > POTS STATS

View the voice port activity and coding type.

L2 PROTOCOL (ATM–NET–CUMTN) > STATUS > PROTOCOL STATUS > CLEAR STATS

Clears all recorded statistics for the interface and returns all counters to 0.

L2 PROTOCOL (ATM FIRMWARE) – V.35 INTERFACE

Configure the **L2 PROTOCOL** parameters and view the status of the V.35 interface using items from this menu. The V.35 interface is only available when the configured network protocol is ATM. Refer to *L2 Protocol (ATM Firmware) – NET> ATM* on page 101.

L2 PROTOCOL (ATM – V35) > PROTOCOL

Configure the **L2 PROTOCOL** mode. Choices are **FRF5** (def) and **FRF8**. Selecting **FRF5** configures the interface for network interworking and should be used for Frame Relay over ATM applications. Selecting **FRF8** configures the interface for service interworking allowing the Total Access 600 Series to make the translation between Frame Relay signaling on the V35 interface and ATM protocols on the network interface.

L2 PROTOCOL (ATM – V35) > CONFIG

Configures the **L2 PROTOCOL** parameters for either FRF5 or FRF8 signaling.

L2 PROTOCOL (ATM – V35) > CONFIG > UNI MAINT PROTOCOL

Specifies the maintenance protocol or signaling protocol between the local V.35 port and the attached DTE port. The choices are **ANNEX D** (def), **ANNEX A**, **LMI**, and **STATIC**.

L2 PROTOCOL (ATM – V35) > CONFIG > UNI POLL TIMEOUT T392 (5-30)

T392 for signaling protocol. This parameter has no meaning if the **UNI MAINT PROTOCOL** is set to **STATIC** (no signaling). The default setting is **10**.

L2 PROTOCOL (ATM – V35)> STATUS

Displays the L2 statistics for FRF5 or FRF8 operation.

L2 PROTOCOL (ATM – V35)> STATUS> PORT

Displays statistics for all the PVCs configured on this port. The following statistics are available:

PORT INDEX	Port number
SIGNAL STATE	Frame relay state
TX FRAMES	Number of frames transmitted
RX FRAMES	Number of frames received
TX BYTES	Number of bytes transmitted
RX BYTES	Number of bytes received
FULL STATUS TX FRAMES	Number of Frame Relay signaling packets transmitted out the port
FULL STATUS RX FRAMES	Number of Frame Relay signaling packets received by the port
LINK INTEGRITY STATUS TX FRAMES	Number of Link Integrity signaling packets transmitted out the port
LINK INTEGRITY STATUS RX FRAMES	Number of Link Integrity signaling received by the port
DROP UNKNOWN DLCI	Number of frames received that were not associated with any known PVC
DROP INVALID DLCI	Number of frames received that had illegal DLCIs
CLEAR STATS	When activated, this field will clear all frame relay port stats

L2 PROTOCOL (V35[2]-ATM)> STATUS> PVC(S)

Displays statistics for all the PVCs configured on this port on a PVC basis. The following statistics are available:

DLCI	DLCI number
STATE	Frame relay state
TX FRAMES	Number of frames transmitted
RX FRAMES	Number of frames received
RX BYTES	Number of bytes received
DE COUNT	Number of packets received on an individual DLCI with the DE bit set
CR COUNT	Number of packets received on an individual DLCI with the CR bit set
BECN COUNT	Number of packets received on an individual DLCI with the BECN bit set
FECN COUNT	Number of packets received on an individual DLCI with the FECN bit set
UNKNOWN FRAME	RX Frames received that were not associated with any PVC entries

L2 PROTOCOL (ATM FIRMWARE) – DSX INTERFACE

Configure the **L2 PROTOCOL** parameters and view the status of the integrated DSX interface using items from this menu.

> **NOTE** *The DSX-1 Interface is optional and only available on 3rd Generation units.*

L2 PROTOCOL (ATM – DSX) > CONFIG

Configures the voice parameters for the interface.

INTERFACES (ATM – DSX) > CONFIG > SIGNALING

Configures the voice signaling implemented on the interface. The signaling must match the network application. The choices are:

E&M (TANDEM)	Sets the DSX interface to use E&M signaling.
LOOP START	Sets the DSX interface to use loop start signaling.
GROUND START	Sets the DSX interface to use ground start signaling.
ISDN PRI	Sets the DSX interface to use common channel signaling for ISDN.

INTERFACES (ATM – DSX) > CONFIG > TX OAM

Configures the Total Access 600 Series to transmit an Operation, Administration, and Maintenance (OAM) cell to the network (voice gateway) when the DSX interface is down.

INTERFACES (ATM – DSX) > CONFIG > RX OAM

Configures the Total Access 600 Series to transmit an alarm condition to the DSX interface when the network (voice gateway) is down.

INTERFACES (ATM – DSX) > CONFIG > LEGACY CONFIG

Digital trunk channel ID's are bits used to identify voice calls being carried within ATM cells. Some gateways do not support higher channel IDs, therefore the Total Access 600 Series supports CIDs from 16 or 65. The default is **DSX CID FROM 65**.

L2 PROTOCOL (ALL FIRMWARE) – ETH INTERFACE > 802.3 PROTOCOL

Configure the **L2 PROTOCOL** parameters and view the status of the Ethernet interface from this menu.

L2 PROTOCOL (ALL–ETH–802.3) > PROTOCOL

Displays the **L2 PROTOCOL** for the 10/100BaseT Ethernet port. Currently only **802.3** is supported.

L2 PROTOCOL (ALL–ETH–802.3) > CONFIG

Configure the mode for this **10/100BASET** Ethernet port from this menu.

L2 PROTOCOL (ALL–ETH–802.3) > CONFIG > MODE

The mode identifies how the data will be forwarded. The choices are:

ROUTE IP (def)	All IP data will be routed
BRIDGE ALL	All data will be bridged
ROUTE IP/BRIDGE OTHER	All IP data will be routed. All other data will be bridged.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS

View the **L2 PROTOCOL** statistics for the **10/100BASET** Ethernet port from this menu.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > TX PACKETS

Total number of packets transmitted out the Ethernet port.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > RX PACKETS

Total number of packets received from the Ethernet port.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > TX ERRORS

Total number of transmit errors encountered on Ethernet port.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > SINGLE COLLISIONS

Total number of single collisions before successful transmission.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > MULTIPLE COLLISIONS

Total number of multiple collisions before successful transmission.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > EXCESSIVE COLLISIONS

Total number of collisions that resulted in packet being dropped.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > DEFERRED TRANSMISSIONS

Total number of packets deferred due to collisions.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > CARRIER SENSE ERRORS

Total number of carrier sense errors encountered (no link integrity).

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > RX ERRORS

Number of packets received in error and dropped.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > CRCS

Number of packets detected with CRC errors.

L2 PROTOCOL (ALL–ETH–802.3]) > STATUS > RX COLLISIONS

Number of collisions which occurred during reception.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > NON-ALIGNED

The NON-ALIGNED parameter is set when the number of bits received is not divisible by 8.

L2 PROTOCOL (ALL–ETH–802.3) > STATUS > CLEAR COUNTS

Selecting this activator clears all the Ethernet stats.

BRIDGE

Configure the bridge parameters and view bridging statistics from this menu as shown in Figure 9.
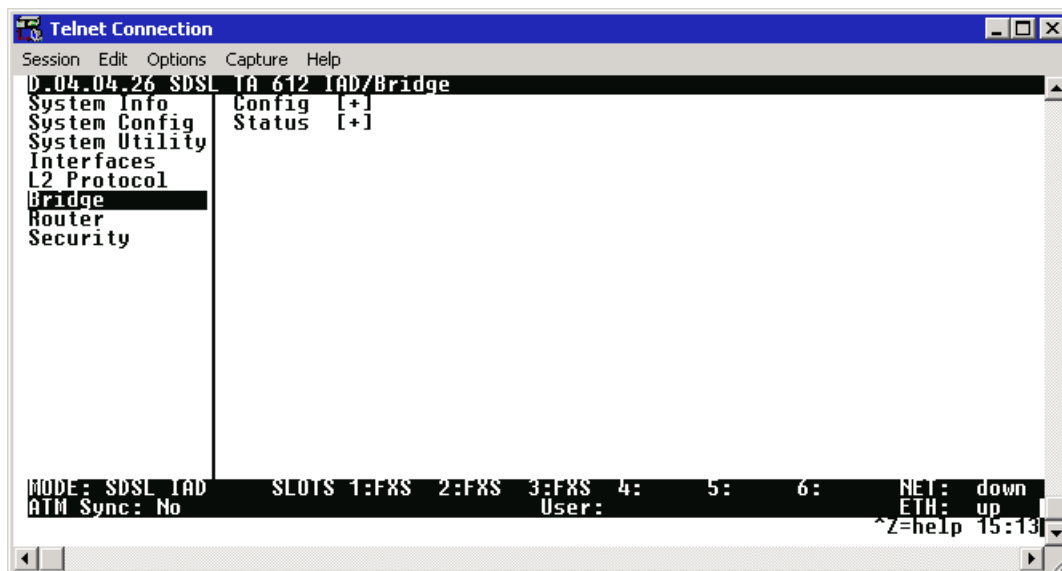
Figure 9. Bridge Menu

BRIDGE > CONFIG

Configure the interfaces and bridge table parameters from this menu.

BRIDGE > CONFIG > INTERFACES (NETWORK)

Configure the network interface bridging parameters from this menu.

BRIDGE > CONFIG > INTERFACES (NET) > SUB-INTERFACE

The network sub-interface is PPP [0.0] if the **L2 PROTOCOL** is set for **PPP**. The [0.0] represents the network physical and logical ports respectively. This is a read-only field. The network sub-interface is **FRE [0.X]** if the **L2 PROTOCOL** is set for **FRAME RELAY**. The [0.X] represents the network physical and logical ports respectively. The network physical port is always 0. The X represents the Frame Relay logical port and will be a number between 0-6 corresponding to the interface number under **L2 PROTOCOL > CONFIG > DLCI MAPPING**. This is a read-only field.

BRIDGE > CONFIG > INTERFACES (ETH)

Configure the Ethernet Bridging parameters from this menu.

> **NOTE**   *The ETH interface will not appear as a bridge interface entry if the mode is set to route IP.*

BRIDGE > CONFIG > INTERFACES (ETH) > SUB-INTERFACE

This is a read-only field which displays the physical and logical port of the interface using the following nomenclature: [A.B], where A represents the physical port (network interface is 0, Ethernet is 1) and B represents the logical port for the Layer 2 protocol (i.e. PVC for Frame Relay, PPP link, etc.) Each configured logical port is assigned a number corresponding to the order in which they are listed in the L2 Protocol configuration fields.

BRIDGE > CONFIG > BRIDGE TABLE

Configure the bridge table parameters from this menu.

BRIDGE > CONFIG > BRIDGE TABLE > BRIDGE TABLE AGING (0-65535)

BRIDGE TABLE AGING is how soon an entry ages out of the Bridge table (in minutes). Default is **5**.

BRIDGE > STATUS

View the bridging statistics from this menu.

BRIDGE > STATUS > BRIDGE TABLE

View the bridge table status from this menu.

BRIDGE > STATUS > BRIDGE TABLE > MAC ADDRESS

Ethernet address for device learned. This is a read-only field.

BRIDGE > STATUS > BRIDGE TABLE > LOCATION

Location indicates if it is LAN or WAN. This is a read-only field.

BRIDGE > STATUS > BRIDGE TABLE > TTL

Time to Live (TTL) is the number of seconds until the address is removed from the table. This is a read only field.

ROUTER

Configure the router parameters and view routing statistics from this menu as shown in Figure 8.
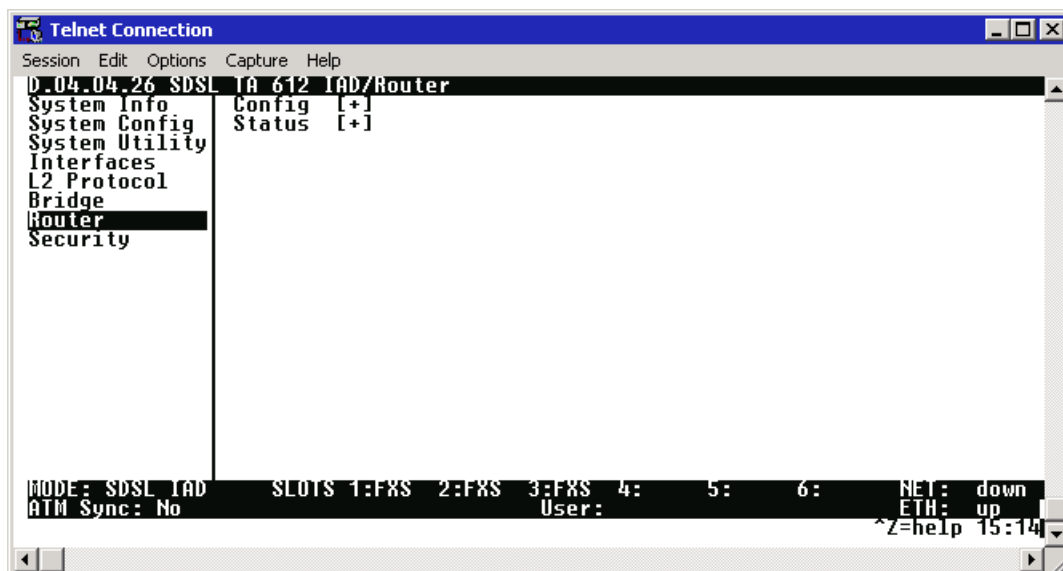
Figure 10. Router Menu

ROUTER > CONFIG

Configure the interfaces, routes, DHCP Server, and UDP Relay options from this menu.

ROUTER > CONFIG > INTERFACES

Configure the layer 3 options for the Ethernet and network interfaces from this menu.

ROUTER > CONFIG > INTERFACES (ETH)

Configure the layer 3 options for the Ethernet parameters from this menu.

> **NOTE**
>
> *The Ethernet port will always appear in the* **ROUTER > CONFIG > INTERFACES** *table regardless of the L2 protocol mode setting.*

ROUTER > CONFIG > INTERFACES (ETH) > SUB-INTERFACE

This is a read-only field which displays the physical and logical port of the interface using the following nomenclature: [A.B], where A represents the physical port (network interface is 0, Ethernet is 1) and B represents the logical port for the Layer 2 protocol (i.e. PVC for Frame Relay, PPP link, etc.) Each configured logical port is assigned a number corresponding to the order in which they are listed in the L2 Protocol configuration fields.

ROUTER > CONFIG > INTERFACES (ETH)> SETUP

Configure the Ethernet addressing, RIP, and Proxy ARP from this menu.

PRIMARY IP

This is used to setup the IP addresses for the LAN on the unit.

IP ADDRESS

The IP address assigned to the unit's Ethernet port is set here. This address must be unique within the network. Default is **10.0.0.1**.

SUBNET MASK

This is the IP network mask that is to be applied to the unit's Ethernet port. Default is **255.255.255.0.**

RIP

Use this menu to enable RIP on the LAN interface.

VERSION

Enables or disables RIP and specifies the RIP protocol. Choices are; **OFF** (which disables RIP), **V1** (RIP Version 1) or **V2** (RIP Version 2). The default is **OFF**.

METHOD

Specifies the way the RIP protocol sends out its advertisements. The following options are available:

SPLIT HORIZON (DEF)
Only routes not learned from this circuit are advertised.

POISON REVERSE
All routes are advertised, but the routes learned from this port are "poisoned" with an infinite metric. The default is Split Horizon.

DIRECTION

Allows the direction at which RIP advertisements are sent and received to be specified.

TX AND RX (DEF)

RIP advertisements are periodically transmitted and are listened to on this port.

TX ONLY

RIP advertisements are periodically transmitted but are not listened to on this port.

RX ONLY

RIP advertisements are listened to on this port, but are not transmitted on this port.

V2 SECRET

Enter the secret used by RIP version 2 here.

PROXY ARP

This feature allows the network portion of a group of addresses to be shared among several physical network segments. The ARP protocol provides a way for devices to create a mapping between physical addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a "proxy" for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to **YES,** when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, the unit will answer the request with its own hardware address. Default is **NO**.

SECONDARY IPS

This allows the unit to specify additional IP addresses and networks on its Ethernet. The maximum number of entries is 5.

NUM

Displays the index number in the secondary IP list.

IP ADDRESS

This is the second IP address the unit will respond to on the Ethernet. Default is **0.0.0.0**.

SUBNET MASK

This is the mask for the network. Default is **255.255.255.255**.

NAT MODE

This mode specifies whether Network Address Translation (NAT) should be used on this interface. When this mode is set to **PRIVATE** (default) and NAT is enabled for the unit, packets to and from this interface are translated. If set to **PUBLIC**, packets to and from this interface will not be translated through NAT.

ROUTER > CONFIG > INTERFACES (NETWORK)

Configure the layer 3 options for the network interface from this menu.

> **NOTE** *The network interface will display in the ROUTER > CONFIG > INTERFACES table showing the name of the network technology (i.e. T1, SHDSL, ADSL, SDSL), but only once a PVC to the router (ATM) or DS0s to the router (TDM) have been configured.*

ROUTER > CONFIG > INTERFACES (NET) > SUB-INTERFACE

This is a read-only field which displays the physical and logical port of the interface using the following nomenclature: [A.B], where A represents the physical port (network interface is 0, Ethernet is 1) and B represents the logical port for the Layer 2 protocol (i.e. PVC for Frame Relay, PPP link, etc.) Each configured logical port is assigned a number corresponding to the order in which they are listed in the L2 Protocol configuration fields.

ROUTER > CONFIG > INTERFACES (NET)> SETUP

Configure the IP parameters for this interface and sub-interface from this menu.

ACTIVE

This Selection enables IP on this PVC.

VPI

ATM virtual port identifier assigned to this sub-interface in the **L2 PROTOCOL** menus. This field is only applicable when L2 protocol for this sub-interface is ATM.

VCI

ATM virtual channel identifier assigned to this sub-interface in the **L2 PROTOCOL** menus. This field is only applicable when L2 protocol for this sub-interface is ATM.

DLCI

Data Link Connection Identifier assigned to this PVC in the **L2 PROTOCOL** menus. This field is only applicable when L2 protocol for this sub-interface is **FRE**.

ADDRESS MODE

Specifies the method the unit uses to determine the local and far-end IP addresses. The choices are **USER SPECIFIED** (default), **DHCP CLIENT**, or **IARP**. **USER SPECIFIED** allows the user configuration for Local IP and Far-End IP addresses, **DHCP CLIENT** is used for the Total Access 6XX to learn his IP address from a DHCP server. IARP allows the unit to determine the far-end IP address using inverse ARP.

LOCAL IP ADDRESS

This is the IP address for this PCV. This field is not visible when **ADDRESS MODE** is set to **DHCP CLIENT**.

IP NETMASK

This is the network mask used for this interface. This field is not visible when **ADDRESS MODE** is set to **DHCP CLIENT**.

FAR-END IP ADDRESS

This is the address of the NEXT hop router on this interface. This field is only visible when **ADDRESS MODE** is set to **USER SPECIFIED**.

MTU

Specifies the maximum size for a packet transmitted on this PVC. Default is **1500**. This field is only valid when L2 protocol for this sub-interface is **FRE**.

NAT

Use this menu to set up and use Network Address Translation on this interface.

PORT TRANSLATION

By enabling port translation, IP packets are modified as they pass through this interface. During transmission, private addresses are translated into a single public (NAPT) IP address. Incoming packets are translated from the public to private address based on the protocol port numbers. Once enabled, additional menus appear and can be used to further customize the NAT configuration. The default is **DISABLED**.

PUBLIC IP ADDRESS MODE

Sets the public NAPT address used for translating. Choices are **INTERFACE** (default) and **SPECIFIED**. Selecting **INTERFACE** configures NAT to use the IP address already specified on the interface; the NAPT address and the interface address are the same. Using **SPECIFIED** defines a particular IP address used as the NAPT address.

PUBLIC IP ADDRESS

This menu only appears when the **PUBLIC IP ADDRESS MODE** is set to **SPECIFIED**, and allows the user to enter a specific NAPT address.

TRANSLATE BODY OF UNMAPPED PARTS

Enabling this function forces NAPT to translate the body of any unmapped solicited traffic originating from the LAN. Default is **DISABLED**.

TRANSLATION TABLE

Table used for defining addresses and port translations. This is an indexed list of all translations defined for the router. It specifies the translations for specified public addresses/ports to private addresses/ports. To insert a new translation entry, highlight the index number of the first translation and press the **<I>** key. To delete a particular entry, highlight the index number of the entry and press the **<D>** key. The **TRANSLATION TABLE** parameter descriptions follow.

PUBLIC ADDRESS MODE

Choose **NAPT ADDR** (default) or **SPECIFIED** to choose which address to use for this translation. Choosing **SPECIFIED** allows the user to define a different public IP address to use for this translation.

PUBLIC ADDRESS

This menu appears when the **PUBLIC ADDRESS MODE** is set to **SPECIFIED**, and allows the user to enter a specific IP address as the NAPT address for this translation.

PROTOCOL MODE

Defines the protocol of the data for this translation. Choices are **TCP**, **UDP**, **ICMP**, **TCP OR UDP**, **ICMP**, **ALL**, **SPECIFIED**, or **NONE** (default). Use this option to specify whether you want to translate a specific protocol, group of protocols, or all protocols.

PROTOCOL

This menu appears when the **PROTOCOL MODE** is set to **SPECIFIED**. Use this option to specify a protocol number that does not appear in the list of choices under the Protocol Mode menu. The most common protocols are:

Protocol Number	Keyword	Protocol
1	ICMP	Internet Control Message
6	TCP	Transmission Control
8	EGP	Exterior Gateway Protocol
17	UDP	User Datagram
47	GRE	General Routing Encapsulation
50	ESP	IPSEC Encap Security Payload
51	AH	IPSEC Authentication Header

PROTOCOL TYPE

(Read only) This menu appears when the **PROTOCOL MODE** is set to **SPECIFIED** and displays the name of the specified protocol number (if the name is known by the Total Access 6XX). For example, entering a value of 47 in the **PROTOCOL** field will cause the **PROTOCOL TYPE** field to display **GRE**.

PUBLIC PORT MODE

This option appears when the **PROTOCOL MODE** is configured with a single protocol (such as TCP, UDP, or ICMP). Choices are **ANY PORT** (default) and **SPECIFIED**. The public destination port associated with this entry can be specified to add more control over certain types of traffic. Leave this configured as **ANY PORT** to cover all port types.

PUBLIC PORT

This menu appears when the **PUBLIC PORT MODE** is set to **SPECIFIED**. Use this option to specify the public port number to translate. Some well known TCP/UDP port numbers are shown below:

Port Number	Keyword	Port Type
20	FTP (data)	File Transfer Protocol Data
21	FTP (control)	File Transfer Protocol Control
23	Telnet	TCP/IP terminal emulation utility
666	DOOM	DOOM
53	DNS	Domain Name Server
69	TFTP	Trivial File Transfer Protocol
80	HTTP	Hypertext Transfer Protocol
110	POP3	Post Office Protocol ver. 3

PRIVATE ADDRESS MODE

Choose **ANY INTERNAL** (default) or **SPECIFIED** to choose which address to use for the private address. The private IP address can be specified to filter certain protocols and ports to specific servers in the private network. Likewise, internal hosts can be steered to certain servers on the public network. A new request from the public network that matches this entry's public parameters is dropped if the **PRIVATE ADDRESS MODE** is set to **ANY INTERNAL** (with the exception of protocols that the internal router is expected to respond to, such as ICMP or SNMP).

PRIVATE ADDRESS

This menu appears when the **PRIVATE ADDRESS MODE** is set to **SPECIFIED**, and allows the user to enter a specific private IP address for this translation. Packets destined for the public IP address (of this translation) are redirected to the private IP address specified here.

PRIVATE PORT MODE

Select **ANY PORT** (default) or a **SPECIFIED** port number for this translation. The private destination port associated with this entry can be specified to provide more control over certain types of traffic. Leave configured as **ANY PORT** to cover all port types.

PRIVATE PORT MODE

This menu appears when the **PRIVATE PORT MODE** is set to **SPECIFIED**, and allows the user to enter the port number that replaces the public port number during the translation of incoming packets. Outgoing packets from the private address space that match this protocol are sent to the specified public address and port, if any.

TRANSLATE BODY

If set to **YES**, the application payload in the packet is scanned for occurrences of the private/public IP address in binary or ASCII form. Set this to **NO** for applications where scanning payload data is undesirable.

NAT VIEW

Provides the user a dynamic view of current active router translations. Once the router has translated an inbound or outbound packet, the translation appears in this table. The main view is a listing of all the translations performed thus far. In order to see the detailed view of one of the entries, select the entry index number and press **<ENTER>**. The NAT View parameters are as follows:

PRIVATE ADDRESS

Private IP address of the active translation.

PUBLIC ADDRESS

Public IP address of the active translation.

SERVER ADDRESS

Server IP address of the public device.

PROTOCOL

Type of protocol active on the translation.

PRIVATE PORT

Private port number used for the translation.

SPOOFED PORT

Spoofed port number for the translation. The Total Access 6XX often needs to use the spoofed ports to determine which private device to translate the packet to. This would be necessary if multiple applications using the same private port were occurring simultaneously.

SERVER PORT

Port number used by the server (public device).

TOTAL TIME UNUSED

Time the translation has been unused, in seconds.

IN COUNT

Number of inbound packets using this translation.

OUT COUNT

Number of outbound packets using this translation.

NAPT ADDRESS

(Read only) Displays the NAPT address for the router. This will either be the interface address or the user-specified NAPT address.

ENTRY COUNT

The number of translation entries that are currently available in the **NAT VIEW** table. The Total Access 6XX supports up to 2000 active translations at any one time.

ENTRY OVERFLOW COUNT

The number of overflow **NAT VIEW** entries. After the maximum number of translations is reached, the Total Access 6XX will not add new translations, but continues to keep a count of any new translation requests it cannot accommodate.

RIP

Use this menu to enable RIP on this interface.

VERSION

Enables or disables RIP and specifies the RIP protocol. Choices are: **OFF** (which disables RIP), **V1** (RIP Version 1) or **V2** (RIP Version 2). The default is **OFF**

METHOD

Specifies the way the RIP protocol sends out its advertisements. The following options are available:

SPLIT HORIZON

(Default) Only routes not learned from this circuit are advertised.

POISON REVERSE

All routes are advertised, but the routes learned from this point are "poisoned" with an infinite metric.

DIRECTION

Allows the direction at which RIP advertisements are sent and received to be specified.

ROUTER > CONFIG > ROUTES

Configures the default gateway and static routes from this menu.

ROUTER > CONFIG > ROUTES > DEFAULT GATEWAY

The default gateway is used by the unit to send IP packets whose destination addresses are not found in the route table (otherwise known as the gateway of last resort). This is a default gateway for the entire unit, not just for the Ethernet port. Default is **0.0.0.0.**, which configures the Total Access 6XX to use the WAN port as the default gateway.

ROUTER > CONFIG > ROUTES > STATIC ROUTES

Use this menu to enter static routes to other networks.

NUM

Displays the index number in the static route table.

ACTIVE

Adds this static route entry to the IP routing table when set to **YES** and removes it (if it was previously added) if set to **NO**. Default is **NO**.

IP ADDRESS

The IP address of the host or network address of the device being routed to. Default is **0.0.0.0**.

SUBNET MASK

Determines the bits in the previous IP address that are used. If this is to be a host route, it must be set to all ones (255.255.255.255). Default is **0.0.0.0**.

GATEWAY

The IP address of the router to receive the forwarded IP packet. Default is **0.0.0.0.**

HOPS

The number of router hops required to get to the network or host. Maximum distance is 16 hops. Default is **1**.

PRIVATE

When set to **NO**, the unit will advertise this static route using RIP. Setting to **YES** means that the route is kept private. Default is **NO**.

ROUTER > CONFIG > DHCP SERVER

Use this menu to set up the DHCP server.

ROUTER > CONFIG > DHCP SERVER > DHCP SERVER

Use this menu to enable the DHCP server (**ON** or **OFF**).

ROUTER > CONFIG > DHCP SERVER > DHCP ADDRESS POOLS

Configures the parameters for the various defined DHCP address pools. Multiple DHCP address pools may be defined using these menus.

NUM

Displays the index number of the defined DHCP address pools. Multiple address pools are valid, and all will be listed in sequential order. This number is for reference only.

NAME

Enter a user-defined alphanumeric text string for the defined DHCP address pool. This text string is for easy identification and reference only.

TYPE

Configures the DHCP address pool as either a Network or Host pool.

LEASE CONFIG

Configures the lease duration for an IP address from this pool assigned by the DHCP server to a host on the network.

LEASE DAYS, HOURS, MINUTES

Defines the lease duration (in days, hours, and minutes) for an IP address from this pool assigned by the DHCP server to a host on the network.

NETWORK ADDRESS

Defines the network address for the configured address pool (for example, 172.24.0.0). The **NETWORK ADDRESS** and **NETWORK MASK** determine the number of addresses available on the network for the configured pool.

NETWORK MASK

Defines the network mask associated with the network address for the configured address pool (for example, 255.255.0.0). The **NETWORK ADDRESS** and **NETWORK MASK** determine the number of addresses available on the network for the configured pool.

POOL INFO

Configures various network parameters assigned to all hosts given an IP address from the configured address pool.

NETWORK MASK

Defines the network mask associated with the network address for the configured address pool (for example, 255.255.0.0). The **NETWORK ADDRESS** and **NETWORK MASK** determine the number of addresses available on the network for the configured pool.

DEFAULT ROUTER (PRI)

Defines the primary default router IP address (in dotted decimal notation) for all hosts given an IP address from the configured pool. When specifying a router to use as the primary/secondary preferred router, verify that the listed router is on the same subnet as the DHCP client.

DEFAULT ROUTER (SEC)

Defines the secondary default router IP address (in dotted decimal notation) for all hosts given an IP address from the configured pool. When specifying a router to use as the primary/secondary preferred router, verify that the listed router is on the same subnet as the DHCP client.

DNS SERVER (PRI)

Defines the primary Domain Name Server IP address (in dotted decimal notation) for all hosts given an IP address from the configured pool.

DNS SERVER (SEC)

Defines the secondary Domain Name Server IP address (in dotted decimal notation) for all hosts given an IP address from the configured pool.

NBNS SERVER (PRI)

Defines the primary NetBIOS Windows Internet Naming Service (WINS) name server IP address (in dotted decimal notation) available for use by the Dynamic Host Configuration Protocol (DHCP) clients.

NBNS SERVER (SEC)

Defines the secondary NetBIOS Windows Internet Naming Service (WINS) name server IP address (in dotted decimal notation) available for use by the Dynamic Host Configuration Protocol (DHCP) clients.

NBNS NODE TYPE

Defines the type of NetBIOS node used with Dynamic Host Configuration Protocol (DHCP) clients. The following node types are available:

    b-node (1) - **BROADCAST** node
    p-node (2) - **PEER-TO-PEER** node
    m-node (4) - **MIXED** node
    h-node (8) - **HYBRID** node (Recommended)

ROUTER > CONFIG > DHCP SERVER > EXCLUSION RANGES

Defines any IP address (or range of addresses) that should not be used the Total Access 600 Series DHCP server when making IP assignments to hosts on the network.

NUM

Displays the index number of the listed IP address exclusion ranges. Multiple address exclusions are valid, and all will be listed in sequential order. This number is for reference only.

START

Configures the start IP address (in dotted decimal notation) for the range of IP addresses to exclude from the DHCP address pool. Use in conjunction with the **END** field to establish a range of IP addresses. To exclude a single IP address, enter the same address in both the **START** and **END** fields.

END

Configures the ending IP address (in dotted decimal notation) for the range of IP addresses to exclude from the DHCP address pool. Use in conjunction with the **START** field to establish a range of IP addresses. To exclude a single IP address, enter the same address in both the **START** and **END** fields.

ROUTER > CONFIG > DHCP SERVER > GLOBAL SERVER OPTIONS

Configures various network parameters that apply to all hosts given an IP address from the configured address pools (regardless of the pool). Use these commands to configure parameters for all address pools when customizing between the address pools is not necessary. Refer to *Pool Info* on page 129 for more details on the available parameters.

ROUTER > CONFIG > UDP RELAY

This menu configures the unit to act as a UDP relay agent for applications requiring a response from UDP hosts that are not on the same network segment as their clients.

ROUTER > CONFIG > UDP RELAY > MODE

When this option is set to **ON**, the unit will act as a relay agent. Default is **OFF**.

ROUTER > CONFIG > UDP RELAY > UDP RELAY LIST

Up to four relay destination servers can be specified in this list.

#

Indicates the entry number in the UDP Relay List table.

RELAY ADDRESS

This is the IP address of the server that will receive the relay packet. Default is **0.0.0.0**.

UDP PORT TYPE

The choices are **STANDARD** (def) and **SPECIFIED**. The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123), NBNS (NetBios Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and BootP. When **SPECIFIED** is set, the UDP port (1 to 65535) can be specified in the UDP Port columns (up to three per server).

UDP PORT 1, 2, 3

Used for specifying UDP ports to be relayed. These fields only apply when **UDP PORT TYPE** is set to **SPECIFIED**. Default is **0**.

ROUTER > STATUS

View the **IP ROUTES**, **IP STATS**, **ARP CACHE**, **DHCP SERVER**, and **DHCP CLIENT** statistics from this menu.

ROUTER > STATUS > IP ROUTES

This lists the contents of the unit's IP route table.

ROUTER > STATUS > IP ROUTES > IP ADDRESS

Network or host destination address.

ROUTER > STATUS > IP ROUTES > NETMASK

Network mask applied to the destination address.

ROUTER > STATUS > IP ROUTES > GATEWAY

Host or router to receive this packet.

ROUTER > STATUS > IP ROUTES > PORT

Port gateway is located on:

LOCAL	Sent directly to the unit's router
ETH0	The unit's Ethernet port
WAN0	The unit's first PPP bundle
FR 0 . . . FR 9	The unit is connected up to 10 DLCIs

ROUTER > STATUS > IP ROUTES > USE

Number of times the unit has referenced the route.

ROUTER > STATUS > IP ROUTES > FLAGS

Important tags associated with this route entry

H	route is a host route
G	route is a gateway route
S	static route, or learned via IPCP, IARP, DHCP
R1	learned from RIP Version 1
R2	learned from RIP Version 2
I	route learned from an ICMP redirect
C	directly connected interface
P	route is private and is not advertised with RIP
T	route is to a triggered port (updates only when table changes)
U	learned by unknown method

ROUTER > STATUS > IP ROUTES > HOPS

Number of routers that must go through to get to destination. Ranges from **0-15** or **16** for infinite (can't get there from here).

ROUTER > STATUS > IP ROUTES > TTL

Seconds until address is removed from table. Value of 999 means route is static.

ROUTER > STATUS > IP STATS

This section describes the following **STATISTICS** submenus (and see the tables on the pages following):

- IP
- ICMP
- TCP
- UDP

All of these statistics are taken from the MIB-II variables in RFC 1156. To clear the accumulated statistics, press the **<ENTER>** key on **CLEAR COUNTS**.

ROUTER > STATUS > IP STATS > IP

View the IP statistics from this menu.

DEFAULT TTL

The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this unit, whenever a TTL value is not supplied by the transport layer protocol.

IP DATAGRAMS RECEIVED

The total number of input datagrams received from interfaces, including those received in error.

BAD HEADER PACKETS

The number of input datagrams discarded due to errors in their IP headers, including bad check sums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

BAD IP ADDRESSES

The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this unit. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

TOTAL FORWARDED DATAGRAMS

The number of input datagrams for which this unit was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this unit, and the Source-Route option processing was successful.

BAD PROTOCOL DISCARDS

The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

DATAGRAMS DISCARDED

The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

SENT DATAGRAMS TO UPPER LAYERS

The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

IP DATAGRAMS SENT

IP packets from the unit's IP stack.

ERRORFREE DISCARDS

The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in **TOTAL FORWARDED DATAGRAMS** if any such packets met this (discretionary) discard criterion.

ROUTELESS DISCARDS

The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in **TOTAL FORWARDED DATAGRAMS** which meet this "no-route" criterion. Note also that this includes any datagrams which a host cannot route because all of its default gateways are down.

IP REASSEMBLY TIMEOUT

The maximum number of seconds received fragments are held while awaiting reassembly at this unit.

DISASSEMBLED FRAGMENTS

The number of IP fragments received which needed to be reassembled at this unit.

IP DATAGRAMS REASSEMBLED

The number of IP datagrams successfully reassembled.

IP REASSEMBLY FAILURES

The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably RFC 815s) can lose track of the number of fragments by combining them as they are received.

SUCCESSFUL FRAGMENTS

The number of IP datagrams that have been successfully fragmented at this unit.

FAILED FRAGMENTS

The number of IP datagrams that have been discarded because they needed to be fragmented at this unit but could not be e.g., because their "Don't Fragment" flag was set.

TOTAL IP FRAGMENTS

The number of IP datagram fragments that have been generated as a result of fragmentation at this unit.

DISCARDED ROUTING ENTRIES

A packet the unit couldn't route.

CLEAR COUNTS

Setting this activator clears the IP Statistics.

ROUTER > STATUS > IP STATS > ICMP

ICMP MESSAGES RECEIVED

The total number of ICMP messages the unit received. Note that this counter includes all those counted by **ICMP SPECIFIC ERRORS**.

ICMP SPECIFIC ERRORS

The number of ICMP messages the unit received but determined as having errors (bad ICMP checksums, bad length, etc.)

ICMP DEST. UNREACHABLE MSGS RCVD

The number of ICMP Destination Unreachable messages received.

ICMP TIMEOUTS RECEIVED

The number of ICMP Time Exceeded messages received.

ICMP PARAMETER PROBLEM MSGS RCVD

The number of ICMP Parameter Problem messages received.

ICMP SOURCE QUENCH MSGS RCVD

The number of ICMP Source Quench messages received.

ICMP REDIRECTED MESSAGES RCVD

The number of ICMP Redirect messages received.

ICMP ECHO REQUEST MSGS RCVD

The number of ICMP Echo (request) messages received.

ICMP ECHO REPLY MSGS RCVD

The number of ICMP Echo Reply messages received.

ICMP TIMESTAMP REQUEST MSGS RCVD

The number of ICMP Timestamp (request) messages received.

ICMP TIMESTAMP REPLY MSGS RCVD

The number of ICMP Timestamp Reply messages received.

ICMP ADDRESS MASK REQUEST MSGS RCVD

The number of ICMP Address Mask Request messages received.

ICMP ADDRESS MASK REPLY MSGS RCVD

The number of ICMP Address Mask Reply messages received.

ICMP MESSAGES SENT

The total number of ICMP messages this unit attempted to send. Note that this counter includes all those counted by **ICMP PACKET ERRORS.**

ICMP PACKET ERRORS

The number of packets the unit did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.

ICMP DEST. UNREACHABLE MSGS SENT

The number of ICMP Destination Unreachable messages sent.

ICMP TIME EXCEEDED MSGS SENT

The number of ICMP Time Exceeded messages sent.

ICMP PARAMETER PROBLEM MSGS SENT

The number of ICMP Parameter Problem messages sent.

ICMP SOURCE QUENCH MSGS SENT

The number of ICMP Source Quench messages sent.

ICMP REDIRECT MSGS SENT

The number of ICMP Redirect messages sent.

ICMP ECHO REQUEST MSGS SENT

The number of ICMP Echo (request) messages sent.

ICMP ECHO REPLY MSGS SENT

The number of ICMP Echo Reply messages sent.

ICMP TIMESTAMP REQUEST MSGS SENT

The number of ICMP Timestamp (request) messages sent.

ICMP TIMESTAMP REPLY MSGS SENT

The number of ICMP Timestamp Reply messages sent.

ICMP ADDR MASK REQUEST MSGS SENT

The number of ICMP Address Mask Request messages sent.

ICMP ADDR MASK REPLY MSGS SENT

The number of ICMP Address Mask Reply messages sent.

CLEAR COUNTS

Selecting this activator will clear the ICMP statistics.

ROUTER > STATUS > IP STATS > UDP

View the UDP statistics from this menu.

UDP DATAGRAMS RECEIVED

The total number of UDP datagrams delivered to UDP users.

NO APPLICATION AT DEST. PORT

The total number of received UDP datagrams for which there was no application at the destination port.

UDP BAD PACKETS

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

UDP DATAGRAMS SENT

The total number of UDP datagrams sent from this unit.

CLEAR COUNTS

Selecting this activator clears the UDP statistics.

ROUTER > STATUS > IP STATS > UDP TABLE

View the UDP table statistics from this menu.

LOCAL IP ADDRESS

The destination IP address of the packet

PORT

The destination UDP port of the packet.

ROUTER > STATUS > IP STATS > TCP

View the TCP statistics from this menu.

RETRANSMISSION TIMEOUT ALGORITHM

The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.

MIN RETRANSMISSION TIMEOUT (MS)

The minimum value permitted by a **TCP** implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the **LBOUND** quantity described in RFC 793.

MAX RETRANSMISSION TIMEOUT (MS)

The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the **UNBOUND** quantity described in RFC 793.

MAX TCP CONNECTIONS

The limit on the total number of **TCP** connections the unit can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

ACTIVE TCP CONNECTIONS

The number of times **TCP** connections have made a direct transition to the **SYN-SENT** state from the **CLOSED** state.

TCP PASSIVE CONNECTIONS

The number of times **TCP** connections have made a direct transition to the **SYN-RCVD** state from the **LISTEN** state.

TCP FAILED ATTEMPTS

The number of times **TCP** connections have made a direct transition to the **CLOSED** state from either the **SYN-SENT** state or the **SYN-RCVD** state, plus the number of times **TCP** connections have made a direct transition to the **LISTEN** state from the **SYN-RCVD** state.

TOTAL TCP RESETS

The number of times TCP connections have made a direct transition to the **CLOSED** state from either the **ESTABLISHED** state or the **CLOSE-WAIT** state.

TCP CURRENT CONNECTIONS

The number of TCP connections for which the current state is either **ESTABLISHED** or **CLOSE-WAIT**.

TCP SEGMENTS RECEIVED

The total number of segments received, including those received in error. This count includes segments received on currently established connections.

TCP SEGMENTS SENT

The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

TOTAL TCP RETRANSMITS

The total number of segments retransmitted -- that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

CLEAR COUNTS

Selecting this activator clears the TCP statistics.

ROUTER > STATUS > IP STATS > TCP CONNS

View the TCP Conns Statistics from this menu. This table shows the different states of each TCP connection.

STATE

The possible states are **FREE**, **CLOSED**, **LISTEN**, **SYNC SENT**, **SYNC RECEIVED**, **ESTABLISHED**, **FINWAIT1**, **FINWAIT2**, **CLOSEWAIT**, **LASTACK**, **CLOSING**, and **TIMEWAIT**.

LOCAL IP ADDRESS

Local IP address of the TCP connection.

LOCAL PORT

Local port of the TCP connection.

REMOTE IP ADDRESS

Remote IP address of the TCP connection.

REMOTE PORT

Remote port of the TPC connection.

ROUTER > STATUS > ARP CACHE

Displays the contents of the unit's ARP table. All resolved cache entries time out after 20 minutes. Unresolved entries time out in 3 minutes. The ARP cache can be cleared by pressing "**f**" while on the menu or by pressing "**d**" on the individual number for that entry.

ROUTER > STATUS > ARP CACHE > IP ADDRESS

IP address used for resolving MAC address.

ROUTER > STATUS > ARP CACHE > MAC ADDRESS

Ethernet address resolved (0=no resolution).

ROUTER > STATUS > ARP CACHE > TIME

Minutes since entry was first entered into the ARP cache.

SECURITY

Set the **SECURITY FILTERS** and **RADIUS SERVER** parameters and configure the unit to forward or block directed broadcasts from this menu as shown in Figure 11.
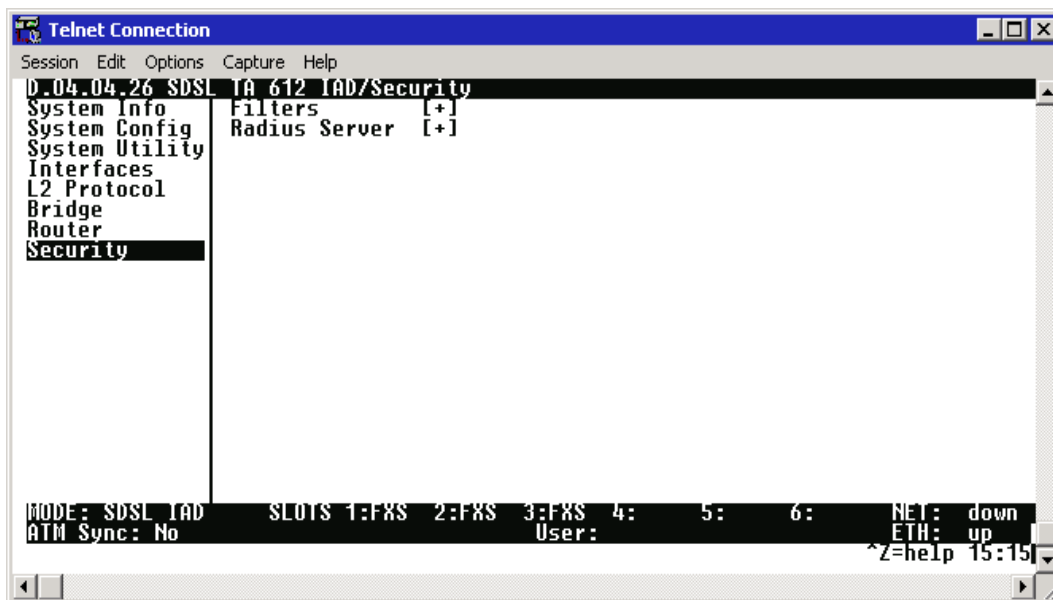
Figure 11. Security Menu

SECURITY > ACCEPT DIRECTED BROADCAST

Configures the Total Access 6XX to allow or disallow reception and forwarding of directed broadcast packets. Default is **DISABLED**. This option is a requirement for routers as described in RFC1812, section 4.2.2.11. Furthermore, it is **DISABLED** by default (RFC2644), with the intended goal of reducing the efficacy of certain types of denial of service attacks.

SECURITY > FILTERS

Configure the filter characteristics from this menu.

SECURITY > FILTERS > FILTER DEFINES

The unit can filter packets based on certain parameters within the packet. The method used by the unit allows the highest flexibility for defining filters and assigning them to a PVC or PPP link. The filters are set up in two steps: (1) defining the filter types, and (2) applying them to an interface. This menu is used to define the individual filter defines based on packet type.

> NOTE   *The Filter Defines option applies to both Frame Relay and PPP operation.*

SECURITY > FILTERS > FILTER DEFINES > MAC FILTER DEFINES

The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of the unit are defined here. Up to 32 MAC defines can be specified.

NUM

Indicates the entry number in the MAC Filter Defines table.

NAME

Identifies the filter entry. Default is no entry in **NAME** field.

FILTER TYPE

Specifies a **NORMAL** or **DEBUG** filter. When a **NORMAL** filer is applied to an interface, traffic is blocked or forwarded according to the filter. When a **DEBUG** filter is applied, packets that match the filter are documented without affecting traffic flow. (Use the **DEBUG** filter with the Syslog or Terminal Mode logging to view the packet contents.)

SRC ADDR

48-bit MAC source address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

SRC MASK

Bits in the MAC source address which are compared. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

DEST ADDR

48-bit MAC destination address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

DEST MASK

Bits in the MAC destination address used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00**.

TYPE

16-bit type field used for comparison. Values are in hexadecimal format. Default is **00:00**.

TYPE MASK

Bits in the type field used for comparison. Values are in hexadecimal format. Default is **00:00**.

SECURITY > FILTERS > FILTER DEFINES > PATTERN FILTER DEFINES

The pattern filter is applied to bridge packets only. That is any packet which is forwarded by the bridge functionality of the unit. Up to 32 pattern defines can be specified.

NUM

Indicates the entry number in the Pattern Filter Defines table.

NAME

Identifies the filter entry. Default is no entry in **NAME** field.

FILTER TYPE

Specifies a **NORMAL** or **DEBUG** filter. When a **NORMAL** filer is applied to an interface, traffic is blocked or forwarded according to the filter. When a **DEBUG** filter is applied, packets that match the filter are documented without affecting traffic flow. (Use the **DEBUG** filter with the Syslog or Terminal Mode logging to view the packet contents.)

OFFSET

Offset from beginning of packet of where to start the pattern comparison. Default is **0**.

PATTERN

64 bits used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00:00:00**.

MASK

Bits in the pattern to be compared. Values are in hexadecimal format. Default is **00:00:00:00:00:00:00:00**.

SECURITY > FILTERS > FILTER DEFINES > IP FILTER DEFINES

The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.

NUM

Indicates the entry number in the IP Filter Defines table.

NAME

Identifies the filter entry. Default is no entry in name field.

FILTER TYPE

Specifies a **NORMAL** or **DEBUG** filter. When a **NORMAL** filer is applied to an interface, traffic is blocked or forwarded according to the filter. When a **DEBUG** filter is applied, packets that match the filter are documented without affecting traffic flow. (Use the **DEBUG** filter with the Syslog or Terminal Mode logging to view the packet contents.)

SRC ADDR

IP address compared to the source address. Value is in dotted decimal format. Default is **0.0.0.0**.

SRC MASK

Bits which are used in the source comparison. Value is in dotted decimal format. Default is **0.0.0.0**.

DEST ADDR

IP address compared to the destination address. Value is in dotted decimal format. Default is **0.0.0.0.**

DEST MASK

Bits which are used in the destination comparison. Value is in dotted decimal format. Default is **0.0.0.0.**

SRC PORT

IP source port number used for comparison. Value is in decimal format. Range: **0 - 65535**. Default is **0**.

SRC PORT COMP

Type of comparison that is performed. Default is **NONE**.

> **=** means ports equal to
>
> **NOT =** means port not equal to
>
> **>** means port greater than
>
> **<** means port less than
>
> **None** - means the source port is not compared

DEST PORT

IP destination port number used for comparison. Value is in decimal format. Range: **0 - 65535**. Default is **0**.

DEST PORT COMP

Type of comparison that is performed. Default is **NONE**.

= means ports equal to

NOT = means port not equal to

> means port greater than

< means port less than

None - means the source port is not compared

PROTOCOL

Protocol used for comparison. Value is in decimal format. Range: **0 - 255**. Default is **0**.

PROTOCOL COMP

Type of comparison that is performed. Default is **NONE**.

= means ports equal to

NOT = means port not equal to

> means port greater than

< means port less than

None - means the source port is not compared

TCP ESTAB

YES - only when TCP established

NO - only when TCP not established

IGNORE - ignore TCP flags (def)

SECURITY > FILTERS > INTERFACES

The unit can block packets in and out of an interface by use of the filters. They are set up in two steps: 1) define the types of packets that would be of interest in the **SECURITY > FILTERS > FILTER DEFINES** menu, and 2) set up the filter type and combination of defines that will cause a packet block.

SECURITY > FILTERS > INTERFACES > SUB-INTERFACE

This is a read-only field which displays the physical and logical port of the interface using the following nomenclature: [A.B], where A represents the physical port (network interface is 0, Ethernet is 1) and B represents the logical port for the Layer 2 protocol (i.e. PVC for Frame Relay, PPP link, etc.) Each configured logical port is assigned a number corresponding to the order in which they are listed in the L2 Protocol configuration fields.

SECURITY > FILTERS > INTERFACES > SET-UP

Enable packet blocking or forwarding and apply pre-defined filter exceptions from this menu.

INCOMING

The packets received on the selected interface can be filtered in three ways:

DISABLE (DEF)	Turns off packet input filtering. No incoming packets are blocked.
BLOCK ALL	All incoming packets from the interface are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > IN EXCEPTIONS** list.
FORWARD ALL	All incoming packets from the interface are not blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > IN EXCEPTIONS** list.

IN EXCEPTIONS

Define exceptions to the forward/block all rules established using the **INCOMING** field. The Total Access 6XX allows for a list of up to 32 filter entries which are performed in the order they appear on the list.

#

Indicates the entry number in the In Exceptions table.

ACTIVE

Turns this entry active when set to **YES**. Default is **NO**.

TYPE

Selects the filter define list to reference (default is **MAC**).

MAC	from the **SECURITY > FILTERS > FILTER DEFINES > MAC FILTER DEFINES** list.
PATTERN	from the **SECURITY > FILTERS > FILTER DEFINES > PATTERN FILTER DEFINES** list.
IP	from the **SECURITY > FILTERS > FILTER DEFINES > IP FILTER DEFINES** list.

FILTER LIST NAME

Selects between filters defined in the list. Default is no entry in filter list name.

NEXT OPER

The next operation to use to combine with the next filter in the list (default is **END**).

END	the last filter to combination.
AND	logically AND this filter with the next filter in the list.
OR	logically OR this filter with the next filter in the list.

HIT COUNT

Displays the number of packets that have matched the criteria for the defined filter.

OUTGOING

The packets transmitted out the interface can be filtered in three ways:

DISABLE (DEF)	Turns off packet outputs filtering. No outgoing packets are blocked.
BLOCK ALL	All outgoing packets from the interface are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > OUT EXCEPTIONS** list.
FORWARD ALL	All outgoing packets from the interface are not blocked except as defined in the **SECURITY > FILTERS > INTERFACES > INTERFACES > SETUP > OUT EXCEPTIONS** list.

OUT EXCEPTIONS

Define exceptions to the forward/block all rules established using the **OUTGOING** field. The Total Access 6XX allows for a list of up to 32 filter entries which are performed in the order they appear on the list.

#

Indicates the entry number in the In Exceptions table.

ACTIVE

Turns this entry active when set to **YES**. Default is **NO**.

TYPE

Selects the filter define list to reference (default is **MAC**):

MAC	from the **SECURITY > FILTERS > FILTER DEFINES > MAC FILTER DEFINES** list.
PATTERN	from the **SECURITY > FILTERS > FILTER DEFINES > PATTER FILTER DEFINES** list.
IP	from the **SECURITY > FILTERS > FILTER DEFINES > IP FILTER DEFINES** list.

FILTER LIST NAME

Selects between filters defines in the list. Default is no entry in filter list name.

NEXT OPER

The next operation to use to combine with the next filter in the list (default is **END**):

END	the last filter to combination.
AND	logically AND this filter with the next filter in the list.
OR	logically OR this filter with the next filter in the list.

HIT COUNT

Displays the number of packets that have matched the criteria for the defined filter.

SECURITY > RADIUS SERVER

The parameters for the **RADIUS SERVER** are configured in this menu.

> **NOTE** *Telnet radius is only available in A.04 firmware or later.*

SECURITY > RADIUS SERVER > SERVER 1

This is the IP address of the first **RADIUS SERVER** that the unit should attempt to communicate with when authenticating a Telnet session. Default is **0.0.0.0**.

SECURITY > RADIUS SERVER > SERVER 2

This is the IP address of the second **RADIUS SERVER** that the unit should attempt to communicate with when the primary server does not respond. Default is **0.0.0.0**.

SECURITY > RADIUS SERVER > SERVER 3

This is the IP address of the third **RADIUS SERVER** that the unit should attempt to communicate with when the primary server does not respond. Default is **0.0.0.0**.

SECURITY > RADIUS SERVER > UDP PORT

This is the UDP port the unit should use when communicating with the **RADIUS SERVER**. The default is **1812**, which the commonly used port.

SECURITY > RADIUS SERVER > SECRET

The **RADIUS SERVER** and unit share this text string. It is used by the **RADIUS SERVER** to authenticate the unit, the RADIUS client. The factory default is not to use a secret.

SECURITY > RADIUS SERVER > RETRY COUNT (1-10)

This is the number of times the unit should send a request packet tho the **RADIUS SERVER** without a response before giving up. If the number of attempts to communicate with the primary server is equal to the retry count, the second server (if defined) is tried. If the second server does not respond within the retry count the third server (if defined) is tried. If the third server does not respond within the retry count, the Telnet session is not authenticated and is dropped. The default is **5**.

DS0 MAPS

> **NOTE** *The DS0 Maps configuration fields only apply for T1 TDM applications.*

The **DS0 MAPS** menu allows you to map data and voice ports to the network T1 time slots. You may edit either of the two maps at any time. If you make changes to the current map, only those DS0s that have changed will be updated (unchanged DS0s will not be affected.) The DS0 menu is shown in Figure 12.

```
Telnet Connection                                                    _ □ X
Session  Edit  Options  Capture  Help
A.04.04.35 TDM TA 612 IAD/DS0 Maps
System Info     Active Map              Map 1
System Config   Apply Template to Map 1 Current Map 1
System Utility  Edit/View Map 1         [+]
Interfaces      Apply Template to Map 2 Current Map 2
L2 Protocol     Edit/View Map 2         [+]
Bridge
Router
Security
DS0 Maps




MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:FXS  4:    5:    6:       NET:  down
DS0 Status: --------------------   User:                           ETH:  up
                                                                  ^Z=help 10:49
```
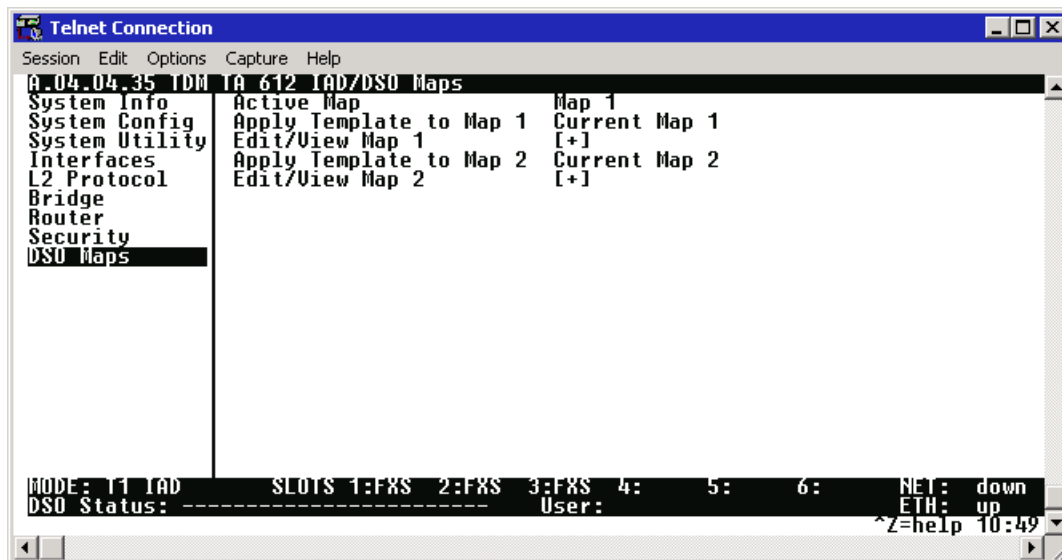
Figure 12. DS0 Maps Menu

DS0 MAPS > ACTIVE MAP

Activates one of the two dedicated maps (**MAP 1** or **MAP 2**), or the **DUAL T1 MAP** (only available in units with the optional DSX-1 interface). In the **DUAL T1** mode, the built-in DSX-1 interface DSX[3] can be utilized as a secondary T1 connection. In **DUAL T1** mode, the second T1 is limited to voice connections on FXS and FXO modules. For example, the user may map all 24 DS0s on the network T1 to the router, and on the second T1 (DSX-1 interface) map all 24 DS0s to the FXS cards. Default is **MAP 1**.

DS0 MAPS > APPLY TEMPLATE TO MAP 1

Choices are **CURRENT MAP 1**, **CURRENT MAP 2**, **D4 MAP**, **D1D MAP**, **FULL ROUTER,** and **CLEAR MAP**. Default is **CURRENT MAP 1**. **D4 MAP** automaps the voice port in a 1-to-1 configuration. **D1D MAP** maps voice ports in an SLC-96 configuration. **FULL ROUTER** maps all 24 DS0s to the router at 64K. **CLEAR MAP** clears the entire map.

DS0 MAPS > EDIT/VIEW MAP 1

Define map 1. The map allows the user to assign services and ports to the individual DS0s 1-24.

> **NOTE**   *In the default configuration for TDM A.04.XX firmware, DS0 24 is mapped to the router at 64K on Map 1.*

DS0 MAPS > EDIT/VIEW MAP 1 > DS0

Displays the network T1 time slot to be assigned.

DS0 MAPS > EDIT/VIEW MAP 1 > SERVICE

When you select this option, a list of available services displays. **OPEN** (default) indicates that the DS0 is not currently assigned to any specified service and is available for use. For a module listing, the module name is shown. For example, **FXS** indicates that an FXS module is installed and **FXO** indicates an FXO module (available as an option only on Total Access 624 systems). Select **TA IAD** to map a network timeslot to the **V.35** port or the internal router for data applications. **DSX-1** maps DS0s from the network T1 to the DSX-1 interface for voice or clear channel data applications. Pick the appropriate service, and press **<ENTER>**.

DS0 MAPS > EDIT/VIEW MAP 1 > PORT

When you select this option, a list of ports appears. Pick the appropriate port, and press **<ENTER>**. The selection list shows only the remaining ports available to be assigned. It may be necessary to unassign a port in order to reassign it elsewhere. For voice connections (FXS or FXO), the valid port range is limited by the number of installed voice ports on your system. For example, a Total Access 604 has 4 available voice ports, a Total Access 608 has 8 available voice ports, etc. When using the DSX-1 interface (specified under the **SERVICE** field), the **PORT** becomes an indicator of DS0 usage and the valid range is 1 to 24 (24 DS0s on a T1).

DS0 MAPS > EDIT/VIEW MAP 1 > RBS

Voice applications require signaling information to identify the state of the channel. In some voice networks a dedicated signaling channel is available to accomplish this (for example, ISDN with a dedicated D channel). Traditional voice networks may employ Robbed Bit Signaling (RBS), also known as Channel Associated Signaling (CAS), where a dedicated signaling channel is unavailable. RBS permanently encodes signaling information by "robbing" a single bit from designated T1 frames and using them as signaling information carriers. The actual location of the signaling information within the T1 frame depends on the framing format of the T1 circuit. For SuperFrame (SF) framing, the T1 channel is comprised of 12, 193-bit frames (192 data bits plus a single framing bit). RBS "robs" the framing bits from the even numbered frames (2, 4, 6, etc) to provide signaling information for that channel. The signaling bits provided in these frames are known as the A and B signaling bits. Voice termination devices use the various combinations of the signaling bits to identify the current state of the voice circuit. Each signaling type (Loop Start, Ground Start, E&M, etc) uses varying combinations of A and B bits to identify the various states of the circuits such as ringing, on-hook, and off-hook. Extended Superframe (ESF) framing is similar to SF in operation. Each ESF T1 channel is comprised of 24, 193-bit frames (192 data bits plus a single framing bit) and allows bit "robbing" in frames 6, 12, 18, and 24. These signaling bits are known as the A, B, C, and D signaling bits, respectively. Again, voice termination devices use the various combinations of the signaling bits to identify the current state of the voice circuit.

The default value for this parameter is **N/A**. Once a port is assigned to a service (using the **SERVICE** field), this parameter changes to **ON** or **OFF** (depending on the selected service). **ON** preserves the signaling bits between the connections and is typically required for analog voice connections; therefore, for FXS interfaces, **RBS** defaults to **ON**. Additionally, when passing voice circuits with in-channel signaling through to the DSX-1 interface, signaling bits are preserved by setting **RBS** to **ON**. For clear channel service to the DSX-1 interface (for voice circuits with a dedicated signaling channel and all data) set **RBS** to **OFF** (which ignores the signaling bits). When **SERVICE** is set to **T1 IAD**, the **RBS** parameter remains at **N/A** because **RBS** is not applicable to data connections.

> **NOTE**   *Map 2 menus are identical to Map 1. Please use the menu explanations above for Map 2.*

4.   APPENDICES (T1 TDM APPLICATIONS)

Appendix A. Configuring the Unit for Routing

Initial Setup

It is best to configure Total Access 6XX TDM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus. Follow the Layer 2 setup with the data "routing" menus (either **BRIDGE** or **ROUTER**). Establish packet forwarding and blocking using the **SECURITY** menus. Lastly, configure the physical mappings using the **DS0 MAPS** menus.

The following example provides step by step instructions for configuring the Total Access 6XX T1 TDM system (**INTERFACES** through **DS0 MAPS**) for a standard routing application. System Info and System Config parameters should be set according to your system need. Refer to *System Info* on page 49 and *System Config* on page 51 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

Network T1 menus beginning on page 71

Ethernet menus beginning on page 81

T1 Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
3	Right arrow to select **FORMAT** and choose **ESF** or **SF**.
NOTE	*This format must match the format used by the other units in the network.*
4	Set the **LINE CODE** to **B8ZS** or **AMI**.
NOTE	*This line code must match the line code used by the other units in the network.*
5	Set the **EQUALIZATION** or line build out. The default setting of **0 DB** is usually sufficient.
6	Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed.

Ethernet Interface Setup Instructions
Most applications should not require a manual setup for the Ethernet interface. By default, the Ethernet interface is configured to auto-detect the data rate (as either 10 or 100 Mbps). The following steps disable the auto-negotiation parameter and manually configure the interface.

Step	Action
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **ETH** interface and press **<ENTER>**.
3	Use the right arrow to select **AUTONEGOTIATION** and press **<ENTER>**. Use the down arrow to choose **OFF**.
4	Select the **DATA RATE** field and specify either **10BASET** or **100BASET**.
5	Select the **DUPLEX TYPE** field and specify either **HALF DUPLEX** or **FULL DUPLEX**.

2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

Layer 2 Protocol (FRE) Configuration – T1 Interface

Step	Action
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Use the arrow keys to select the **PROTOCOL** field for the **T1** interface. Press **<ENTER>**. Select **FRE** from the list of available protocols.
3	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
4	Set the **MAINTENANCE PROTOCOL** to **ANNEX D** (ANSI)**, ANNEX A** (q933a)**, LMI, OR STATIC** (no sig).
NOTE	*The **MAINTENANCE PROTOCOL** should be set based on the Frame Relay switch.*
5	Down arrow and press **<ENTER>** on **DLCI MAPPING**. Press the right arrow key to create an entry. To create additional entries, highlight the **NUM** field and press the **<I>** key. To delete an entry, highlight the **NUM** field for the entry to delete and press the **<D>** key.
6	Set **ACTIVE** to **YES**.

Layer 2 Protocol (FRE) Configuration – T1 Interface *(Continued)*	
7	Set **DLCI** to the DLCI number. This DLCI should match what is programmed in the network Frame Relay switch.
8	Set mode to **ROUTE IP**. Using this menu you also have the option to route only IP packets and bridge all other data packets (**ROUTE IP/BRIDGE OTHER**) or bridge all data packets on this PVC (**BRIDGE ALL**).
9	Left arrow back to the main menu to save the changes.

Layer 2 Protocol (PPP) Configuration – T1 Interface	
Step	**Action**
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Use the arrow keys to select the **PROTOCOL** field for the **T1** interface. Press **<ENTER>**. Select **PPP** from the list of available protocols.
3	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
4	Set mode to **ROUTE IP**. Using this menu you also have the option to route only IP packets and bridge all other data packets (**ROUTE IP/BRIDGE OTHER**) or bridge all data packets on this connection (**BRIDGE ALL**).
5	Highlight **AUTHENTICATION** and press **<ENTER>** to change options related to how the link is established. Default is **TX METHOD = NONE** and **RX METHOD = NONE**. If **TX METHOD** and **RX METHOD** are set to any option other than **NONE**, **TX/RX USERNAME** and **PASSWORD** options appear. The Total Access 6XX supports various combinations of PAP, CHAP, and EAP for PPP authentication. Refer to *L2 Protocol (TDM–T1–PPP) > Config > Authentication* on page 91 for more details.
6	Left arrow out of the **AUTHENTICATION** menus, highlight the **PPP** menu, and press **<ENTER>**. Use the PPP menus to configure parameters associated with the PPP link. Refer to *L2 Protocol (T1 TDM–T1–PPP) > Config* on page 91 for more details.
7	Left arrow back to the main menu to save the changes.

Layer 2 Protocol Configuration – Ethernet Interface	
Step	**Action**
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Highlight the **CONFIG** menu for the **ETH** (Ethernet) interface and press **<ENTER>**.

Layer 2 Protocol Configuration – Ethernet Interface	
3	Set mode to **ROUTE IP**. Using this menu you also have the option to route only IP packets and bridge all other data packets (**ROUTE IP/BRIDGE OTHER**) or bridge all data packets on this connection (**BRIDGE ALL**). Refer to *L2 Protocol (ALL–ETH–802.3) > Config > Mode* on page 116 for more details.
4	Left arrow back to the main menu to save the changes.

3. Setting the Router Options

For more details on the configuration parameters discussed in this section, refer to the following pages:

Router Options – Ethernet Interface	
Step	**Action**
1	From the main menu, select **ROUTER** and press **<ENTER>**.
2	Use the right arrow key to highlight **CONFIG** and press **<ENTER>**.
3	Select **INTERFACES** and press **<ENTER>**. Use the right arrow key to highlight the **SETUP** field for the **ETH** (Ethernet) interface and press **<ENTER>**.
4	Highlight the **PRIMARY IP** field and press **<ENTER>**.
5	Set the **IP ADDRESS** of the Ethernet port.
6	Set the **SUBNET MASK** for the Ethernet port.
7	By default, RIP is disabled on the Ethernet interface. If RIP needs to be enabled, highlight the **RIP** field and press **<ENTER>**. Set the appropriate **VERSION**, **RIP METHOD**, **DIRECTION**, and **V2 SECRET** (where applicable) to configure RIP on the interface. For more details, refer to *Router > Config > Interfaces (ETH) > Sub-Interface* on page 120.
8	Press the left arrow key to return to the Ethernet sub-interface menu (displays **PRIMARY IP** and **SECONDARY IP**).
9	If your application requires additional secondary IP address, highlight the **SECONDARY IP** field and press **<ENTER>**. The Total Access 6XX supports up to 5 additional LAN segments. Enter each additional secondary IP address and corresponding subnet mask. To add a new IP address entry, highlight the **NUM** field and press the **<I>** key. To delete an existing entry, highlight the **NUM** field for the entry to delete and press the **<D>** key.
10	Left arrow back to the main menu to save the changes.

Router Options – T1 Interface (L2 Protocol = FRE or PPP)	
Step	**Action**
1	From the main menu, select **ROUTER** and press **<ENTER>**.
2	Use the right arrow key to highlight **CONFIG** and press **<ENTER>**.
3	Select **INTERFACES** and press **<ENTER>**. Use the right arrow key to highlight the **SETUP** field for the **T1** interface and press **<ENTER>**. Each PVC (frame relay) on the T1 interface defined in the **DLCI MAP** has a separate listing in the **ROUTER INTERFACES** table.
4	Set **ACTIVE** to **YES** to activate the virtual circuit.
5	Select the desired **ADDRESS MODE**. Refer to *Address Mode* on page 122 for more details.
6	Enter the Total Access 6XX **LOCAL IP ADDRESS** and corresponding **IP NETMASK** for the selected virtual circuit.
7	Enter the IP address for the next hop router in the **FAR-END IP ADDRESS** field.
8	For NAT configuration, refer to *Appendix C. RFC1483 Quick Start (IP Routing with NAT)* on page 179.
9	Left arrow back to the main menu to save the changes.

Router Options – Setting the Default Gateway	
Step	**Action**
1	From the main menu, select **ROUTER** and press **<ENTER>**.
2	Use the right arrow key to highlight **CONFIG** and press **<ENTER>**.
3	Select **ROUTES** and press **<ENTER>**. Set the **DEFAULT GATEWAY** field to the appropriate IP address.
4	Left arrow back to the main menu to save the changes.

4. Mapping the DS0s

For more details on the configuration parameters discussed in this section, refer to the following pages:

DS0 Map menus beginning on page 149

DS0 Mapping Instructions	
Step	**Action**
1	From the main menu, select **DS0 MAPS**.
2	Verify that the **ACTIVE MAP** is set to either **MAP 1** or **MAP 2**. This is the map that is actively running on the unit. The unit has the ability to store two maps. • To edit the current map, press **<ENTER>** on **EDIT/VIEW MAP 1** to view the map. (If Map 1 is the Active Map) • To edit the standby map, press **<ENTER>** on **EDIT/VIEW MAP 2** to view the map. (If Map 2 is the Active Map)
NOTE	*The **DS0** listed on the left side of the menu corresponds to DS0s (1 through 24) on the network T1 interface. At least one DS0 must be mapped to the **ROUTER** to utilize the Total Access 6XX for routing purposes.*
3	Scroll down to the DS0 that will be mapped. (Any DS0 can be mapped to the router.)
4	Set the **SERVICE** for the DS0 that you are mapping to **TA IAD**.
5	Set the **PORT** of the DS0 that you are mapping to **ROUTER 64K** or **ROUTER 56K**.
6	Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map.
7	Make sure the **ACTIVE MAP** is set to the correct map (the map you want running) before exiting the **DS0 MAPS** menu.
8	Left arrow back to the main menu.

Appendix B. Configuring the Unit for Bridging

Initial Setup

It is best to configure Total Access 6XX TDM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus. Follow the Layer 2 setup with the data "routing" menus (either **BRIDGE** or **ROUTER**). Establish packet forwarding and blocking using the **SECURITY** menus. Lastly, configure the physical mappings using the **DS0 MAPS** menus.

The following example provides step by step instructions for configuring the Total Access 6XX T1 TDM system (**INTERFACES** through **DS0 MAPS**) for a standard bridging application. System Info and System Config parameters should be set according to your system need. Refer to *System Info* on page 49 and *System Config* on page 51 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

Network T1 menus beginning on page 71

Ethernet menus beginning on page 81

T1 Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
3	Right arrow to select **FORMAT** and choose **ESF** or **SF**.
NOTE	*This format must match the format used by the other units in the network.*
4	Set the **LINE CODE** to **B8ZS** or **AMI**.
NOTE	*This line code must match the line code used by the other units in the network.*
5	Set the **EQUALIZATION** or line build out. The default setting of **0 DB** is usually sufficient.
6	Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed.

Ethernet Interface Setup Instructions

Ethernet Interface Setup Instructions

Most applications should not require a manual setup for the Ethernet interface. By default, the Ethernet interface is configured to auto-detect the data rate (as either 10 or 100 Mbps). The following steps disable the auto-negotiation parameter and manually configure the interface.

Step	Action
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **ETH** interface and press **<ENTER>**.
3	Use the right arrow to select **AUTONEGOTIATION** and press **<ENTER>**. Use the down arrow to choose **OFF**.
4	Select the **DATA RATE** field and specify either **10BASET** or **100BASET**.
5	Select the **DUPLEX TYPE** field and specify either **HALF DUPLEX** or **FULL DUPLEX**.

2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Layer 2 Frame Relay Protocol menus beginning on *

*Layer 2 PPP Protocol menus beginning on *

*Layer 2 Ethernet menus beginning on *

Layer 2 Protocol (FRE) Configuration – T1 Interface

Layer 2 Protocol (FRE) Configuration – T1 Interface

Step	Action
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Use the arrow keys to select the **PROTOCOL** field for the **T1** interface. Press **<ENTER>**. Select **FRE** from the list of available protocols.
3	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
4	Set the **MAINTENANCE PROTOCOL** to **ANNEX D** (ANSI)**, ANNEX A** (q933a)**, LMI, OR STATIC** (no sig).
NOTE	*The **MAINTENANCE PROTOCOL** should be set based on the Frame Relay switch.*
5	Down arrow and press **<ENTER>** on **DLCI MAPPING**. Press the right arrow key to create an entry. To create additional entries, highlight the **NUM** field and press the **<I>** key. To delete an entry, highlight the **NUM** field for the entry to delete and press the **<D>** key.
6	Set **ACTIVE** to **YES**.

Layer 2 Protocol (FRE) Configuration – T1 Interface *(Continued)*	
7	Set **DLCI** to the DLCI number. This DLCI should match what is programmed in the network Frame Relay switch.
8	Set mode to **BRIDGE ALL**. Using this menu you also have the option to route only IP packets and bridge all other data packets (**ROUTE IP/BRIDGE OTHER**) or route all IP data packets on this PVC (**ROUTE IP**).
9	Left arrow back to the main menu to save the changes.

Layer 2 Protocol (PPP) Configuration – T1 Interface	
Step	**Action**
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Use the arrow keys to select the **PROTOCOL** field for the **T1** interface. Press **<ENTER>**. Select **PPP** from the list of available protocols.
3	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
4	Set mode to **BRIDGE ALL**. Using this menu you also have the option to route only IP packets and bridge all other data packets (**ROUTE IP/BRIDGE OTHER**) or route all IP data packets on this connection (**ROUTE IP**).
5	Highlight **AUTHENTICATION** and press **<ENTER>** to change options related to how the link is established. Default is **TX METHOD = NONE** and **RX METHOD = NONE**. If **TX METHOD** and **RX METHOD** are set to any option other than **NONE**, **TX/RX USERNAME** and **PASSWORD** options appear. The Total Access 6XX supports various combinations of PAP, CHAP, and EAP for PPP authentication. Refer to *L2 Protocol (TDM–T1–PPP) > Config > Authentication* on page 91 for more details.
6	Left arrow out of the **AUTHENTICATION** menus, highlight the **PPP** menu, and press **<ENTER>**. Use the PPP menus to configure parameters associated with the PPP link. Refer to *L2 Protocol (T1 TDM–T1–PPP) > Config* on page 91 for more details.
7	Left arrow back to the main menu to save the changes.

Layer 2 Protocol Configuration – Ethernet Interface	
Step	**Action**
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Highlight the **CONFIG** menu for the **ETH** (Ethernet) interface and press **<ENTER>**.

Layer 2 Protocol Configuration – Ethernet Interface *(Continued)*	
3	Set mode to **BRIDGE ALL**. Using this menu you also have the option to route only IP packets and bridge all other data packets (**ROUTE IP/BRIDGE OTHER**) or route all IP data packets on this connection (**ROUTE IP**). Refer to *L2 Protocol (ALL–ETH–802.3) > Config > Mode* on page 116 for more details.
4	Left arrow back to the main menu to save the changes.

3. Verifying the Bridge Options

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Bridge menus beginning on *

Bridge Options	
Step	**Action**
1	From the main menu, select **BRIDGE** and press **<ENTER>**.
2	Use the right arrow key to highlight **CONFIG** and press **<ENTER>**.
3	Select **INTERFACES** and press **<ENTER>**. Verify that the desired interface is listed in this table.
4	Left arrow back to the **BRIDGE > CONFIG** menu.
5	Select **BRIDGE TABLE** and set the **BRIDGE TABLE AGING** to the desired time (in minutes) it takes an entry to age out of the Bridge table.
6	Left arrow back to the main menu to save the changes.

4. Mapping the DS0s

For more details on the configuration parameters discussed in this section, refer to the following pages:

*DS0 Map menus beginning on *

DS0 Mapping Instructions	
Step	**Action**
1	From the main menu, select **DS0 MAPS**.

DS0 Mapping Instructions *(Continued)*	
2	Verify that the **ACTIVE MAP** is set to either **MAP 1** or **MAP 2**. This is the map that is actively running on the unit. The unit has the ability to store two maps. • To edit the current map, press **<ENTER>** on **EDIT/VIEW MAP 1** to view the map. (If Map 1 is the Active Map) • To edit the standby map, press **<ENTER>** on **EDIT/VIEW MAP 2** to view the map. (If Map 2 is the Active Map)
NOTE	*The **DS0** listed on the left side of the menu corresponds to DS0s (1 through 24) on the network T1 interface. At least one DS0 must be mapped to the **ROUTER** to utilize the Total Access 6XX for routing purposes.*
3	Scroll down to the DS0 that will be mapped. (Any DS0 can be mapped to the router.)
4	Set the **SERVICE** for the DS0 that you are mapping to **TA IAD**.
5	Set the **PORT** of the DS0 that you are mapping to **ROUTER 64K** or **ROUTER 56K**.
6	Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map.
7	Make sure the **ACTIVE MAP** is set to the correct map (the map you want running) before exiting the **DS0 MAPS** menu.
8	Left arrow back to the main menu.

Appendix C. Configuring the Unit for Voice Applications

Initial Setup

It is best to configure Total Access 6XX TDM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus. Follow the Layer 2 setup with the data "routing" menus (either **BRIDGE** or **ROUTER**). Establish packet forwarding and blocking using the **SECURITY** menus. Lastly, configure the physical mappings using the **DS0 MAPS** menus.

The following example provides step by step instructions for configuring the Total Access 6XX T1 TDM system (**INTERFACES** through **DS0 MAPS**) for a standard voice application. System Info and System Config parameters should be set according to your system need. Refer to *System Info* on page 49 and *System Config* on page 51 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

T1 Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
3	Right arrow to select **FORMAT** and choose **ESF** or **SF**.
NOTE	*This format must match the format used by the other units in the network.*
4	Set the **LINE CODE** to **B8ZS** or **AMI**.
NOTE	*This line code must match the line code used by the other units in the network.*
5	Set the **EQUALIZATION** or line build out. The default setting of **0 DB** is usually sufficient.
6	Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed.

FXS Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **FXS** interface and press **<ENTER>**.
3	Right arrow to select **MODE** and choose **LOOP START**, **GROUND START**, **TANDEM (E&M)**, **TR08 SINGLE**, **TR08 UVG**, or **DPO**.
NOTE	*This mode should be set based on the network configuration and the operation of each FXS port. All FXS ports are independent and do not need to have the same mode.*
4	Set the **Tx (dB)** or transmit direction level for each port. The default value is recommended.
5	Set the **Rx (dB)** or received direction level for each port. The default value is recommended.
6	Set the **SVC MODE** to **IN SERVICE** to activate the port.
7	Set the **LINE Z** (line impedance) of each port based on the size of the network. The default value is recommended.
8	Set the **MSG IND** to **DISABLE** or **ENABLE**. When set to **ENABLE**, talk path is always open, even in on-hook conditions, in order for FXS message tones to pass through. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID.
9	Configure the on-hook battery voltage using the **BATT MODE** field. For most IAD installs, the FXS loop is short with 6 to 7 V present on tip / ring. To reduce power dissipated during off-hook conditions, the battery is lowered for short loop lengths. When set to **AUTO SWITCH**, the IAD uses a higher on-hook battery voltage (48-52 V). When off-hook, it automatically switches to low battery (24-26 V) to minimize power dissipation. When set to **LOW BATTERY** mode, the higher battery is not used and the voltage is a constant 26 V even while on-hook. The tip/ring voltage is reduced to 26 V when using the **LOW BATTERY** mode.
10	Specify the interval of battery removal during a forward disconnect state using the **FWD DISC TIMER** field. Choices are **FOLLOW SWITCH** (default), **500MS**, **750MS**, **1000MS**, and **2000MS**. When using ATM mode, there is an additional choice of **IGNORE SWITCH**. If the timer is set to **FOLLOW SWITCH**, the Total Access 6XX will follow the switch at all times; this is normal operation. If a time period has been selected, the Total Access 6XX will remove battery for the specified time period OR as long as the switch requests battery removal, whichever is longer. For example, if the timer expires but the switch continues to request battery removal, the Total Access 6XX will follow the switch and continue to remove battery. For ATM mode, if the timer is set to **IGNORE SWITCH**, the IAD will never remove battery.

FXS Interface Setup Instructions *(Continued)*	
11	Press **<ENTER>** on the **TANDEM [+]** option to view the **TANDEM** options if the port mode is set to **TANDEM (E&M)**.
12	Set the **CONVERSION MODE** of the port to either **LOOP START** or **GROUND START**.
13	Set the **SUPERVISION** of the port to either **IMMEDIATE** or **WINK**.
NOTE	*Be sure to set the **TANDEM** options for each port set to **TANDEM E&M**.*

2. Mapping the DS0s

For more details on the configuration parameters discussed in this section, refer to the following pages:

*DS0 Map menus beginning on *

DS0 Mapping Instructions	
Step	**Action**
1	From the main menu, select **DS0 MAPS**.
2	Verify that the **ACTIVE MAP** is set to either **MAP 1** or **MAP 2**. This is the map that is actively running on the unit. The unit has the ability to store two maps. • To edit the current map, press **<ENTER>** on **EDIT/VIEW MAP 1** to view the map. (If Map 1 is the Active Map) • To edit the standby map, press **<ENTER>** on **EDIT/VIEW MAP 2** to view the map. (If Map 2 is the Active Map)
NOTE	*The **DS0** listed on the left side of the menu corresponds to DS0s (1 through 24) on the network T1 interface.*
3	Scroll down to the DS0 that will be mapped.
4	Set the **SERVICE** for the DS0 that you are mapping to **FXS**.
5	Set the **PORT** of the DS0 that you are mapping. The port number entered must match the voice port the DS0 is being mapped to. **RBS** (robbed bit signaling) will automatically turn on when a port number has been selected.
6	Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map.
7	Make sure the **ACTIVE MAP** is set to the correct map (the map you want running) before exiting the **DS0 MAPS** menu.
8	Left arrow back to the main menu.

Appendix D. Configuring the Unit for DSX-1 Applications

The Total Access 600 Series systems are available with an integrated DSX-1 interface for both voice and data applications. Regardless of the application (either voice or data), the Total Access 6XX has the ability to map DS0s from the network T1 to DS0s on the DSX-1 interface (cross-connect) without affecting the data present on the DS0s. This feature allows the Total Access 6XX to support voice with dedicated signaling channels (ISDN), voice with in-channel signaling information (Robbed Bit Signaling (RBS) to a PBX, key system, etc.), as well as clear channel data to an external T1 router.

Initial Setup

It is best to configure Total Access 6XX TDM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus. Follow the Layer 2 setup with the data "routing" menus (either **BRIDGE** or **ROUTER**). Establish packet forwarding and blocking using the **SECURITY** menus. Lastly, configure the physical mappings using the **DS0 MAPS** menus.

The following example provides details for configuring the Total Access 6XX to pass analog voice over the DSX-1 interface (using RBS), digital voice (fractional PRI with D-Channel), and data bandwidth. The Total Access 6XX provides a single DSX-1 interface, so it is unlikely that your application will require all three features on the DSX-1 interface simultaneously; therefore ignore any steps that do not pertain to your application.

Perform the following steps in order to configure the applications (**INTERFACES** through **DS0 MAPS**). **SYSTEM INFO** and **SYSTEM CONFIG** parameters should be set according to your system need. Refer to *System Info* on page 49 and *System Config* on page 51 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

> *Network T1 menus beginning on page 71*
> *DSX-1 menus beginning on page 78*

T1 Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
3	Right arrow to select **FORMAT** and choose **ESF** or **SF**.
NOTE	*This format must match the format used by the other units in the network.*
4	Set the **LINE CODE** to **B8ZS** or **AMI**.

T1 Interface Setup Instructions *(Continued)*	
NOTE	*This line code must match the line code used by the other units in the network.*
5	Set the **EQUALIZATION** or line build out. The default setting of **0 DB** is usually sufficient.
6	Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed.

DSX-1 Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **DSX** interface and press **<ENTER>**.
3	Right arrow to select **FORMAT** and choose **ESF** or **SF**.
NOTE	*This **FORMAT** must match the format used by the equipment connected to the DSX-1 interface. A **FORMAT** mismatch normally results in a Red Alarm condition.*
4	Set the **LINE CODE** to **B8ZS** or **AMI**.
NOTE	*This line code must match the line code used by the equipment connected to the DSX-1 interface.*
5	Set the **EQUALIZATION** or line build out. The default setting of **0 DB** is usually sufficient.
6	Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed.

2. Mapping the DS0s

For more details on the configuration parameters discussed in this section, refer to the following pages:

DS0 Map menus beginning on

DS0 Mapping Instructions	
Step	**Action**
1	From the main menu, select **DS0 MAPS**.
2	Verify that the **ACTIVE MAP** is set to either **MAP 1** or **MAP 2**. This is the map that is actively running on the unit. The unit has the ability to store two maps. • To edit the current map, press **<ENTER>** on **EDIT/VIEW MAP 1** to view the map. (If Map 1 is the Active Map) • To edit the standby map, press **<ENTER>** on **EDIT/VIEW MAP 2** to view the map. (If Map 2 is the Active Map)
NOTE	*The **DS0** listed on the left side of the menu corresponds to DS0s on the network T1 interface. The **PORT** number identifies the DS0 on the DSX-1 interface. The **DS0** and **PORT** do not need to match; DS0s can be cross-connected from the network T1 to any DS0 on the DSX-1 interface.*
3	Scroll down to the DS0 that will be mapped. (Any DS0 can be mapped to the DSX-1 interface.)
4	Set the **SERVICE** for the DS0 that you are mapping to **DSX-1**.
5	Set the **PORT** of the DS0 that you are mapping. The port number entered specifies the DS0 on the DSX-1 interface and can be set to any available DS0. When mapping voice circuits with dedicated signaling channels, be sure to map the signaling channel to the proper DS0 on the DSX-1 interface. For example, ISDN D channel signaling is normally carried on DS0 24. Unless the equipment connected to the Total Access 6XX DSX-1 interface has been specifically programmed, it will expect a D channel on DS0 24. Map DS0 24 to Port 24 to provide the D channel in the appropriate timeslot.
6	Set **RBS** to **OFF** or **ON** depending on the application. When passing voice circuits with in-channel signaling through to the DSX-1 interface, signaling bits are preserved by setting **RBS** to **ON**. For clear channel service to the DSX-1 interface (for voice circuits with a dedicated signaling channel and all data) set **RBS** to **OFF** (which ignores the signaling bits).
7	Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map.
8	Make sure the **ACTIVE MAP** is set to the correct map (the map you want running) before exiting the **DS0 MAPS** menu.
9	Left arrow back to the main menu.

5.   APPENDICES (T1 ATM APPLICATIONS)

> **NOTE**
> *The following example is for configuring T1 units with ATM firmware. However, all units using ATM firmware (SDSL, ADSL, SHDSL) may be configured in the same manner. To configure ATM Voice applications with other network types, disregard the T1 Interface Setup Instructions and configure your network interface as needed.*

Appendix A. Voice Gateway Quick Start Procedure (Voice Turn Up)

A typical VoATM application (see Figure 7) uses a Total Access 6XX connected to an ATM network. For voice applications, a Voice Gateway is needed to interface with the PSTN. Jetstream, Tollbridge, CopperCom, and LES-CAS are popular Gateway types.
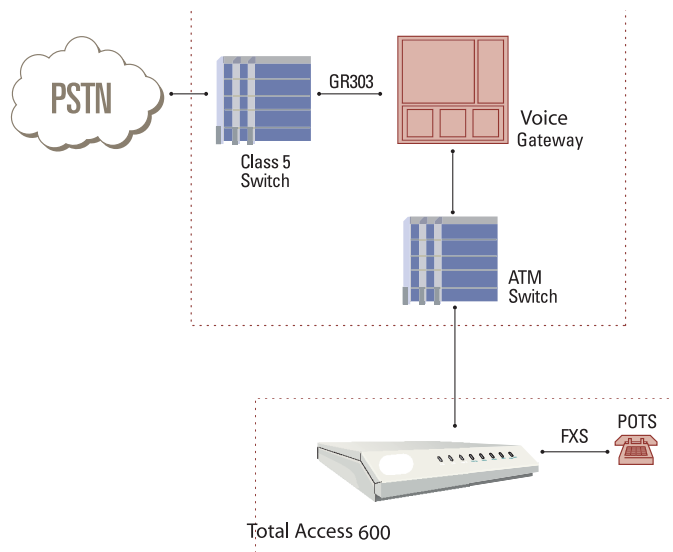
Figure 7. Application Diagram

To configure a Total Access 6XX for use with the Voice Gateway, you need to know the VPI and VCI used on the ATM network to access the Gateway from this Total Access 6XX. You also need to know the format for **IDLE CELLS** and whether **DATA SCRAMBLING** is used on this ATM network. The following procedure will help you navigate the Total Access 6XX menus for configuring the necessary elements for VoATM with the Voice Gateway.

Perform the following steps in order to configure the application.

Initial Setup
It is best to configure Total Access 6XX ATM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus.

The following example provides step by step instructions for configuring the Total Access 6XX T1 ATM system (**INTERFACES** and **L2 PROTOCOL**) for a standard voice application. System Info and System Config parameters should be set according to your system need. Refer to *System Info* on page 49 and *System Config* on page 51 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

<table>
<tr><td colspan="2" align="center">**T1 Interface Setup Instructions**</td></tr>
<tr><td align="center">**Step**</td><td align="center">**Action**</td></tr>
<tr><td align="center">**1**</td><td>From the main menu, select **INTERFACES**.</td></tr>
<tr><td align="center">**2**</td><td>Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.</td></tr>
<tr><td align="center">**3**</td><td>Right arrow to select **FORMAT** and choose **ESF** or **SF**.</td></tr>
<tr><td align="center">*NOTE*</td><td>*This format must match the format used by the other units in the network.*</td></tr>
<tr><td align="center">**4**</td><td>Set the **LINE CODE** to **B8ZS** or **AMI**.</td></tr>
<tr><td align="center">*NOTE*</td><td>*This line code must match the line code used by the other units in the network.*</td></tr>
<tr><td align="center">**5**</td><td>Set the **EQUALIZATION** or line build out. The default setting of **0 DB** is usually sufficient.</td></tr>
<tr><td align="center">**6**</td><td>Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed.</td></tr>
</table>

FXS Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **FXS** interface and press **<ENTER>**.
3	Right arrow to select **MODE** and choose **LOOP START**, **GROUND START**, **TANDEM (E&M)**, **TR08 SINGLE**, **TR08 UVG**, or **DPO**.
NOTE	*This mode should be set based on the network configuration and the operation of each FXS port. All FXS ports are independent and do not need to have the same mode.*
4	Set the **Tx (dB)** or transmit direction level for each port. The default value is recommended.
5	Set the **Rx (dB)** or received direction level for each port. The default value is recommended.
6	Set the **SVC MODE** to **IN SERVICE** to activate the port.
7	Set the **LINE Z** (line impedance) of each port based on the size of the network. The default value is recommended.
8	Set the **MSG IND** to **DISABLE** or **ENABLE**. When set to **ENABLE**, talk path is always open, even in on-hook conditions, in order for FXS message tones to pass through. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID.
9	Configure the on-hook battery voltage using the **BATT MODE** field. For most IAD installs, the FXS loop is short with 6 to 7 V present on tip / ring. To reduce power dissipated during off-hook conditions, the battery is lowered for short loop lengths. When set to **AUTO SWITCH**, the IAD uses a higher on-hook battery voltage (48-52 V). When off-hook, it automatically switches to low battery (24-26 V) to minimize power dissipation. When set to **LOW BATTERY** mode, the higher battery is not used and the voltage is a constant 26 V even while on-hook. The tip/ring voltage is reduced to 26 V when using the **LOW BATTERY** mode.
10	Specify the interval of battery removal during a forward disconnect state using the **FWD DISC TIMER** field. Choices are **FOLLOW SWITCH** (default), **500MS**, **750MS**, **1000MS**, and **2000MS**. When using ATM mode, there is an additional choice of **IGNORE SWITCH**. If the timer is set to **FOLLOW SWITCH**, the Total Access 6XX will follow the switch at all times; this is normal operation. If a time period has been selected, the Total Access 6XX will remove battery for the specified time period OR as long as the switch requests battery removal, whichever is longer. For example, if the timer expires but the switch continues to request battery removal, the Total Access 6XX will follow the switch and continue to remove battery. For ATM mode, if the timer is set to **IGNORE SWITCH**, the IAD will never remove battery.

FXS Interface Setup Instructions *(Continued)*	
11	Press **<ENTER>** on the **TANDEM [+]** option to view the **TANDEM** options if the port mode is set to **TANDEM (E&M)**.
12	Set the **CONVERSION MODE** of the port to either **LOOP START** or **GROUND START**.
13	Set the **SUPERVISION** of the port to either **IMMEDIATE** or **WINK**.

> **NOTE** *Be sure to set the **TANDEM** options for each port set to **TANDEM E&M**.*

2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Layer 2 ATM Network T1 menus beginning on *

Layer 2 Protocol Configuration – T1 Interface	
Step	**Action**
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Use the arrow keys to select the **PROTOCOL** field for the **T1** interface. Press **<ENTER>**. Select **ATM** from the list of available protocols.
3	Use the arrow keys to select the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
4	Highlight the **ATM CONFIG** menu for the **T1** interface and press **<ENTER>**.
5	Enter the **IDLE CELLS** format for your network.
6	Set **DATA SCRAMBLING** appropriately for your network.
7	Back all the way out to one level to the **PVC CONFIG** menu, and press **<ENTER>**. Enter the VPI and VCI values for communicating with that Gateway. (From this menu, the appropriate Voice information for working with the Voice Gateway is entered by selecting **VOICE** under the **CONNECTION** field.)

	Layer 2 Protocol Configuration – T1 Interface *(Continued)*
8	Select **SETUP**, and from the **SETUP** menu, enter the Gateway type under **CALL CONTROL** and enter the VPI and VCI values for communicating with that Gateway. For this application, **CALL CONTROL** and virtual identifier (**VPI** and **VCI**) values should be set appropriately for your network.
9	To verify correct setup, use the **PVC STATUS** menu (under the **STATUS** menu located at **L2 PROTOCOL [0] > STATUS**) to look at the current status of the voice connection. Under **STATUS**, view information about the voice PVC along with information about the POTS ports available on the unit.

Appendix B. RFC1483 Quick Start (IP Routing)

The Total Access 6XX allows for complete integration of voice and data delivery from one compact platform (see Figure 10). Once you have completed the voice turn up procedure from the previous example, adding data to the circuit requires some additional setup.
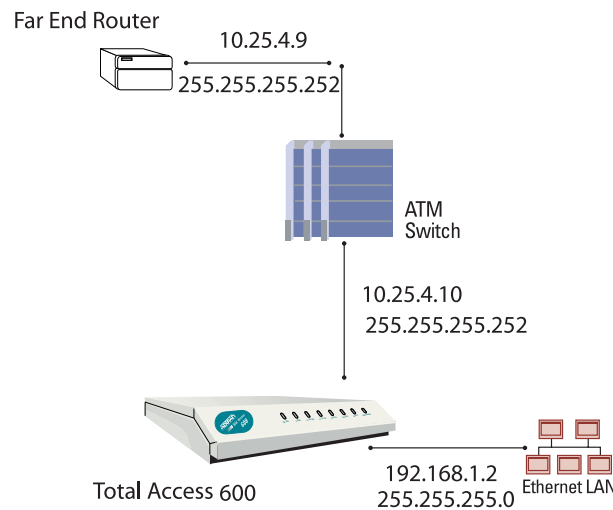
Figure 10. Application Diagram

To configure a Total Access 6XX for IP routing, you need to know the VPI and VCI values for the data circuit on your network. You also need the IP address of the next hop router in the circuit.

Perform the following steps in order to configure the application.

Initial Setup
It is best to configure Total Access 6XX ATM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus. Follow the Layer 2 setup with the data "routing" menus (either **BRIDGE** or **ROUTER**). Finally, establish packet forwarding and blocking using the **SECURITY** menus.

The following example provides step by step instructions for configuring the Total Access 6XX T1 ATM system (**INTERFACES** and **L2 PROTOCOL**) for a standard routing application. System Info and System Config parameters should be set according to your system need. Refer to *System Info* on page 49 and *System Config* on page 51 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

T1 Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
3	Right arrow to select **FORMAT** and choose **ESF** or **SF**.
🖉 **NOTE**	*This format must match the format used by the other units in the network.*
4	Set the **LINE CODE** to **B8ZS** or **AMI**.
🖉 **NOTE**	*This line code must match the line code used by the other units in the network.*
5	Set the **EQUALIZATION** or line build out. The default setting of **0 DB** is usually sufficient.
6	Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed.

Ethernet Interface Setup Instructions	
Most applications should not require a manual setup for the Ethernet interface. By default, the Ethernet interface is configured to auto-detect the data rate (as either 10 or 100 Mbps). The following steps disable the auto-negotiation parameter and manually configure the interface.	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **ETH** interface and press **<ENTER>**.
3	Use the right arrow to select **AUTONEGOTIATION** and press **<ENTER>**. Use the down arrow to choose **OFF**.
4	Select the **DATA RATE** field and specify either **10BASET** or **100BASET**.
5	Select the **DUPLEX TYPE** field and specify either **HALF DUPLEX** or **FULL DUPLEX**.

.2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

Layer 2 ATM Network Interface Protocol menus beginning on

	Layer 2 Protocol (ATM) Configuration – T1 Interface
Step	**Action**
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Use the arrow keys to select the **PROTOCOL** field for the **T1** interface. Press **<ENTER>**. Select **ATM** from the list of available protocols.
3	Use the arrow keys to select the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
4	Highlight the **ATM CONFIG** menu for the **T1** interface and press **<ENTER>**.
5	Enter the **IDLE CELLS** format for your network.
6	Set **DATA SCRAMBLING** appropriately for your network.
7	Back all the way out to one level to the **PVC CONFIG** menu, and press **<ENTER>**. Enter the VPI and VCI values for communicating with that Gateway. Select **ROUTER** under the **CONNECTION** field.
8	Select the **SETUP** menu and configure the virtual circuit for **IP** or **PPP** operation. (Our example selects **IP**.) Refer to *L2 Protocol (ATM–NET–ATM) > Config > PVC Config > Setup (Router)* on page 103 for more details.
9	Set mode to **ROUTE IP**. Using this menu you also have the option to route only IP packets and bridge all other data packets (**ROUTE IP/BRIDGE OTHER**) or bridge all data packets on this connection (**BRIDGE ALL**). Refer to *L2 Protocol (ATM–NET–ATM) > Config > PVC Config > Setup (Router)* on page 103 for more details.
10	Left arrow back to the main menu to save the changes.

3. Setting the Router Options

For more details on the configuration parameters discussed in this section, refer to the following pages:

Router Options – Ethernet Interface	
Step	**Action**
1	From the main menu, select **ROUTER** and press **<ENTER>**.
2	Use the right arrow key to highlight **CONFIG** and press **<ENTER>**.
3	Select **INTERFACES** and press **<ENTER>**. Use the right arrow key to highlight the **SETUP** field for the **ETH** (Ethernet) interface and press **<ENTER>**.
4	Highlight the **PRIMARY IP** field and press **<ENTER>**.
5	Set the **IP ADDRESS** of the Ethernet port.
6	Set the **SUBNET MASK** for the Ethernet port.
7	By default, RIP is disabled on the Ethernet interface. If RIP needs to be enabled, highlight the **RIP** field and press **<ENTER>**. Set the appropriate **VERSION**, **RIP METHOD**, **DIRECTION**, and **V2 SECRET** (where applicable) to configure RIP on the interface. For more details, refer to *Router > Config > Interfaces (ETH) > Sub-Interface* on page 120.
8	Press the left arrow key to return to the Ethernet sub-interface menu (displays **PRIMARY IP** and **SECONDARY IP**).
9	If your application requires additional secondary IP address, highlight the **SECONDARY IP** field and press **<ENTER>**. The Total Access 6XX supports up to 5 additional LAN segments. Enter each additional secondary IP address and corresponding subnet mask. To add a new IP address entry, highlight the **NUM** field and press the **<I>** key. To delete an existing entry, highlight the **NUM** field for the entry to delete and press the **<D>** key.
10	Left arrow back to the main menu to save the changes.

Router Options – T1 Interface (L2 Protocol = ATM)	
Step	**Action**
1	From the main menu, select **ROUTER** and press **<ENTER>**.
2	Use the right arrow key to highlight **CONFIG** and press **<ENTER>**.

	Router Options – T1 Interface (L2 Protocol = ATM) *(Continued)*
3	Select **INTERFACES** and press **<ENTER>**. Use the right arrow key to highlight the **SETUP** field for the **T1** interface and press **<ENTER>**. Each virtual circuit on the T1 interface defined in the **PVC CONFIG** has a separate listing in the **ROUTER INTERFACES** table.
4	Set **ACTIVE** to **YES** to activate the virtual circuit.
5	Enter the appropriate **VPI** and **VCI** values.
6	Select the desired **ADDRESS MODE**. Refer to *Address Mode* on page 122 for more details.
7	Enter the Total Access 6XX **LOCAL IP ADDRESS** and corresponding **IP NETMASK** for the selected virtual circuit.
8	Enter the IP address for the next hop router in the **FAR-END IP ADDRESS** field.
9	For NAT configuration, refer to *Appendix C. RFC1483 Quick Start (IP Routing with NAT)* on page 179.
10	Left arrow back to the main menu to save the changes.

	Router Options – Setting the Default Gateway	
Step	**Action**	
1	From the main menu, select **ROUTER** and press **<ENTER>**.	
2	Use the right arrow key to highlight **CONFIG** and press **<ENTER>**.	
3	Select **ROUTES** and press **<ENTER>**. Set the **DEFAULT GATEWAY** field to the appropriate IP address.	
4	Left arrow back to the main menu to save the changes.	

Appendix C. RFC1483 Quick Start (IP Routing with NAT)

To illustrate the use of NAT, consider the example from *Appendix B. RFC1483 Quick Start (IP Routing)* on page 174. To add NAT to the IP routing example, use the **NAT** menus.

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Router Network Interface Configuration menus beginning on *

IP Routing with NAT	
Step	**Action**
1	The **NAT** menu is found under **ROUTER >CONFIGURATION > INTERFACES > SETUP > NAT**. The **NAT** menu can easily be accessed by pressing **<CTRL+N>**.
NOTE	*The network interface will not appear if a virtual circuit is not defined using the **L2 PROTOCOL** menus.*
2	From the **NAT** menu, set **PORT TRANSLATION** to **ENABLED**. (This will enable translation and populate the corresponding NAT menu options.)
3	Set **PUBLIC IP ADDRESS MODE** to either **INTERFACE** or **SPECIFIED**. • **INTERFACE** (default) configures NAT to use the IP address already assigned to the interface. (In other words, the interface address and the NAPT address are the same.) • **SPECIFIED** allows you to define a different IP address for the NAPT address (public address for private addresses to be translated into). For basic NAT, this is all of the configuration that needs to be done. For specific port translations or 1:1 mapping, you can enter **TRANSLATION TABLE**.
4	From the **TRANSLATION TABLE** menu, create a new entry by using the right arrow to enter the table. Additional entries can be created by highlighting the first entry index number and pressing the **<I>** key. Entries can be deleted by highlighting the selected entry index number and pressing the **<D>** key.
5	Create specific NAT translations based on your application. **PUBLIC IP ADDRESS MODE** Use the configured interface IP address as the NAPT address or use **SPECIFIED** to set a different public address to be used for the translation. **PROTOCOL MODE** Protocol for this translation. (TCP, UCP, ICMP, TCP or UDP, TCP UDP or ICMP, All, Specified, and NONE.) **PRIVATE ADDRESS MODE** **SPECIFIED** or **ANY INTERNAL**. Choosing **SPECIFIED** brings up the **PRIVATE ADDRESS** option. **TRANSLATE BODY** **YES** or **NO**. If set to **YES**, this will translate the body of the data packet and replace the private address with the NAPT address. Default is **NO**, which is used for most applications.

Appendix D. RFC 1483 Quick Start (Bridging)

Initial Setup

It is best to configure Total Access 6XX ATM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus. Follow the Layer 2 setup with the data "routing" menus (either **BRIDGE** or **ROUTER**). Finally, establish packet forwarding and blocking using the **SECURITY** menus.

The following example provides step by step instructions for configuring the Total Access 6XX T1 ATM system (**INTERFACES** and **L2 PROTOCOL**) for a standard bridging application. System Info and System Config parameters should be set according to your system need. Refer to *System Info* on page 49 and *System Config* on page 51 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

Network T1 menus beginning on page 71

Ethernet menus beginning on page 81

T1 Interface Setup Instructions	
Step	**Action**
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
3	Right arrow to select **FORMAT** and choose **ESF** or **SF**.
NOTE	*This format must match the format used by the other units in the network.*
4	Set the **LINE CODE** to **B8ZS** or **AMI**.
NOTE	*This line code must match the line code used by the other units in the network.*
5	Set the **EQUALIZATION** or line build out. The default setting of **0 DB** is usually sufficient.
6	Set the **CSU LPBK** option to **ENABLE, DISABLE,** or **DISABLE ALL** based on whether looping to this unit from another unit will be allowed.

Ethernet Interface Setup Instructions
Most applications should not require a manual setup for the Ethernet interface. By default, the Ethernet interface is configured to auto-detect the data rate (as either 10 or 100 Mbps). The following steps disable the auto-negotiation parameter and manually configure the interface.

Step	Action
1	From the main menu, select **INTERFACES**.
2	Highlight the **CONFIG** menu for the **ETH** interface and press **<ENTER>**.
3	Use the right arrow to select **AUTONEGOTIATION** and press **<ENTER>**. Use the down arrow to choose **OFF**.
4	Select the **DATA RATE** field and specify either **10BASET** or **100BASET**.
5	Select the **DUPLEX TYPE** field and specify either **HALF DUPLEX** or **FULL DUPLEX**.

.2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Layer 2 ATM Network Interface Protocol menus beginning on *

Layer 2 Protocol (ATM) Configuration – T1 Interface

Step	Action
1	From the main menu, select **L2 PROTOCOL** and press **<ENTER>**.
2	Use the arrow keys to select the **PROTOCOL** field for the **T1** interface. Press **<ENTER>**. Select **ATM** from the list of available protocols.
3	Use the arrow keys to select the **CONFIG** menu for the **T1** interface and press **<ENTER>**.
4	Highlight the **ATM CONFIG** menu for the **T1** interface and press **<ENTER>**.
5	Enter the **IDLE CELLS** format for your network.
6	Set **DATA SCRAMBLING** appropriately for your network.
7	Back all the way out to one level to the **PVC CONFIG** menu, and press **<ENTER>**. Enter the VPI and VCI values for communicating with that Gateway. Select **ROUTER** under the **CONNECTION** field.
8	Select the **SETUP** menu and configure the virtual circuit for **IP** or **PPP** operation. (Our example selects **IP**.) Refer to *L2 Protocol (ATM–NET–ATM) > Config > PVC Config > Setup (Router)* on page 103 for more details.

	Layer 2 Protocol (ATM) Configuration – T1 Interface *(Continued)*
9	Set mode to **ROUTE IP**. Using this menu you also have the option to route only IP packets and bridge all other data packets (**ROUTE IP/BRIDGE OTHER**) or bridge all data packets on this connection (**BRIDGE ALL**). Refer to *L2 Protocol (ATM–NET–ATM) > Config > PVC Config > Setup (Router)* on page 103 for more details.
10	Left arrow back to the main menu to save the changes.

3. Verifying the Bridge Options

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Bridge menus beginning on *

	Bridge Options	
Step	**Action**	
1	From the main menu, select **BRIDGE** and press **<ENTER>**.	
2	Use the right arrow key to highlight **CONFIG** and press **<ENTER>**.	
3	Select **INTERFACES** and press **<ENTER>**. Verify that the desired interface is listed in this table.	
4	Left arrow back to the **BRIDGE > CONFIG** menu.	
5	Select **BRIDGE TABLE** and set the **BRIDGE TABLE AGING** to the desired time (in minutes) it takes an entry to age out of the Bridge table.	
6	Left arrow back to the main menu to save the changes.	

DETAIL LEVEL PROCEDURES

DLP-1   Connecting a VT100 Terminal or PC to the CRAFT Port

Introduction

Total Access 6XX shelf management and provisioning are facilitated by a series of intuitive menus that are accessible on a computer screen. Connecting either a VT100 terminal or a PC emulating a VT100 terminal to the RJ-48 **CRAFT** port on the rear of the unit allows access to the menus and management features of the Total Access 6XX. An adapter is required for access to this rear port. For more details concerning this adapter, refer to *CRAFT Port* on page 31. This DLP specifies how to connect the VT100 terminal or PC to the unit.

Prerequisite Procedures

The Total Access 6XX must be powered for terminal communication to function.

Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software. A VT100 emulation program is provided with your shipment as part of the ADTRAN Utilities software suite.
- Appropriate cable to connect terminal to the Total Access 6XX (customer-provided).
- DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

1. Connecting a VT100 terminal to Total Access 6XX:

    •   Set the parameters of the VT100 terminal or PC to:
        –   9600 baud rate
        –   8 data bits
        –   No parity
        –   1 stop bit
        –   No flow control

    •   If the terminal has a parallel setting, disable it and use the serial port.

    Using the CRAFT Port

    •   Plug the RJ-48 end of the data cable into the Total Access 6XX **CRAFT** port on the back of the unit. Make the connection to the VT100 terminal as appropriate for your equipment.

2. Connect a PC emulating a VT-100 terminal to Total Access 6XX.
    Most personal computers (PCs) or laptops can run communications software that emulates a VT100 terminal. Examples include Windows programs such as Terminal® or Hyperterminal®. However, there are many other adequate, commercially available software packages which will allow your PC or laptop to emulate a VT100 terminal.

    •   Set the parameters of the communications software to:
        –   9600 baud rate
        –   8 data bits
        –   No parity
        –   1 stop bit
        –   No flow control

    •   Set the PC for direct connect on the appropriate com port (instead of dial up connection).

    Using the CRAFT Port

    •   Plug the RJ-48 end of the data cable into the Total Access 6XX **CRAFT** port on the back of the unit. Make the connection to the VT100 terminal as appropriate for your equipment.

You are now ready to log in to the Total Access 6XX, as described in *DLP-2, Logging in to the System*.

DLP-2   Logging in to the System

Introduction

Once connected to the Total Access 6XX, you must login to the system to gain access to the management and provisioning functions. This DLP assumes you are connected to the Total Access 6XX and provides specific steps for logging into the system.

Prerequisite Procedures

Complete DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*.

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

NOTE	*After the IP parameters have been provisioned (see DLP-3, Setting IP Parameters), you can also log in via Telnet.*

Perform the steps below in the order listed.

---

1. After connecting to the system, press any key to display the Login screen shown here. The blinking cursor at the Login field indicates that a password must be entered.

2. Enter the password for the Total Access 6XX at the Login field. There is no manufacturer's default password; press **<Enter>** to enter the Total Access 6XX menus.

3. Upon entering the correct password, the Total Access 6XX main menu is displayed as shown below.

4. You are now logged in to the Total Access 6XX menu system.

DLP-3   Setting IP Parameters

Introduction

If the Total Access 6XX is connected to an IP network for Telnet, TFTP, or SNMP management, there are several IP parameters which must be set for the unit to communicate with the network. These parameters are described in this DLP along with the procedures for setting them.

> **NOTE**
> *Please see your Network Administrator for the proper assignment of the following parameters: **IP ADDRESS**, **SUBNET MASK**, and **DEFAULT GATEWAY**.*

Prerequisite Procedures

This procedure assumes that the Total Access 6XX unit is connected to an IP network and is powered up.

Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 6XX (customer-provided).
- DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

> **WARNING**
> *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*
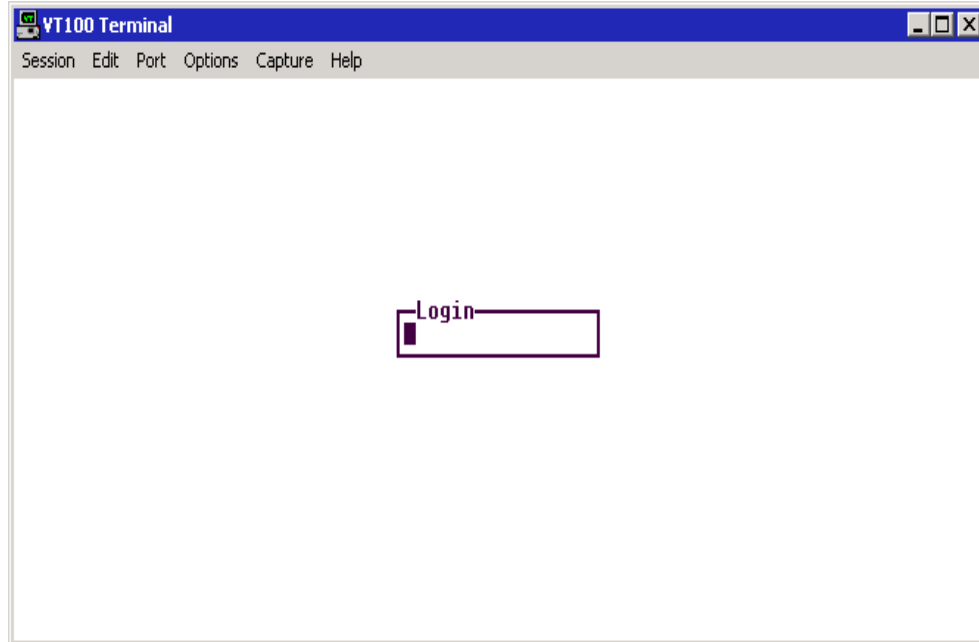
> **CAUTION**
> *Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*
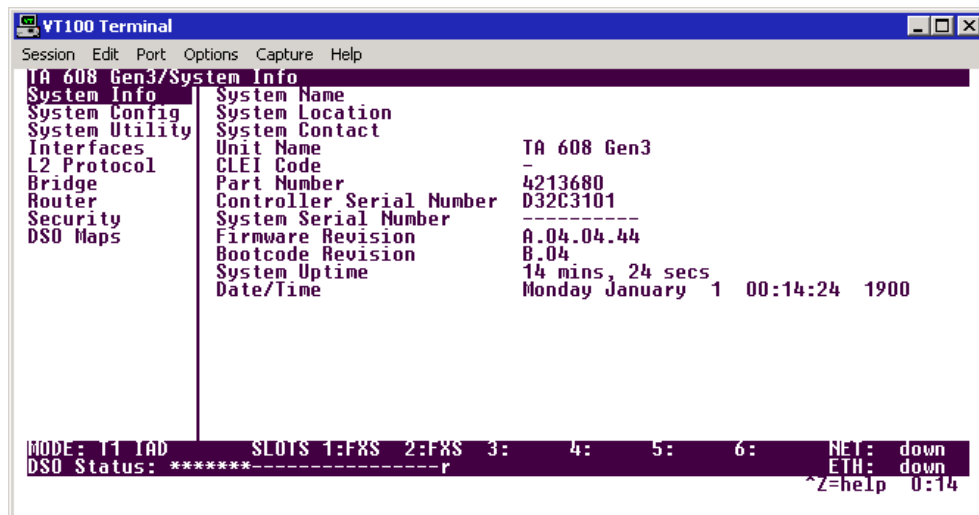

Perform the steps below in the order listed.

---

1. Connect the Total Access 6XX unit to your VT100 system (details found in DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*).

2. Log in to the system.

3. From the **ROUTER/CONFIG** menu, select the **INTERFACES** option and press **<Enter>**.

4. Select **SETUP** for the **ETH** interface, then **PRIMARY IP**.

5. Highlight the **IP ADDRESS** field and press **<Enter>**. Enter the appropriate IP address (as given by your system administrator).

6. Highlight the **SUBNET MASK** field and press **<Enter>**. Enter the appropriate subnet mask (as given by your system administrator).

7. Use the left arrow key to back out to the **ROUTER/CONFIG** menu. Select **ROUTES** and press **<Enter>**. Use the arrow key to highlight the **DEFAULT GATEWAY** field and press <Enter>. Enter the appropriate default gateway (as given by your system administrator).

8. Press the left arrow key to back out to the main **ROUTER** menu. This action saves your changes and requires confirmation.

> **NOTE**
>
> *The presence of an asterisk in the lower right corner of the menu window indicates that changes have NOT been saved to flash memory. Changes are automatically saved to flash as the user backs out of the menu system or after a manual save (by pressing **<CTRL+W>**. Always ensure that the asterisk is not present before logging off the system. Failure to save changes could result in a configuration loss if a power failure occurs. (For more details on the asterisk indicator, refer to Config Status on page 45.*

9. Log off the system by pressing **<CTRL+L>**.

DLP-4   Verifying Communications Over an IP LAN

Introduction

When the Ethernet port is connected to a local area network (LAN), test steps must be performed on the Total Access 6XX to ensure that the unit is communicating properly over the network. This procedure outlines those steps.

Prerequisite Procedures

Before beginning this procedure, the unit should be physically connected to the LAN and the provisioning tasks detailed in DLP-3, *Setting IP Parameters*, should be complete.

Tools and Materials Required

• Access to a PC or other computer connected to the LAN

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

1. Verify the Total Access 6XX IP address.

   If you do not already have the IP Address for the Total Access 6XX, obtain it from the network administrator or manually check for the address in the **ROUTER CONFIG/INTERFACE/SETUP/PRIMARY IP/IP ADDRESS** menu of the Network Management interface.

> **NOTE**
>
> *You must log in with a security level of 2 to modify the IP parameters on the Total Access 6XX. (See DLP-2, Logging in to the System, for more details.)*

---

2. Ping the Total Access 6XX unit from a remote computer on the network.

   Using a remote computer system connected to the LAN, perform an ICMP Ping on the IP Address of the Total Access 6XX. Verify that the unit responds properly.

   If the Total Access 6XX fails to respond, try the following:

   - Verify that the proper IP Address, Subnet Mask, and Default Gateway are provisioned in the unit (see DLP-2, *Logging in to the System*, for details).
   - Verify that the Total Access 6XX is properly cabled into the LAN and that the Ethernet cable is properly seated in the RJ-45 10/100BaseT interface on the rear of the unit.
   - Verify the link light on the front panel is lit. If not lit, check the cabling between the hub and the shelf.
   - If the Total Access 6XX is connected to a hub or other network device that provides a carrier sense light for each port, verify that the carrier sense light for the port to which the Total Access 6XX is connected is lit. If this light is not lit, check the cabling between the hub and the shelf.
   - Verify the IP Address, Subnet Mask, and Default Gateway on the remote computer system.
   - Use Ethernet straight-through cable for connection to hub or switch. Use Ethernet crossover if connecting directly to a PC without using a hub.

   If none of these steps are successful, contact the LAN Administrator for assistance.

> **NOTE**
>
> *Refer to the documentation of the computer system if you are unsure how to perform a Ping command. Most computers running a networked version of Microsoft Windows™ or UNIX allow a Ping to be performed by simply typing **ping <IP Address>** at a command line prompt. Typically, the Ping program will respond by indicating that the remote IP Address has responded in a certain amount of time or that no response was received.*

> **NOTE**
>
> *Some versions of Ping will continue running until you explicitly tell them to stop. If the program does not terminate on its own, press **<CTRL+C>** to get the program to stop.*

---

3. Telnet to the Total Access 6XX.

From the same computer used in the previous step, Telnet to the Total Access 6XX and verify that the Telnet session is properly opened (see DLP-5, *Connecting to the Unit Using Telnet*). Once the Telnet session is established, press **<CTRL+L>** to logout and close the session.

> **NOTE**
>
> *Refer to the documentation of the computer system if you are unsure how to perform a Telnet. Most computers running a networked version of Microsoft Windows™ or UNIX allow a Telnet to be performed by simply typing* **Telnet <IP Address>** *at a command line prompt. Telnet is a utility common on many local area networks that allows remote access to another computer or piece of equipment.*

DLP-5   Connecting to the Unit Using Telnet

Introduction

NOTE	*The Total Access 6XX comes pre-programmed for default Telnet access. The following IP parameters apply:* • IP Address: 10.0.0.1 • Subnet Mask: 255.255.255.0 • User: guest • Password: password *For security purposes, change the default Telnet password during the initial unit configuration. (Refer to System Config > Management > Telnet Access > User List on page 53 for more details.)*

If the Total Access 6XX is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. This procedure details the steps which must be performed to Telnet into the unit.

Prerequisite Procedures

Complete DLP-3, *Setting IP Parameters* and DLP-4, *Verifying Communications Over an IP LAN*.

Tools and Materials Required

• Access to a PC or other computer connected to the LAN.

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

1. Connect the computer to the Total Access 6XX **CRAFT** interface (details in DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*).

2. Log in to the unit.

3. Select the **SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS** menu and set the **TELNET ACCESS** to **ON**.

4. Under the **SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS** menu, select the **TELNET USER LIST**; press **<Enter>**. The following screen appears.

```
VT100 Terminal                                                _ □ ×
Session  Edit  Port  Options  Capture  Help
TA 608 Gen3/System Config/Management/Telnet Access/User List
User List         #      Name        Password     Idle Time(mins)   Level
Active Sessions   1      guest       *******            10          Full
IP Access List




















MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:     4:     5:     6:      NET:  down
DSO Status: *******---------------r                                 ETH:  down
                                                            ^Z=help  0:05
```

5. Use the right arrow key to select the NAME field; press **<Enter>**. All new Telnet entries have a **INACTIVE** as the **NAME**. Enter a specific username to use for Telnet login. Each Telnet entry in the list must have a unique assigned name because duplicate names are not allowed.

6. Use the right arrow key to select **PASSWORD**; press **<Enter>**. Enter a password to use for Telnet logins.

7. Use the right arrow key to select **IDLE TIME (MINS)**; press **<Enter>**. This field defines the amount of time in minutes the Telnet session may be idle before the user is logged off. The range is 1-255 and the default value is 10 minutes. Enter the appropriate **IDLE TIME**.

8. Use the right arrow key to select **LEVEL**; press **<Enter>**. Select the appropriate security level. (Reference DLP-6, *Adding/Removing Users and Changing Password Security Levels*, for security level definitions.)

9. This completes the addition of one Telnet user. Repeat steps 1-11 for each additional Telnet user access.

10. Press the left arrow key to escape out to the main menu. This saves your changes.

> **NOTE**
>
> *The presence of an asterisk in the lower right corner of the menu window indicates that changes have NOT been saved to flash memory. Changes are automatically saved to flash as the user backs out of the menu system or after a manual save (by pressing **<CTRL+W>**. Always ensure that the asterisk is not present before logging off the system. Failure to save changes could result in a configuration loss if a power failure occurs. (For more details on the asterisk indicator, refer to Config Status on page 45.)*

11. Press **<CTRL+L>** to log off the Total Access 6XX terminal menu system.

12. From a remote computer system connected to the LAN, Telnet to the Total Access 6XX.

> *Refer to the documentation of the computer system if you are unsure how to perform a Telnet. Most computers running a networked version of Microsoft Windows™ or UNIX allow a Telnet to be performed by simply typing "Telnet <IP Address>" at a command line prompt. Telnet is a utility common on many local area networks that allows remote access to another computer or piece of equipment.*

The following screen appears.
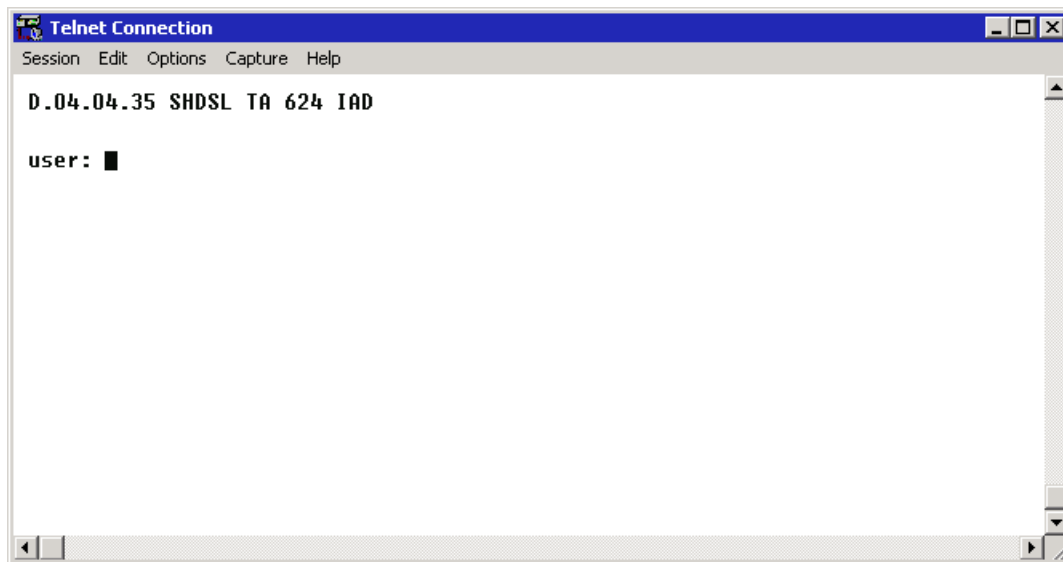
13. Enter the user name assigned in step 5 and press enter. The following screen appears.
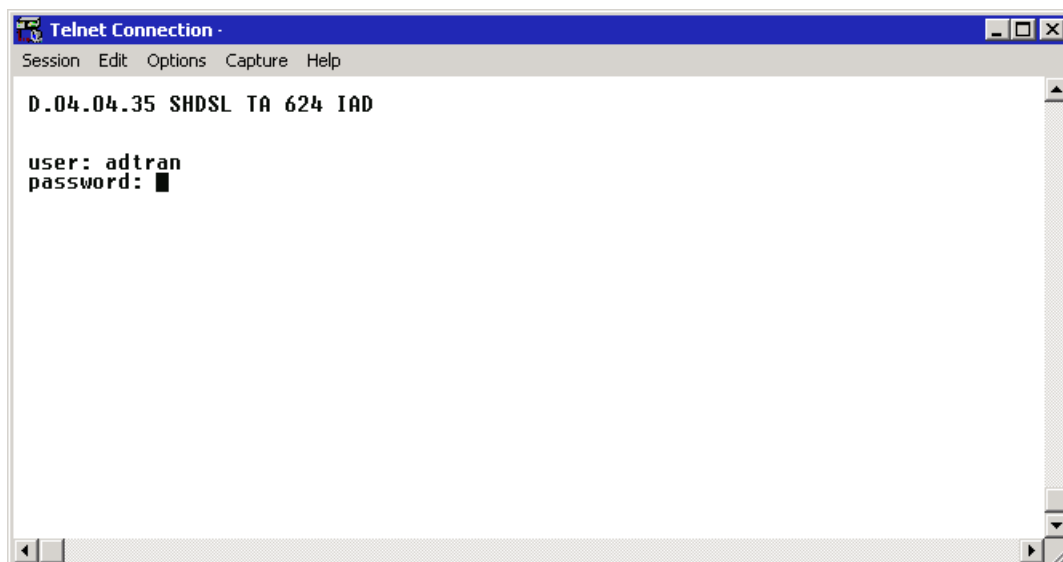
14. Enter the password assigned in step 6.

After entering the correct password, the Total Access 6XX main menu is displayed (see below):

```
VT100 Terminal                                                        _ □ X
Session  Edit  Port  Options  Capture  Help
TA 608 Gen3/System Info
System Info    System Name
System Config  System Location
System Utility System Contact
Interfaces     Unit Name                    TA 608 Gen3
L2 Protocol    CLEI Code                    -
Bridge         Part Number                  4213680
Router         Controller Serial Number     D32C3101
Security       System Serial Number         ----------
DSO Maps       Firmware Revision            A.04.04.44
               Bootcode Revision            B.04
               System Uptime                14 mins, 24 secs
               Date/Time                    Monday January  1  00:14:24  1900




MODE: T1 IAD      SLOTS 1:FXS  2:FXS  3:    4:    5:    6:        NET:  down
DSO Status: *******----------------r                             ETH:  down
                                                                ^Z=help  0:14
```

15. After completing your configuration changes they are automatically saved (or manually save them by pressing **<CTRL+W>**), press **<CTRL+L>** to log off the menus, and close the Telnet window.

DLP-6 Adding/Removing Users and Changing Password Security Levels

Introduction

	*Password security levels only apply to users connecting to the Total Access 6XX system through Telnet access. All connections made through the **CRAFT** interface ALWAYS have maximum security rights.*
NOTE	

All menu items in the Total Access 6XX are protected by passwords of varying security levels. By assigning different passwords to different security levels, the Total Access 6XX System Administrator can control which users can view or change various menu items. You can assign multiple passwords at the same access level. This way, different users with the same access privileges can have different passwords. This procedure details the steps which must be performed to add/remove user profiles and assign password security levels in the Total Access 6XX.

Tools and Materials Required

- VT100 compatible terminal or PC with VT100 terminal emulation software

	To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.
WARNING	

	Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.
CAUTION	

Perform the steps below in the order listed.

1. Connect to the Total Access 6XX using either the **10/100BASET** or **CRAFT** interface.

    If you are not already connected to the unit's **CRAFT** interface (either with a VT100 compatible terminal or with a PC running VT100 emulation software), follow the procedure in DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*).

    Alternately, if the unit is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. Use the procedures in DLP-3, *Setting IP Parameters*, and DLP-5, *Connecting to the Unit Using Telnet*, to connect to the **10/100BASET** interface.

2. Log in to the unit using the read-write password (see DLP-2, *Logging in to the System*, for more details).

> NOTE
>
> *Password security levels only apply to users connecting to the Total Access 6XX system through Telnet access. All connections made through the **CRAFT** interface ALWAYS have maximum security rights.*

3. Go to the **SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS** menu, select the **USER LIST** menu, and press **<Enter>**.

4. Add a new user profile and password by selecting the first column (0) and pressing **<I>** (for insert).

5. Give the new user profile a name by selecting the **NAME** field, pressing **<Enter>**, and typing the user defined name. All new Telnet entries have a **INACTIVE** as the **NAME**. Enter a specific username to use for Telnet login. Each Telnet entry in the list must have a unique assigned name because duplicate names are not allowed. Refer to *System Config > Management > Telnet Access > User List* on page 53 for more details.

6. Personalize the password for the appropriate level by selecting the **PASSWORD** field, pressing **<Enter>**, then typing the appropriate password. You will have to type the new password again to confirm it.

    Passwords for the Total Access 6XX system are case sensitive. There is no default password for a new user (i.e., you can configure a user as blank with no password). The current password displays as a series of asterisks (********).

7. Select the **IDLE TIME** field and press **<Enter>**. This field defines the amount of time in minutes the session may be idle before the user is logged off. The range is **1-255** and the default value is **10**.

8.   Determine the password level for the corresponding label. The Total Access 6XX contains seven
     different password levels. The following chart gives a brief description of each level.

Select Level...	If you want the user to....
STATUS	Have read-only permission for all menu items - **minimum rights**.
VOICE	Have read permission for all menu items and permission to use test commands.
ROUTER	Have access to all commands except passwords, flash download, authentication methods, interface configurations, and Telnet security levels.
CONFIG	Have access to all commands except passwords, flash download, authentication methods, and Telnet security levels.
SUPPORT	Have access to all commands except passwords and Telnet security levels.
FULL	Have permission to edit every menu item, including creating and editing passwords -- **maximum rights**.
ROUTER ONLY	Have read access to all menu items and write access to only the router menu.

9.   Assign the password level to the appropriate label by selecting the **LEVEL** field and choosing the level
     decided upon in Step 8.

DLP-7 Updating the Firmware using TFTP

Introduction

The Total Access 6XX supports firmware updates using TFTP or XMODEM. (Use the **10/100BASET** Ethernet port and TFTP from a network server, or use XMODEM and the rear **CRAFT** interfaces.) This DLP provides the steps for a successful firmware upgrade using the **10/100BASET** Ethernet port and a TFTP server. (See DLP-8, *Updating the Firmware using XMODEM*, for instructions on using XMODEM.)

Tools and Materials Required

- A PC with Telnet client software
- A TFTP server accessible on the local network

NOTE	*A TFTP server is provided as part of the ADTRAN Utilities software suite supplied with your shipment.*

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

1. Connect to the Total Access 6XX using the **10/100BASET** interface.

   If you are not already connected to the unit's **ETHERNET** port using Telnet client software, use the procedure in DLP-5, *Connecting to the Unit Using Telnet*, to connect to the unit.

2. Log in to the unit using the read-write password (see DLP-2, *Logging in to the System* for details).

3. Verify the TFTP server is running on the network. The user may ping the TFTP server from the Total Access 6XX to verify communication.

> **NOTE**
> *A TFTP server ships as part of the ADTRAN Utilities. If using ADTRAN Utilities, choose* **START > PROGRAMS > ADTRAN UTILITIES > TFTP SERVER** *to start the server.*

4. Download the firmware upgrade file to your computer.

> **NOTE**
> *If using ADTRAN Utilities, save the upgrade file to the* **"ADTNUTIL"** *directory on your hard drive.*

5. Go to the **SYSTEM UTILITY** menu and select the **UPDATE FIRMWARE** menu; press **<Enter>**.

6. Go to the **TRANSFER METHOD** menu and select **TFTP**.

7. Set the **TFTP SERVER ADDRESS** to the IP address of the machine running the TFTP server program.

> **NOTE**
> *If using ADTRAN Utilities, this will be the IP address that appears in the* **TFTP SERVER STATUS** *window.*

8. Enter the filename of the update file into the **TFTP SERVER FILENAME** field. If the file is located in a directory other than **ADTNUTIL**, the entire path and filename are required.

9. Select **START TRANSFER** to start the update. Enter **Y** to confirm the upgrade.

Prior to the start of the upgrade, the transfer status will display **IDLE**. During the TFTP upload process, various status messages display in **CURRENT UPDATE STATUS** to indicate progress. The following table describes these messages.

Message	Meaning
Transferring... [X KB]	Indicates communication with the TFTP network server has been established and the update file is being transferred between the Total Access 6XX and the TFTP network server.
Flash Programmed Successfully	The unit has been upgraded successfully.
Loaded code ver x.x.x chksum = xxxx	Unit displays the version and checksum of the upgraded code.
Resetting	Unit is power cycling.
RECV Error	Unit will display this message if server filename is incorrect.
Can not start tftp client **Reload	Unit will display this message if TFTP server address is incorrect.
Transfer aborted	User has selected **ABORT TRANSFER**.

10. When the update has successfully completed, **FLASH PROGRAMMED SUCCESSFULLY** displays briefly in the **TRANSFER STATUS** field. This will be followed by a **LOADED CODE VER X.X.X CHKSUM = XXXX** message. Finally the **TRANSFER STATUS** field displays **RESETTING ...**

The Total Access 6XX will restart immediately and resume operation. After giving the unit sufficient time to reboot, the user may Telnet back into the unit and log in.

DLP-8   Updating the Firmware using XMODEM

Introduction

The Total Access 6XX supports firmware updates using TFTP or XMODEM. (Use the **10/100BASET** Ethernet port and TFTP from a network server, or use XMODEM and the rear **CRAFT** interface.) This procedure outlines the steps for a successful firmware upgrade using the rear **CRAFT** interface and XMODEM software. (See *DLP-7, Updating the Firmware using TFTP*, for instructions on using TFTP.)

Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software
- XMODEM software (XMODEM capability is provided using the ADTRAN Utilities VT100 program).
- Appropriate cable to connect terminal to the Total Access 6XX (customer-provided).
- DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Updating Firmware via the Console Menus

Perform the steps below in the order listed.

1. Connect to the Total Access 6XX using **CRAFT** (RJ-48) interface. Selecting a higher baud rate connection makes the file transfer process faster. Verify that the baud rate setting on the Total Access 6XX matches the VT100 emulation software COM port settings.

   If you are not already connected to the **CRAFT** interface (either with a VT100 compatible terminal or with a PC running VT100 emulation software), follow the procedure in *DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port*. Connecting to the **CRAFT** interface limits the upgrade procedure to XMODEM only.

2. Log in to the unit.

3. Go to the **SYSTEM UTILITY** menu and select the **UPGRADE FIRMWARE** menu; press **<Enter>**.

4. Go to the **TRANSFER METHOD** menu and select **XMODEM**.

> **NOTE** *Total Access 6XX XMODEM transfers are compatible with both XMODEM and 1K XMODEM on the VT100 terminal system. Selecting 1K XMODEM on your terminal session will make the configuration transfer faster.*

5. Select **START TRANSFER** to start the update process. Enter **Y** to confirm the upgrade.

6. From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. If necessary, refer to the terminal emulation software documentation for help.

   Also, when specifying the filename, ensure that the file transferred is the one provided by ADTRAN, otherwise, the update will not complete successfully. This may take several minutes.

   Because XMODEM data is being transferred in-band through the menu interface, the VT100 menus of the Total Access 6XX will be inoperable from the **CRAFT** interface. You can cancel the update at any time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)

7. When the update process has successfully completed, the following messages will display:

   Verifying downloaded FLASH image...

   Erasing FLASH...

   Programming FLASH...

   FLASH programmed successfully.

   The Total Access 6XX will restart immediately and the user may then log back into the system.

   Alternately, if the unit is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. By utilizing the **ETHERNET** port, the Total Access 6XX may be quickly upgraded using TFTP, provided there is a TFTP server on the local network. The Total Access 6XX ships with ADTRAN Utilities software, which includes a TFTP server. See *DLP-7, Updating the Firmware using TFTP*, for more details.

DLP-9   Saving the Current Configuration Using TFTP

Introduction

The Total Access 6XX supports configuration transfers from the unit (via the **10/100BASET** Ethernet port) to a TFTP server located on the network. This DLP provides the steps to follow for a successful configuration transfer using the **10/100BASET** Ethernet port and a TFTP Server.

Tools and Materials Required

• A PC with a Telnet client software

• A TFTP Server accessible on the local network (A TFTP server is provided with the unit as part of the ADTRAN Utilities software.)

WARNING *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION *Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

1. Connect to the Total Access 6XX using the **10/100BASET** interface.

   If you are not already connected to the unit's **10/100BASET** port using Telnet client software, use the procedure in DLP-5, *Connecting to the Unit Using Telnet*, to connect to the unit.

2. Log in to the unit using the read-write password (see DLP-2, *Logging in to the System*, for details).

3. Verify the TFTP server is running on the network.

> ✎ **NOTE** *A TFTP server ships as part of the ADTRAN Utilities. If using ADTRAN Utilities, choose* **START > PROGRAMS > ADTRAN UTILITIES > TFTP SERVER** *to start the server.*

4. Go to the **SYSTEM UTILITY** menu and select the **CONFIGURATION TRANSFER** menu; press **<Enter>**.

5. Verify the **TRANSFER METHOD** is set to **TFTP**.

6. Set the **TFTP SERVER IP ADDRESS** to the IP address of the machine running the TFTP Server Program.

> ✋ **CAUTION** *If you are using the ADTRAN TFTP server, the IP address displays in the **STATUS** field. For other TFTP servers, please refer to the appropriate documentation.*

7. Change **TFTP SERVER FILENAME** to a unique filename (for example, **ta604.cfg**). This will be the name of the configuration file saved to the remote server.

   Some TFTP servers constrain the format of the filename depending on the operating system of the server. For example, a TFTP server running on a PC under Windows 3.1 may only permit 8.3 format filenames (8 characters, period and three extension characters).

8. Select the **SAVE CONFIG REMOTELY** menu field and press **<Enter>**. Respond with **Y** to confirm the request.

9. View **CURRENT TRANSFER STATUS** to verify the progress of the current transfer. During a successful transfer, you will first see **DOWNLOAD: COPYING INTERNAL CONFIG**, and then **DOWNLOAD IN PROGRESS....**

10. When the transfer process has successfully completed, **IDLE** displays in the **CURRENT TRANSFER STATUS** field and **DOWNLOAD COMPLETE** displays in the **PREVIOUS TRANSFER STATUS** field.

> **WARNING** *TFTP is **not** secure. No passwords are required for client access. Anyone can access files through the IP port on the server machine if they know the target filename.*

DLP-10 Loading a Configuration Using TFTP

Introduction

The Total Access 6XX supports configuration uploads from a unit (via the **10/100BASET** Ethernet port) to a TFTP server located on the network. This DLP provides the steps to follow for a successful configuration upload using the **10/100BASET** Ethernet port and a TFTP Server.

Tools and Materials Required

- A PC with a Telnet client software
- A TFTP Server accessible on the local network (A TFTP server is provided with the unit as part of the ADTRAN Utilities software.)

WARNING   *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION   *Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

1. Connect to the Total Access 6XX using the **10/100BASET** interface.

    If you are not already connected to the unit's **10/100BASET** port using Telnet client software, use the procedure in DLP-5, *Connecting to the Unit Using Telnet*, to connect to the unit.

2. Log in to the unit using the read-write password (see DLP-2, *Logging in to the System*, for details).

3. Verify the TFTP server is running on the network.

> **NOTE** *A TFTP server ships as part of the ADTRAN utilities. If using ADTRAN utilities, choose* **START > PROGRAMS > ADTRAN UTILITIES > TFTP SERVER** *to start the server.*

4. Go to the **SYSTEM UTILITY** menu and select the **CONFIGURATION TRANSFER** menu; press **<Enter>**.

5. Verify the **TRANSFER METHOD** is set to **TFTP**.

> **WARNING** *TFTP is **not** secure. No passwords are required for client access. Anyone can access files through the IP port on the server machine if they know the target file's name.*

6. Set the **TFTP SERVER IP ADDRESS** to the IP address of the machine running the TFTP Server Program.

> **CAUTION** *If you are using the ADTRAN TFTP server, the IP address displays in the **STATUS** field. For other TFTP servers, please refer to the appropriate documentation.*

7. Change **TFTP SERVER FILENAME** to a unique filename. (This will be the name of the configuration file retrieved from the remote server.) If the ADTRAN Utilities TFTP server is used and no path is specified, the configuration file is retrieved from the default **ADTNUTIL** directory. To retrieve a configuration file from a particular folder, enter the entire filename including path.

    Some TFTP servers constrain the format of the filename depending on the operating system of the server. For example, a TFTP server running on a PC under Windows 3.1 may only permit 8.3 format filenames (8 characters, period and three extension characters).

8. Select the **LOAD AND USE CONFIG** menu field and press **<Enter>**. Respond with **Y** to confirm the request.

9. View **CURRENT TRANSFER STATUS** to verify the progress of the current upload.

10. When the upload process has successfully completed, **IDLE** displays in the **CURRENT TRANSFER STATUS** field and **DOWNLOAD COMPLETE** displays in the **PREVIOUS TRANSFER STATUS** field.

DLP-11 Saving and Transferring a Current Configuration Using XMODEM

Introduction

The Total Access 6XX supports configuration transfers from the unit via the **CRAFT** interface using a VT100 terminal or terminal emulator (with XMODEM). This DLP provides the steps for a successful configuration transfer using the **CRAFT** port and XMODEM.

Tools and Materials Required

- VT100 terminal or PC with VT100 terminal emulation software
- XMODEM software
- Appropriate cable to connect terminal to the Total Access 6XX (customer-provided).
- DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

WARNING | *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION | *Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the following steps in the order listed.

---

1. Connect to the Total Access 6XX using the **CRAFT** (RJ-48) port on the back of the Total Access 6XX.

   If you are not already connected to the unit's rear **CRAFT** interface, either with a VT100 compatible terminal or with a PC running VT100 emulation software, follow the procedure in DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*. Connecting to the **CRAFT** interface limits the configuration transfer procedure to **XMODEM** only.

2. Log in to the unit.

3. Go to the **SYSTEM UTILITY** menu and select **CONFIGURATION TRANSFER** menu; press **<Enter>**.

4. Set the **TRANSFER METHOD** menu to **XMODEM**.

5. Select **SAVE CONFIG REMOTELY** to start the transfers. Enter **Y** to confirm the transfer and prepare the Total Access 6XX for the transfer download.

   The following message is displayed: **This will begin sending a copy of the current system configuration.**

6. Configure the VT100 terminal or terminal emulation software to **RECEIVE** (and prompt for a filename).

7. View the **CURRENT TRANSFER STATUS** to verify the progress of the current transfer.

8. From the terminal emulation software, begin the XMODEM transfer by using the appropriate command sequence. For Windows HyperTerminal, select **TRANSFER>RECEIVE FILE**. Enter the filename (including path) and select **XMODEM** as the transfer method.

   If necessary, refer to the terminal emulation software documentation for help.

   > **NOTE**
   > *When specifying the filename, ensure that the saved file has a .cfg extension; otherwise, the file may not be available for uploading into other Total Access 6XX units.*

   Because XMODEM data is being transferred inband through the menu interface, the VT100 menus of the Total Access 6XX will be inoperable from the **CRAFT** interface. You can cancel the update at any time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)

9. When the transfer has successfully completed, **IDLE** displays in the **CURRENT TRANSFER STATUS** field and **XMODEM DOWNLOAD COMPLETE** displays in the **PREVIOUS TRANSFER STATUS** field.

DLP-12 Loading a Configuration Using XMODEM

Introduction

The Total Access 6XX supports configuration uploads from a unit via the **CRAFT** interface using a VT100 terminal or terminal emulator (with XMODEM). This DLP provides the steps for a successful configuration upload using the rear **CRAFT** port and XMODEM protocol.

Tools and Materials Required

- VT100 terminal or PC with VT100 terminal emulation software
- XMODEM software
- Appropriate cable to connect terminal to the Total Access 6XX (customer-provided).
- DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

WARNING   *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION   *Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the following steps in the order listed.

1. Connect to the Total Access 6XX using the **CRAFT** (RJ-48) interface.

    If you are not already connected to the unit's rear **CRAFT** interface, either with a VT100 compatible terminal or with a PC running VT100 emulation software, follow the procedure in DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*. Connecting to the rear **CRAFT** interface limits the configuration transfer procedure to XMODEM only.

2. Log in to the unit using the read-write password (see DLP-2, *Logging in to the System*, for details).

3. Go to the **SYSTEM UTILITY** menu and select **CONFIGURATION TRANSFER** menu; press **<Enter>**

4. Set the **TRANSFER METHOD** menu to **XMODEM**.

5. Select **LOAD AND USE CONFIG** to start the transfer. Enter **Y** to confirm the transfer and prepare the Total Access 6XX for the transfer download.

    When the Total Access 6XX is ready to receive the XMODEM configuration file, the menu screen clears and displays **AWAITING XMODEM UPLOAD....<CTRL+X> TWICE TO CANCEL**. If this does not appear, please review the preceding steps above for possible configuration errors.

6. From the terminal emulation software, begin the XMODEM transfer by using the appropriate command sequence. For Windows HyperTerminal, select **TRANSFER>SEND FILE**. Enter the filename (including path) and select **XMODEM** as the transfer method. Total Access 6XX configuration files should have a .cfg extension.

    If necessary, refer to the terminal emulation software documentation for help.

    Because XMODEM data is being transferred inband through the menu interface, the VT100 menus of the Total Access 6XX will be inoperable during this procedure from the **CRAFT** interface. You can cancel the update at any time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)

7. View **CURRENT TRANSFER STATUS** to verify the progress of the current upload.

DLP-13 Saving and Loading Text Configuration using Terminal Command Line

Introduction

The Total Access 6XX has the ability to download a text file which contains the configuration of the entire unit. This configuration may then be altered in a text editor and uploaded to any Total Access 6XX.

This DLP will explain how to save and load the text configuration file for the ADTRAN Total Access 6XX.

Prerequisite Procedures

You must connect to the Total Access 6XX with a VT100 terminal session (reference DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*).

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

Saving the Total Access 6XX configuration

1. Establish a connection to the Total Access 6XX with the VT100 terminal software using the **CRAFT** port or Telnet via the **10/100BASET** Ethernet interface.

2. From the main menu, select **SYSTEM UTILITY**, then **TERMINAL MODE**; press **<Enter>**.

3. The following screen appears.

```
 Telnet Connection                                            _ □ ×
 Session  Edit  Options  Capture  Help
 >
```
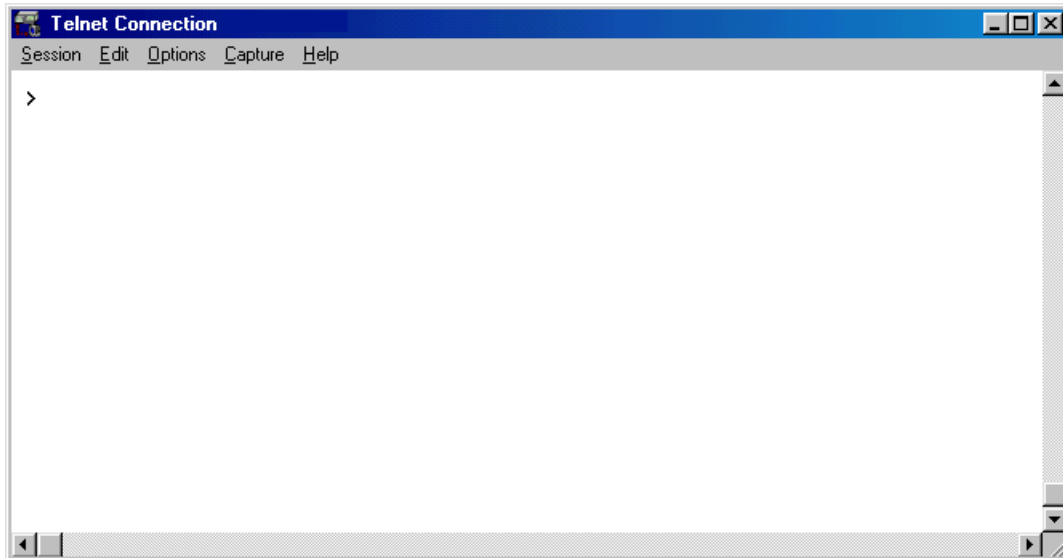
4. At the terminal prompt, type *DOWNLOAD*; press **<Enter>**. The following screen appears.

```
 Telnet Connection ·                                          _ □ ×
 Session  Edit  Options  Capture  Help
 >download
 Press any key to continue . . .
```
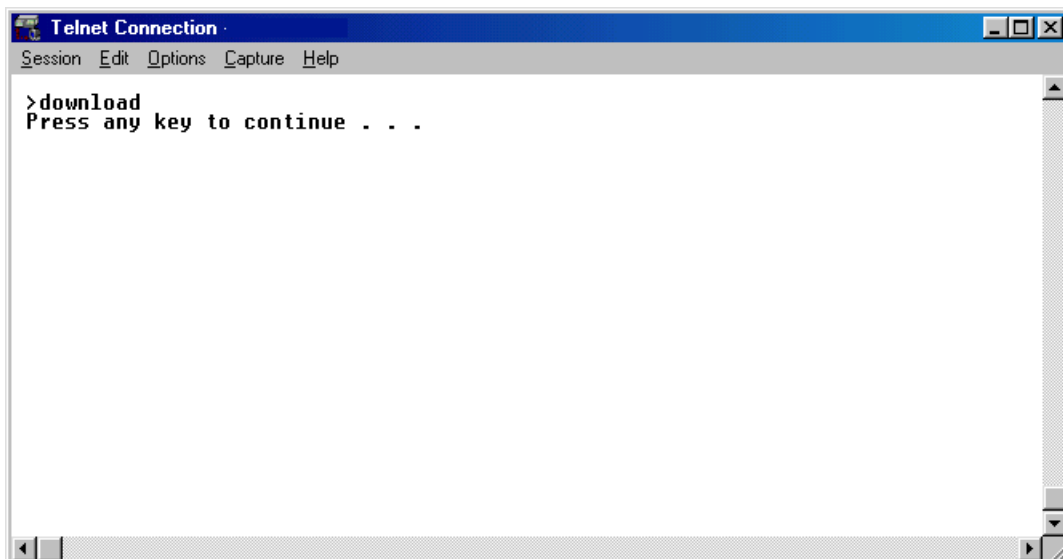
> **NOTE** *Do not enter further key commands until completing Step 5.*

5. Enable "capture" or "logging" in the terminal software, saving it to a file on your computer.

6. Press the *SPACE BAR* to continue. The unit prints its configuration to the terminal screen. (With capture enabled, the terminal software will capture the configuration and write it to the designated file.)

7. When the configuration stops printing, end the capture. The unit configuration is now saved to the designated file.

8. At the terminal prompt, type *EXIT* to enter the unit configuration menu.

> NOTE
> *Always use <CTRL+L> to exit the configuration menu before closing the Telnet or terminal software.*

Loading a configuration into the Total Access 6XX

The following steps explains the process for uploading the text file back into the Total Access 6XX. These text files can be the entire configuration, or just partial commands that affect specific configuration changes. The uploading steps are the same, regardless of the size of the file.

1. Establish a connection to the Total Access 6XX with the VT100 terminal software using the **CRAFT** port or Telnet via the **10/100BASET** Ethernet interface.

2. From the main menu, select **SYSTEM UTILITY**, then **TERMINAL MODE**; press **<Enter>**.

3. In the terminal software, initiate a SEND TEXT FILE or SEND CFG FILE using the saved configuration file.

4. Once the file transfer is complete, type *SAVE* to save the configuration in the unit. Type *EXIT* to enter the unit configuration menu.

> NOTE
> *Always use <CTRL+L> to exit the configuration menu before closing the Telnet or terminal software.*

Entering commands at the command prompt

Precede each instruction with a ">" when manually entering commands at the command prompt. After entering commands, type *SAVE* at the command prompt. (This applies ALL commands to current operation and saves all changes.) To save the changes to flash only (without affecting current operation), return to the menu system and press <**CTRL+W**>.

The commands are based on string comparisons with the menu system (with spaces replaced with underscores). For example, the config command appears at the command prompt exactly as it appears in the Total Access 6XX terminal menus. To change a configuration, type in the desired option exactly as it appears on the menu. For example, to change the T1 timing mode, the command line should read

>interfaces t1 config timing_mode network (sets timing to recover from the network) **or**

>interfaces t1 config timing_mode internal (sets timing to internal Total Access 6XX oscillator) **or**

>interfaces t1 config timing_mode dsx-1 (sets timing to recover from the DSX-1 interface).

DLP-14 A.03 to A.04 Firmware Upgrade

Introduction

The Total Access line of Integrated Access Devices includes both the ATM and TDM versions of the Total Access 6XX. Until now, the Total Access TDM units have been running firmware version A.03.xx. Recently, A.04.xx has been released to support the TDM Total Access IADs. The development of A.04.xx code is a significant step in the evolution of the Total Access product line, as it allows all Total Access family members to share the same base code. This means that features and fixes are more easily implemented and are propagated across the product line.

The two possible A.03 to A.04 upgrade paths are described in this DLP.

> **CAUTION** *The choice of upgrade path will determine whether the unit's configuration is saved.*

> **NOTE** *Since the A.03 and A.04 firmware loads are significantly different, the text configuration files for the two revisions are also different. It is recommended that the customer save a text configuration file for both the A.03 revision (prior to the upgrade) and for the A.04 revision (after completion of the upgrade). Refer to DLP-9, Saving the Current Configuration Using TFTP, DLP-11, Saving and Transferring a Current Configuration Using XMODEM, or DLP-13, Saving and Loading Text Configuration using Terminal Command Line, for further instructions on how to save the configuration.*

> **WARNING** *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

Prerequisite Procedures

Obtain the A.04 firmware and the A.03.92 (Transition Build) firmware from the ADTRAN website (http://www.ADTRAN.com).

> **NOTE** *For the Total Access 6XX units, select **SERVICE/SUPPORT > TECHNICAL SUPPORT > TOTAL ACCESS PRODUCTS > TOTAL ACCESS 600**.*

If further assistance is required, contact ADTRAN Technical Support at 1-888-4ADTRAN.

Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the unit (customer-provided)
- DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

Perform the steps below in the order listed.

Upgrade From A.03 to A.03.92 (Transition Build) to A.04

1. Upgrade the firmware from A.03 to A.03.92 (Transition Build) firmware. See DLP-7 (TFTP) or DLP-8 (XMODEM) for instructions on how to perform this upgrade.

2. Once the upgrade to A.03.92 is complete, immediately upgrade the unit to A.04. See DLP-7 (TFTP) or DLP-8 (XMODEM) for instructions on how to perform this upgrade.

> **NOTE**   *Upgrading from A.03 to A.03.90 (Transition Build) to A.04 will save the unit's configuration.*

Upgrade From A.03 to A.04 Directly

1. Upgrade the firmware from A.03 to A.04 firmware. See DLP-7 (TFTP) or DLP-8 (XMODEM) for instructions on how to perform this upgrade.

2. The unit must then be factory defaulted by one of the following methods:

   - Select **SYSTEM UTILITY>TERMINAL MODE.** At the > prompt, type **fac**. You will then see "Restore Factory Defaults and Reset Unit? (press 'y')." Press the **y** key to confirm default. The unit will then automatically reset.

3. Reconfigure the unit for the specific application.

> **NOTE**   *Upgrading from A.03 to A.04 directly (or from A.04 to A.03 directly) will erase the unit's configuration.*

DLP-15 Using the ADTRAN Utility Syslog

Introduction

The Total Access 6XX Syslog Utility records various message types at settable threshold levels to an external Syslog server (software supplied with the Total Access 6XX system ADTRAN Utilities).

Prerequisite Procedures

This procedure assumes that the Total Access 6XX unit is connected to an IP network and is powered up.

Tools and Materials Required

• Syslog server (provided on Total Access 6XX System CD in ADTRAN Utilities)

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Setting up the Total Access 6XX to use Syslog:

1. Log in to the system with maximum rights (see DLP-2, *Logging in to the System*). Once you have logged into the Total Access 6XX, go to **SYSTEM CONFIG/SYSLOG**. Set the options as follows:

    • **SYSLOG IP**: Enter the IP address of the PC where the Syslog host resides

    • **SYSLOG FORMAT**: Specify the Syslog format as either **ADTRAN** (to work with ADTRAN Utilities) or **UNIX** (to work with a standard UNIX Syslog server)

    • **SYSLOG FACILITY**: Specify the facility destination of log events; Options are **LOCAL0** to **LOCAL7**

Setting Up the Syslog Host:

1. On your PC, go to **START/PROGRAMS/ADTRAN UTILITIES/SYSLOG**. When the Syslog window opens, you will see **LOCAL0** through **LOCAL7** listed on the left. This should correspond with the **HOST FACILITY** specified in the Total Access 6XX. The Syslog program must be open on your PC in order for it to record Total Access 6XX information. The Syslog files can be viewed through the Syslog window, and they are also available under the ADTRAN Utilities Folder named **LOCALX.TXT**, where X can equal 0 through 7. You can also view the **LOCALX.TXT** file by clicking on **EDIT LOG**.
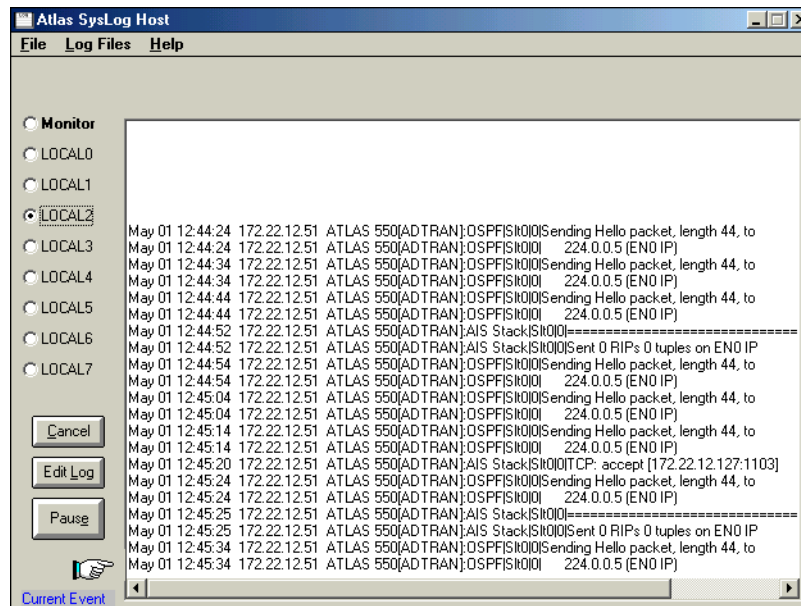
Additional Syslog Features:

- The **MONITOR** feature allows all Syslog messages to be prefiltered by **SYSTEM NAME**, **SOURCE**, **SLOT**, and **PORT** before displaying these messages to the user and logging the message to the pre-designated monitor log file. Various filter options may be defined by selecting **SOURCE**. The figure below shows the **SOURCE FILTER** window. When the **MONITOR** button is selected, the file will be logged to **LOCAL8.TXT**. To look at the text file, click on the **EDIT LOG** button on the left side of the Syslog screen. Only the **SOURCE** options that are selected with an 'x' will be displayed in the Syslog file. In this example, all options are displayed.
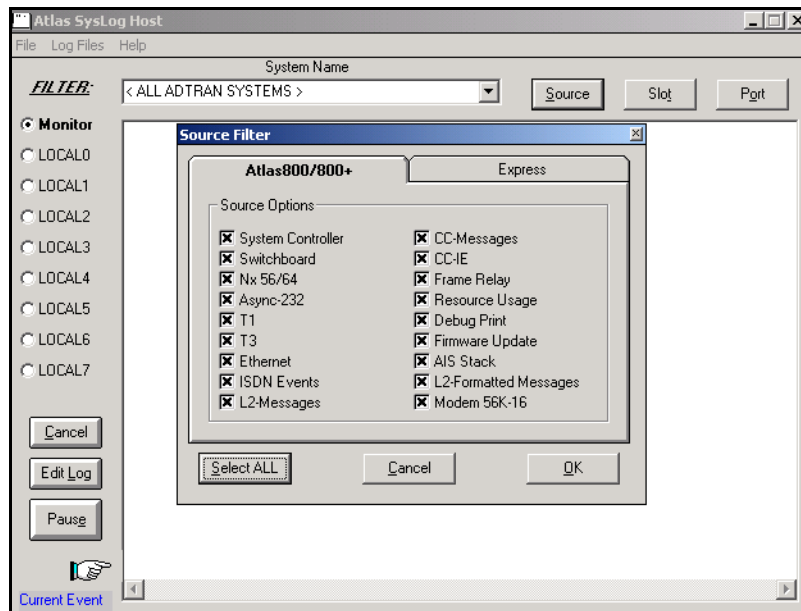
- Under the **LOG FILES** menu option, the user may erase log files, define Red events, set priorities, and clear Red events. The **ERASE LOG FILES** option erases the specified text log file.

  - **DEFINE RED EVENTS** allows the user to predefine a message priority condition so that if the condition occurs, the file is highlighted in red. In the figure below, any **CRITICAL** or **MAJOR** condition causes any **LOCAL0** through **LOCAL7** facility to become highlighted in red if it receives a critical or major alarm.
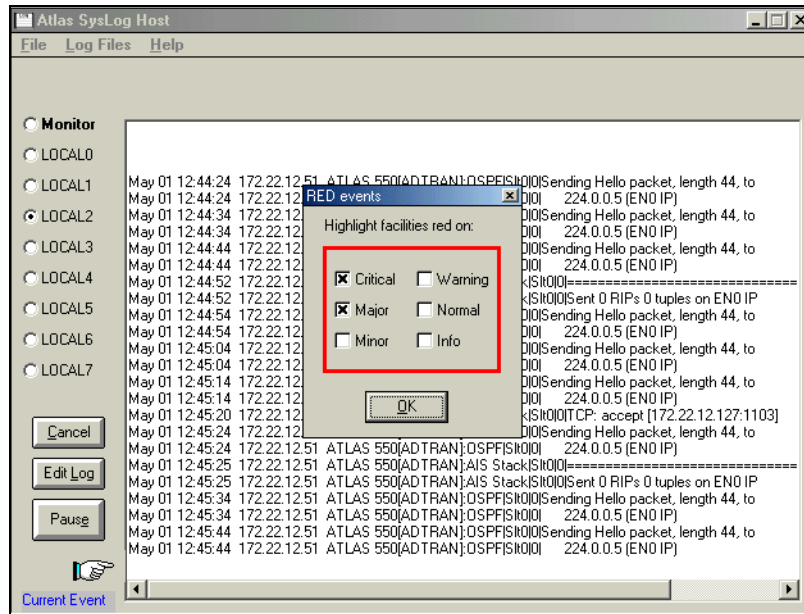
- The **PROPERTIES** menu allows the user to specify the types of messages to be logged to an ASCII text file. Mark the lowest priority Syslog message you want to log to the Syslog server text file. For example, the figure below shows that all messages will be logged to the text file.
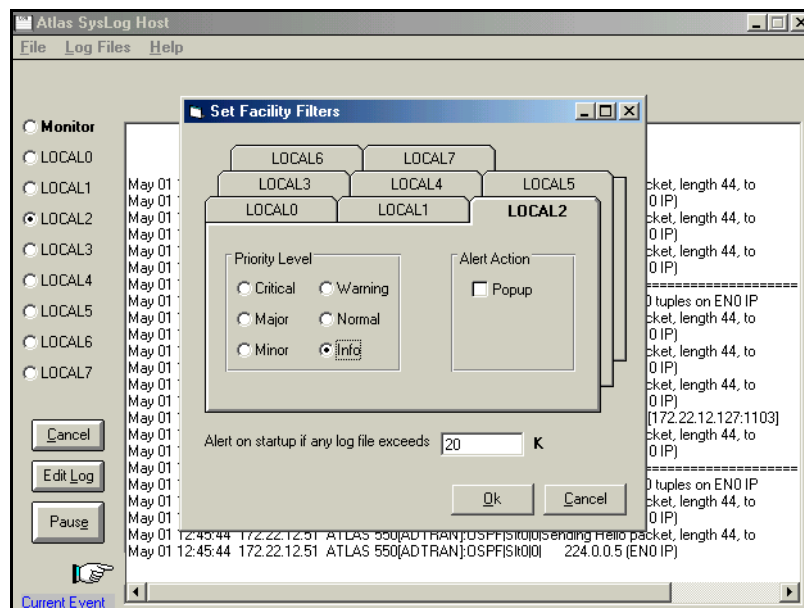
- The **HELP** menu also explains these features. Click on **HELP/CONTENTS/SYSLOG HOST DAEMON** for further explanation of Syslog features.

DLP-16 Executing Terminal Mode Commands

Introduction

Once connected to the unit via either a VT100 terminal or PC configured as a VT100 terminal or via Telnet using the **10/100BASET** interface, selecting the terminal mode gives the user a command-line prompt to perform utilities such as pings, traceroutes, resets, firmware updates, configuration, and more. **TERMINAL MODE** can also be accessed by using the shortcut keys **<Ctrl + T>** from other menu screens.

Prerequisite Procedures

Complete DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*, before logging in to the unit.

Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software. A VT100 emulation program is provided with your shipment as part of the ADTRAN Utilities software suite.
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided).
- DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

---

1. Connect to the unit using either the **10/100BASET** or **CRAFT** interfaces.

    If you are not already connected to the unit's **CRAFT** interface (either with aVT100 compatible terminal or with a PC running VT100 emulation software), follow the procedure in DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*.

    Alternately, if the unit is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. Use the procedures in DLP-3, *Setting IP Parameters*, and DLP-5, *Connecting to the Unit Using Telnet*, to connect to the **10/100BASET** interface.

2. Log in to the unit (see DLP-2, *Logging in to the System*, for details).

3. Go to **SYSTEM UTILITY > TERMINAL MODE** and press **<Enter>**. From this prompt you can:

    a. Perform a reset with the command **reset**

    b. Perform a factory restore with the command **factory_reset**

    c. Configure the unit. The unit has the ability to download a text file which contains the configuration of the entire unit. This configuration may then be altered in a text editor, and then uploaded to a unit.

    d. Debug and troubleshoot. This function would be carried out with the assistance of ADTRAN Technical Support.

    e. Start and stop the fail-safe time for the auto-config feature.

    > **fs_timer start x** (**x** is in seconds) OR **fs_timer stop**

    f. Perform a firmware upgrade via TFTP.

    > **upgrade_firmware** *hostname filename*

    g. Use the **save** command to write the entire configuration flash.

    h. Display the unit's MAC address with the command **mac**.

    i. Perform a ping or extended ping. Syntax is:

    > **ping hostname/address [repeat xx] [size xx] [timeout xx] [source xx] [no Nat]**

    Options:

repeat <repeat count>	Number of pings to send (default 5)
size (datagram size)	Range is 40-1500
timeout (seconds)	Timeout in seconds (range 1-10)
source (address or name)	Source address or interface name to use
noNat	Do not NAT the ping packet

    Options may be entered in any order and may be truncated.
    Valid interface names are eth0, fdl0, ppp0, fr0, fr1, etc.

    Example usage: **ping 10.0.0.5 r 10 si 1500 so eth0 n**

    This will ping with a repeat count of 10. The datagram size is 1500 bytes, and the source address used in the ping packet will be the ethernet IP address. The "noNat" option has been specified, so if NAT is enabled, this packet will NOT be translated.

---

j. Perform a traceroute or extended traceroute. Syntax is:
    traceroute hostname/address [hops xx] [timeout xx] [retries xx] [source xx] [noNat]

    Options:

hops <hops count>	Max number of hops (default 30)
timeout <seconds>	Timeout in seconds (default 3)
retries <seconds>	Number of retries per hop (default 3)
source <address or name>	Source address or interface name to use
noNat	Do not NAT the trace packets

    Options may be entered in any order and may be truncated.

    Valid interface names are eth0, fdl0, ppp0, fr0, fr1, etc.

    Example usage: **trace 10.0.0.5 h 20 t 1 r 1 so eth0**

    This will perform a trace to 10.0.0.5 with a max hop count of 20. The timeout for each hop is 1 second, and the retry count per hop is 1. The Ethernet IP will be used as the source address, and the packet WILL go through NAT if NAT is enabled, meaning that the packet will be translated and the source address will be replaced by the NAPT address.

k. Use the Telnet client feature to Telnet to a remote host. Syntax is:
    Telnet hostname/address [port xx]

Default port is 23 (TELNET).

l. To exit terminal mode, type **exit** or **!exit**,
    exit – if any configuration have been made, you will be prompted whether or not to save these changes. If no changes were made, the terminal session will exit without the confirm message.

    !exit – exit without saving or applying any configuration changes.

> **NOTE** *Extended ping, extended traceroute, and Telnet client are new features initially available in A.04.02. These functions may be performed simultaneously from multiple user sessions.*

DLP-17 Configuring Dual T1 Maps

Introduction

Total Access 6XX T1 TDM systems with the optional DSX-1 interface have a **DUAL T1 MAP** feature that allows two network T1 connections for the termination of data and voice applications. The primary network **T1 MAP** can be configured for internal router usage (FT1/24 DS0s maximum) or any other interfaces. The **DSX MAP** can be used for FXS/FXO interfaces. There are several steps that must be followed in order for the Dual T1 Map to be configured successfully. These steps are described in this DLP.

Prerequisite Procedures

This procedure assumes that the user has access to the Total Access 6XX system menus and has completed the T1 and DSX-1 interface configuration (as detailed in *Appendix D. Configuring the Unit for DSX-1 Applications* on page 166).

NOTE	*Refer to DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port, for details on making a terminal connection to the Total Access 6XX.*

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

1. Connect the Total Access 6XX unit to your VT100 system (details found in DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*).

2. Log in to the system with maximum rights (details are in DLP-2, *Logging in to the System*).

3. From the **DS0 MAPS** menu, select the **ACTIVE MAP** option and press **<Enter>**.

4. From the **DS0 MAPS > ACTIVE MAPS** menu, select the **DUAL T1 MAP** option; press **<Enter>**. Select "Y" for yes to confirm the Active Map change and press **<Enter>**. The following screen appears.

> ✎ NOTE
> *The second T1 connected to the DSX port may only be used for voice connections (FXS/FXO).*

```
TA 608 Gen3/DS0 Maps/Active Map
System Info    x Active Map          Dual T1 Map
System Config x Edit/View T1 Map    [+]
System Utilityx Edit/View DSX Map   [+]
Interfaces     x
L2 Protocol    x
Bridge         x
Router         x
Security       x
DS0 Maps       x
               x
               x
               x
               x
               x
               x
               x
               x
               x
               x
MODE: T1 IAD        SLOTS 1:FXS  2:FXS  3:      4:      5:      6:      NET:  down
DS0 Status: *******---------------r                                    ETH:  down
                                                                       ^Z=help 23:45_
```

Figure 1. Dual T1 Map

5.   Edit the Primary T1 Map by pressing **<Enter>** on **EDIT/VIEW T1 MAP [+]**.The following screen appears.

```
TA 608 Gen3/DS0 Maps/Edit/View T1 Map
Edit/View T1 Map ×  DS0  Service        Port        Rbs
Edit/View DSX Map×   1    TA IAD     V.35 64K      n/a
                ×   2    TA IAD     V.35 64K      n/a
                ×   3    TA IAD     V.35 64K      n/a
                ×   4    TA IAD     V.35 64K      n/a
                ×   5    TA IAD     V.35 64K      n/a
                ×   6    TA IAD     V.35 64K      n/a
                ×   7    TA IAD     V.35 64K      n/a
                ×   8     open        n/a         n/a
                ×   9     open        n/a         n/a
                ×  10     open        n/a         n/a
                ×  11     open        n/a         n/a
                ×  12     open        n/a         n/a
                ×  13     open        n/a         n/a
                ×  14     open        n/a         n/a
                ×  15     open        n/a         n/a
                ×  16     open        n/a         n/a
                ×  17     open        n/a         n/a
                ×  18     open        n/a         n/a
                ×  19     open        n/a         n/a
MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:    4:    5:    6:    NET:  down
DS0 Status: *******---------------r                           ETH:  down
                                                            ^Z=help 23:49_
```

Figure 2. Primary T1 Map

NOTE   *The T1 Map can be mapped to the internal router or other available interfaces.*

6.   Edit the Secondary T1 Map (DSX Map) by pressing **<Enter>** on **EDIT/VIEW DSX MAP [+]**. The following
     screen appears.

```
TA 608 Gen3/DS0 Maps/Edit/View DSX Map
Edit/View T1 Map  ×  DS0   Service       Port        Rbs
Edit/View DSX Map×    1      open         n/a         n/a
                  ×    2      open         n/a         n/a
                  ×    3      open         n/a         n/a
                  ×    4      open         n/a         n/a
                  ×    5      open         n/a         n/a
                  ×    6      open         n/a         n/a
                  ×    7      open         n/a         n/a
                  ×    8      open         n/a         n/a
                  ×    9      open         n/a         n/a
                  ×   10      open         n/a         n/a
                  ×   11      open         n/a         n/a
                  ×   12      open         n/a         n/a
                  ×   13      open         n/a         n/a
                  ×   14      open         n/a         n/a
                  ×   15      open         n/a         n/a
                  ×   16      open         n/a         n/a
                  ×   17      open         n/a         n/a
                  ×   18      open         n/a         n/a
                  ×   19      open         n/a         n/a
MODE: T1 IAD       SLOTS 1:FXS  2:FXS  3:    4:    5:    6:      NET:  down
DS0 Status: *******----------------r                           ETH:  down
                                                               ^Z=help 23:51
```

Figure 3. DSX Map

NOTE   *The DSX Map can be mapped to the FXS and FXO access modules only.*

---

7.   Left arrow back to **DS0 MAPS** and log off by pressing **<CTRL+L>**.

DLP-18 Unit Installation Using the Auto-Config Feature

Introduction

AUTO-CONFIG allows the service provider to gain initial access to a newly installed IAD while in its factory default state. This eliminates the need for a skilled technician on-site during installation, as it only requires someone to make the network interface and power connections to the IAD. After accessing the unit, the service provider remotely loads a configuration script. A fail-safe timer is then set and the configuration is saved. Next, the service provider reprovisions the network to match the IAD's configuration and accesses the unit. If the service provider can access the unit, the **AUTO-CONFIG** was successful, the unit is operational, and the fail-safe timer should be cancelled. If access is not gained prior to the fail-safe timer expiration, the fail-safe mechanism is invoked and the IAD returns to the default configuration.

This DLP details the steps involved in an IAD installation using the **AUTO-CONFIG** feature.

Prerequisite Procedures

The unit must be at factory default. If the unit is not a new unit, factory default the unit by one of the following methods:

*   Select **SYSTEM UTILITY > TERMINAL MODE**. At the > prompt, type **fac**. You will then see "Restore Factory Defaults and Reset Unit? (press **Y**)." Press the **Y** key to confirm default. The unit then resets.
*   If connected to the **CRAFT** port (must be at 9600 baud), power reset the unit and then restore power to the unit while holding down the **F** key. You will then be prompted to confirm the factory default.

Obtain the desired configuration file. The config file may be one of the following two formats:

*   A .cfg file which is loaded via TFTP. See DLP-9, *Saving the Current Configuration Using TFTP*.
*   A script obtained via the terminal mode. See DLP-13 (*Saving the Router's Configuration* section only).

> **NOTE**
>
> *The service provider's access network Layer 1 must be provisioned to map a single 64 K DS0 from the provider's network to DS0 24 on the customer's T1 circuit with matching circuit parameters (ESF, B8ZS).*

Tools and Materials Required

*   VT100 compatible terminal or computer with terminal emulation software (only required if unit has to be factory defaulted)
*   Appropriate cable to connect terminal to the unit (customer-provided, only required if unit has to be factory defaulted)
*   DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

WARNING   *To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

CAUTION   *Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

1. Verify the unit is at factory default.

2. Connect the network interface cable to the **NTWK** port on the rear of the unit.

3. Power up the unit.

4. Using DS0 24 (mapped to the router by default), the unit begins the process of auto-detecting whether the packets received on the WAN interface are PPP LCP packets or Frame Relay signaling packets. When the second consecutive control packet of the same type is received, the unit configures itself for the detected L2 protocol. When the next control packet of the same type is received, the L2 protocol is confirmed, and the auto-detection of the L2 protocol is complete.

    If PPP is detected:
    - The unit's PPP interface is set to accept its IP address from the service provider's peer router via the PPP IPCP config-NAK mechanism as described in RFC 1332.
    - The unit automatically sets its default route to the service provider's edge router address as identified by PPP IPCP.

    If Frame Relay is detected:
    - The frame relay network signaling is further analyzed to automatically detect the signaling protocol being used (Annex D, Annex A, or LMI).
    - Next, the unit automatically adds the first indicated Frame Relay PVC as an interface to the IAD router.
    - When the PVC becomes active, the unit broadcasts a DHCP request toward the provider edge router over the active PVC.
    - When a DHCP response is received, the unit assigns the address indicated by the DHCP server as its WAN IP address. The address indicated as the gateway address is set as the default gateway. Additional information provided may also be used such as DNS server addresses, WINS addresses, Domain name, Host name, etc.

5. Once the L2 protocol detection is complete, the service provider can telnet into the unit using the IP address assigned by the router/DHCP server.

> **NOTE**
>
> *The service provider's access network Layer 1 must be provisioned to map a single 64 K DS0 from the provider's network to DS0 24 on the customer's T1 circuit with matching circuit parameters (ESF, B8ZS).*

6. Load the desired configuration file. The config file may be one of the following two formats:
    *   A .cfg file which is loaded via TFTP. See DLP-9, *Saving the Current Configuration Using TFTP.*
    *   A script obtained via the terminal mode. See DLP-13 (*Saving the Router's Configuration* section only).

7. Set the failsafe timer by selecting **SYSTEM UTILITY > TERMINAL MODE** and typing *fstimer start x*, (where x is in seconds) at the > prompt. Select a value for x which will allow enough time for the service provider to reconfigure the network to match the unit's new configuration and which will allow an extra 3 to 5 minutes for the unit to sync up with the network.

> **CAUTION**
>
> *Set the failsafe timer prior to doing the save. Typing* **save** *will apply the configuration changes, and the unit will not be accessible until the network is reconfigured.*

8. Type *Save* at the > prompt. This applies all configuration changes and the current connection is lost.

9. At this point, the service provider reconfigures the network to match the unit's new configuration.

10. After the network configuration is complete, the service provider attempts to connect to the unit. If the connection is successful, deactivate the failsafe timer by selecting **SYSTEM UTILITY > TERMINAL MODE** and typing *fstimer stop* at the > prompt.

11. If the connection is not successful, wait until the timer expires and the unit will factory default back to the **AUTO-CONFIG** mode. Repeat steps 4-10 of this DLP.

DLP-19 TDM to ATM Upgrade

Introduction

The Echo Canceller Module provides G.165/G.168 echo cancellation for voice over ATM applications and is available with Adaptive Differential Pulse Code Modulation (ADPCM). ADPCM is a speech coding method which uses fewer bits than traditional Pulse Code Modulation (PCM), allowing the user to get more analog voice calls on less bandwidth. Echo cancellation and ADPCM resources are built into all 600 Series units except the Total Access 612/616/624 T1 TDM units (P/N 4200612L1#TDM, 4200616L1#TDM, and 4200624L1#TDM). These units may be upgraded to include echo cancellation via three methods. This DLP discusses those three methods.

NOTE	*Total Access 604/608 units and third generation Total Access 612/616/624 units (P/N 1203612L1, 1203616L1, and 1203624L1) have built-in Echo Canceller capability and do not need a hardware upgrade for TDM to ATM applications.*

Prerequisite Procedures

*   Purchase the EC/ADPCM (P/N 1200613L1).

Tools and Materials Required

*   VT100 compatible terminal or computer with terminal emulation software
*   Appropriate cable to connect terminal to the unit (customer-provided)
*   DB-9 female to RJ-48 female adapter (ADTRAN proprietary) for connecting to the **CRAFT** port on the rear of the unit (see *CRAFT Port* on page 31).

NOTE	*Refer to DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port, for details on making a terminal connection to the Total Access 6XX.*

WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

|	
CAUTION	*Electronic equipment can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic components. Place equipment in antistatic packing material when transporting or storing. When working on equipment, always place it on an approved antistatic mat that is electrically grounded.*

Perform the steps below in the order listed.

The upgrade package may be purchased from ADTRAN. This package includes the EC/ADPCM (P/N 1200613L1) and the ADTRAN installation and test. If this package is ordered, the customer must send the Total Access TDM 612/616/624 unit back to ADTRAN. Once received, the EC/ADPCM module is installed along with the latest VoATM firmware. The upgraded unit is then tested and returned to the customer. Please call ADTRAN CAPs department at 800-9-ADTRAN extension 7722 for this service.

Purchase and Installation of the EC/ADPCM Module by the Customer

An EC/ADPCM module may be purchased separately and installed in the Total Access 612/616/624 T1 TDM unit by the customer.

1. Remove power from the Total Access 612/616/624.

2. Remove the screws from the back of the Total Access 612/616/624, and then remove the cover.

3. Install the EC/ADPCM Module in the Total Access 612/616/624 as shown in the following figure.

Network Card

FXS Card

**EC/ADPCM Card
(Installed and secured)**
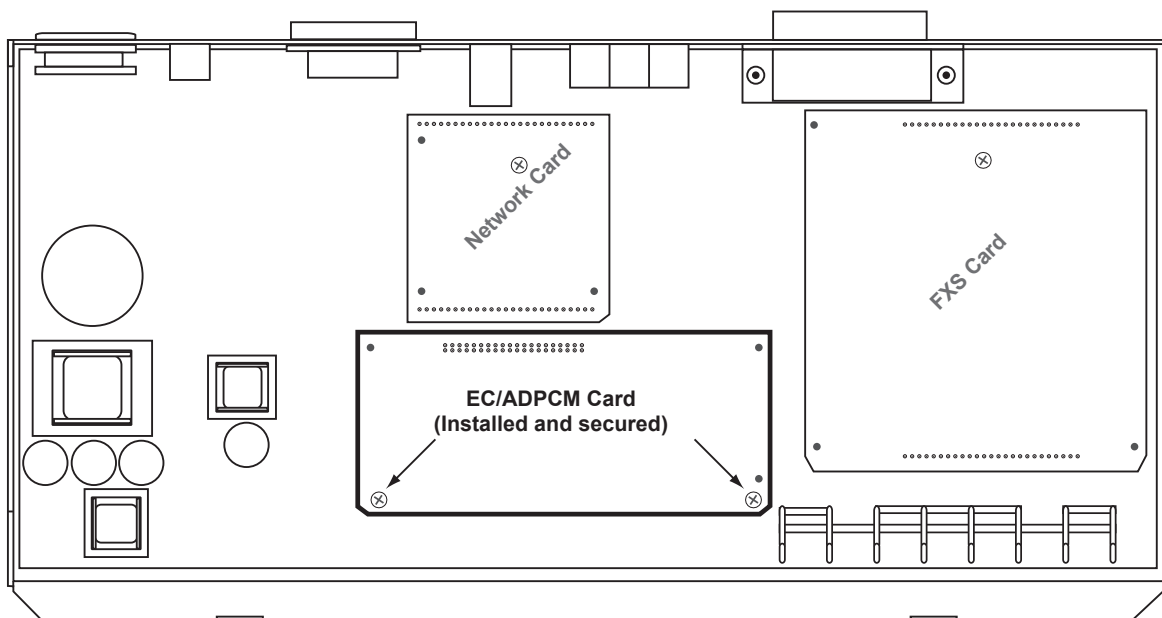
4. Remove the two screws from the motherboard, install the two standoffs, and insert the screws through the top the EC/ADPCM board into the standoffs.

5. Replace the cover on the Total Access 612/616/624 and tighten the screws.

6. Restore power to the Total Access 612/616/624.

7. Obtain the latest VoATM firmware from the ADTRAN website (http://www.ADTRAN.com). Select **SUPPORT > POST-SALES TECHNICAL SUPPORT > FIRMWARE UPDATES > 612/616/624 ATM** or contact Post-Sales Technical Support at 888-4ADTRAN.

8. Upgrade the Total Access 612/616/624 with the latest VoATM firmware (see *Updating the Firmware using TFTP* and DLP-8, *Updating the Firmware using XMODEM* for details on upgrading the firmware).

9. Factory default the Total Access 612/616/624 by one of the following methods:

   • Select **SYSTEM UTILITY > TERMINAL MODE**. At the > prompt, type **factory_reset**. You will then see "Restore Factory Defaults and Reset Unit? (press **Y**)." Press the **Y** key to confirm default. The unit then resets.

   • If connected to the **CRAFT** port (must be 9600 baud), power reset the unit and then restore power to the unit while holding down the **F** key. You will then be prompted to confirm the factory default.

10. In the ATM code, the upgrade was successful if the **SYSTEM INFO > FIRMWARE REVISION** field does not display Error.

11. Reconfigure the unit for the specific application.

Purchase of a T1 TDM 612/616/624 Unit with the EC/ADPCM Card Installed for Later Upgrade to ATM

For customers who plan to operate a TDM application initially, but eventually upgrade to an ATM application, a Total Access 612/616/624 unit may be purchased with the EC/ADPCM card installed (P/N 4200612L2#TDM, 4200616L2#TDM, 4200642L2#TDM).

1. When the circuit is converted to ATM, the customer may obtain the latest VoATM firmware from the ADTRAN website (http://www.ADTRAN.com). Select **SUPPORT > POST-SALES TECHNICAL SUPPORT > FIRMWARE UPDATES > 612/616/624 ATM** or contact Post-Sales Technical Support at 888-4ADTRAN.

2. Upgrade the Total Access 612/616/624 with the latest VoATM firmware (see *Updating the Firmware using TFTP* and DLP-8, *Updating the Firmware using XMODEM* for details on upgrading the firmware).

3. Factory default the Total Access 612/616/624 by one of the following methods:

   • Select **SYSTEM UTILITY > TERMINAL MODE**. At the > prompt, type **fac**. You will then see "Restore Factory Defaults and Reset Unit? (press **Y**)." Press the **Y** key to confirm default. The unit then resets.

   • If connected to the **CRAFT** port, power reset the unit and then restore power to the unit while holding down the **F** key. You will then be prompted to confirm the factory default.

4. In the ATM code, the upgrade was successful if the following two things occur:

   • The **SYSTEM INFO > FIRMWARE REVISION** field does not display Error.

ADTRAN UTILITIES

This section provides instructions for configuring and using the ADTRAN Utilities software programs including Telnet, VT100, Syslog, and TFTP.

ADTRAN delivers several PC software utilities with the Total Access 600 Series. These utilities are located on the CD-ROM that came with your shipment. The utilities make it easier to interface with the terminal menu and transfer configuration files to and from TFTP servers. The utilities all run on Microsoft Windows 3.1 or higher. The following sections describe the Syslog, Telnet, VT100, and TFTP Server utilities.

> **NOTE**   *Review the readme file (Readme.txt) on the CD-ROM for the latest information about the utilities.*

CONTENTS

FIGURES

---

1.   TELNET UTILITY

Access the Telnet program remotely through the Ethernet port. For a detailed description of how to work within the terminal menu, refer to *Navigating the Terminal Menu* on page 43 (in the User Interface Guide section of this manual). The Telnet menus include **SESSION**, **EDIT**, **OPTIONS**, **CAPTURE**, and **HELP** (see the menu tree in Figure 1).

|			
		Connect	Host Name
			Port
	Session	Disconnect	Edit Entry
		Transfer Cfg	Add New
		Exit	Delete
			Connect
	Edit	Copy	
		Paste	
			Background
Telnet	Options	Colors	Bold
		Local Echo	Text
		Auto Repeat	
		File	Start Cfg Capture
			Stop Cfg Capture
	Capture	Buffer Size	
		Save Buffer As	
		Screen Capture	
	Help	Contents	
		IP Status	
		About	

Figure 1. Telnet Menu Tree

Session Menu

Click on **SESSION** to open the Telnet session.

Connect

Opens dialog box for setting **HOST NAME** and
PORT parameters for a Telnet session. Also lets
you **EDIT ENTRY**, **ADD NEW** entry, and **DELETE**
stored entries. When the parameters are set, click
CONNECT to make the connection. Click **CANCEL**
to end the session.
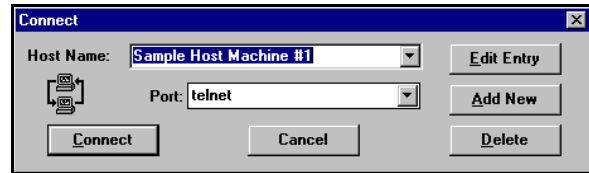
Host Name

Accepts and stores host names. You may enter either a name, an IP address, or a domain name directly
from this field. Click on the drop-down arrow to display a complete list of previously stored host
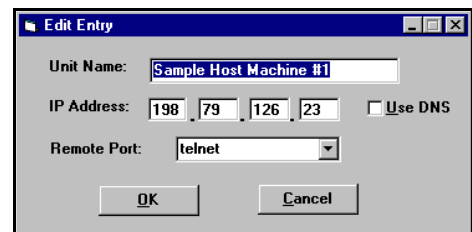names.

Port

Provides several port options. You may enter port numbers directly into this field to connect to
non-standard ports or select the drop-down combo-box to display the following options:

TELNET	establishes a Telnet session
ECHO	provides a loopback for troubleshooting
DISCARD	bit bucket; discards data
DAYTIME	returns the time
CHARGEN	displays as a unique character stream; used for self-tests

Edit Entry

Changes either the unit name or the IP address of each host.
Press either **Tab, Return,** or a **period** (**.**) after each number in
the IP address to move to the next field. If you press **Return**
or enter a period while the cursor is located in an IP field,
that field entry is deleted.

Add New

Prompts you for the same information as the **EDIT ENTRY**
dialog box for new host. When enabled, the **USE DNS** (Domain Name Server) feature allows users to
request **DOMAIN LOOK UP** via a DNS server on the network, rather than specifying an IP address. The
name then appears in the **HOST NAME** field.

Delete

Removes a host name from the list; select the host name you want to remove, and, at the prompt, click
DELETE.

Connect

Establishes the Telnet session.

Disconnect

Terminates the Telnet session.

To re-establish the session, select **CONNECT** from **SESSION MENU** or press **ENTER** three times. This action restores the previous connection.

Transfer Cfg

This feature is used with ADTRAN products to send configuration files to the unit.

Exit

Ends the Telnet session and closes the Telnet screen.

Edit Menu

Provides **COPY** and **PASTE** commands.

Options Menu

Provides viewing alternatives for the terminal screen.

Colors

Three options change the color of the background window (**BACKGROUND**), bold highlights (**BOLD**), and text (**TEXT**).

Local Echo

Echoes each character that you enter.

AutoRepeat

Repeats characters you select from the keyboard, if you hold down the key.

Capture Menu

Provides options for capturing screen images.

File

Sends screen options data to a file in the format options listed below:

Start Cfg Capture

Used with the ADTRAN product line to start sending the scrolling screen capture to a file storage location.

Stop Cfg Capture

Used with the ADTRAN product line to stop sending the scrolling screen capture to a file storage location.

Buffer Size

Disables terminal window scroll bars when set to zero. (This is the normal setting for Total Access 600 Series.) This number represents the number of lines to capture in the memory buffer.

Save Buffer As

Save screen capture to a file.

Screen Capture

Copies the text on the current Telnet screen to the clipboard. You can open any word processor and paste the clipboard contents into the program. This option is helpful when debugging.

Help Menu

Provides online help for using the ADTRAN Utilities.

Contents
Opens the online help.

IP Status
Displays the local port address and the status of the connection.

About
Displays version and owner information.

2.   VT100 UTILITY

Use the VT100 to configure a unit which is directly connected to a PC. The VT100 display is almost identical to the Telnet display. For a detailed description of how to work within the terminal menu, refer to *Navigating the Terminal Menu* on page 43 (in the User Interface Guide section of this manual). If you need help setting up the unit for a VT100 session, refer to DLP-1, *Connecting a VT100 Terminal or PC to the CRAFT Port*. VT100 menus include **SESSION**, **EDIT**, **PORT**, **OPTIONS**, **CAPTURE**, and **HELP** (see the menu tree in Figure 2).
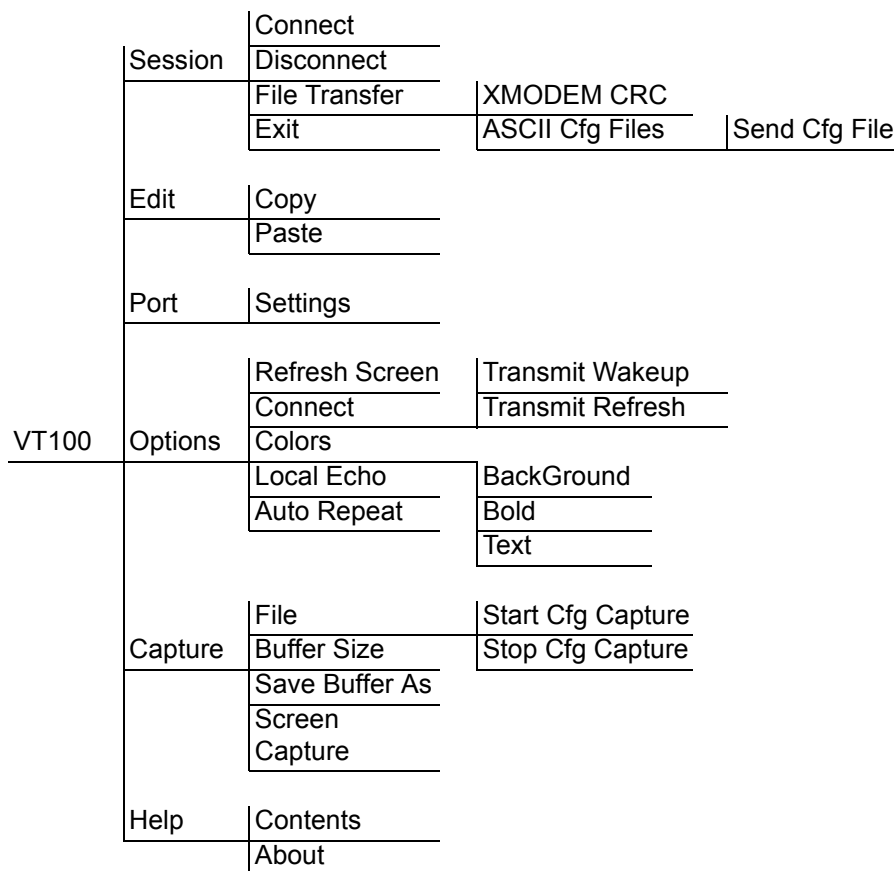

Figure 2. VT100 Menu Tree

Session Menu

Opens VT100 terminal emulation session.

Connect

Opens a specified serial port for a VT100 session.

Disconnect

Closes a specified serial port at the end of a VT100 session.

File Transfer

Uploads and downloads files to and from a unit.

XMODEM CRC

Selects the XMODEM file transfer protocol.

ASCII Cfg Files

Selects ASCII transfer mode. Primarily useful for configuration transfers for the ADTRAN products.

Edit Menu

Identical to the Telnet **EDIT MENU** (see *Edit Menu* on page 246).

Port Menu

Changes serial COM port **SETTINGS**. Provides data rate settings from 300-57600 bps.

Options Menu

Provides terminal screen commands.

Refresh Screen

Redraws the screen.

Connect

Provides the options **TRANSMIT WAKEUP** and **TRANSMIT REFRESH**.

Transmit Wakeup

Provides a control sequence that puts the unit's Control Port online in terminal mode.

Transmit Refresh

Provides a control sequence to refresh the screen automatically when connecting. (This is the default setting for the unit.)

Colors
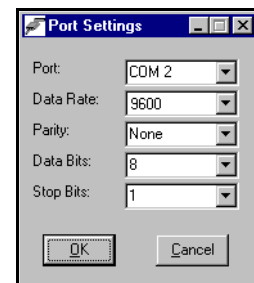
Identical to Telnet **COLORS MENU** (see *Colors* on page 246).

Local Echo

Echoes each character that you enter.

AutoRepeat

Repeats characters you select from the keyboard, if you hold down the key.

Capture Menu
Identical to the Telnet **CAPTURE MENU** (see *Capture Menu* on page 246).

Help Menu
Provides online help and information about the version number.

Contents
Opens online help.

About
Displays version and owner information.

3.   TFTP SERVER

The TFTP Server utility transfers unit configuration files to and from a TFTP server (see Figure 3 for the menu tree). You can install this program on a PC running any version of Microsoft Windows. The configuration of a unit can be saved offline as a backup file. The saved file may also be used to send the same configuration to multiple units. Transfer configuration files using the TFTP protocol (a TCP/IP user protocol) via the Ethernet port. The unit must have a valid IP address, subnet mask, and default gateway (if required), and be connected to an Ethernet network before proceeding. Figure 4 on page 250 shows the TFTP server interface. For information on transferring and saving configurations using TFTP, refer to DLP-9, *Saving the Current Configuration Using TFTP*.

> **NOTE**
> *Files must be placed in the Application directory where you installed the product. Received files are also placed here.*

TFTP Server	Server	Enable
		Disable
		Abort
		Exit
	Print Log	...to Clipboard
		...to Printer
		Clear Log
	Help	Contents
		About
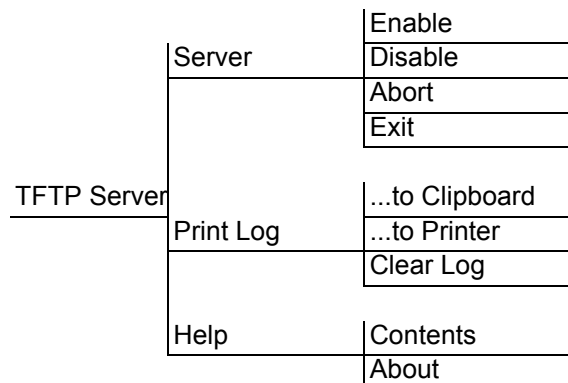
Figure 3. TFTP Server Interface Menu Tree
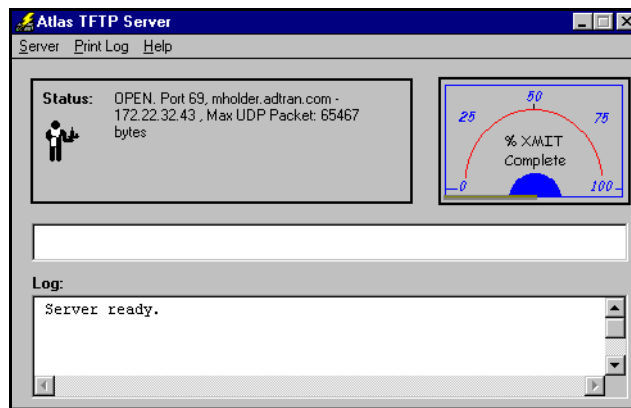
Figure 4. TFTP Server Interface

Only one configuration transfer session (upload or download) may be active at a time. The TCP/IP parameters are not saved or overwritten as part of a unit's transferred configuration to allow sending identical configurations to multiple units. When you start this program, a port is automatically opened.

Server Menu
Provides enable, disable, abort, and exit options.

Enable
Enables the TFTP server. The IP address displays in the Status field and **Server Ready** displays in the Log field.

Disable
Disables the TFTP server. When you select this option, the message **Port Closed** displays in the **STATUS** field and in the **LOG** field.

Abort
Terminates a transfer that is in progress.

Exit
Terminates active transfers and closes the TFTP window.

Print Log
Provides print options.

...to Clipboard
Copies the information in the **LOG** field to the clipboard. You can then open any word processor and paste the information into the program for review.

...to Printer
Sends the information in the **LOG** field to the default printer.

Clear Log
Deletes the information stored in the **LOG** field.

Help

Provides online help and version information.

Contents

Opens online help.

About

Displays version and owner information.

4.   STATUS FIELD

This field displays general information about port and transfer status. This field is read-only. The unlabeled field in the center of the screen displays prompts about the status of active transfers, such as bytes transferred and received.

5.   METER FIELD

The **XMIT** meter provides a visual record of the transfer progress.

6.   LOG FIELD

This field displays a record of all of the events that occur during the time the TFTP Server is enabled. Use the scroll bar to move up and down the list. To clear the information in this field, select **CLEAR LOG** from the **PRINT LOG** menu. Save this information to a file before deleting it with the **...TO CLIPBOARD** command.

© 2004 ADTRAN, Inc.

MIBS

This section is divided into two parts: (1) SNMP information for TDM units and (2) SNMP information for ATM units. Each section details the Management Information Bases (MIBs) supported, MIB Compilation Order, Traps Supported, and MIB Variables supported.

CONTENTS

1.   MIBS SUPPORTED BY TDM UNITS

> 📝 **NOTE**   *All TDM MIBs are SNMPv2.*

Standard RFC MIBs:

RFC1573.mi2	IANAifType-MIB
RFC1907.mi2	SNMPv2-MIB
RFC2011.mi2	IP-MIB
RFC2096.mi2	IP-FORWARD-MIB
RFC2115.mi2	FRAME-RELAY-DTE-MIB
RFC2493.mi2	PerfHist-TC-MIB
RFC2494.mi2	DS0-MIB and DS0BUNDLE-MIB
RFC2495.mi2	DS1-MIB
RFC2665.mi2	EtherLike-MIB
RFC2863.mi2	IF-MIB

Enterprise MIBs:

adtran.mi2	ADTRAN-MIB
adIadSys.mi2	ADTRAN-ADIADSYS-MIB
adIadRtr.mi2	ADTRAN-ADIADROUTER-MIB
adIadVoi.mi2	ADTRAN-ADIADVOICE-MIB

> 📝 **NOTE**   *SNMPv2-SMI, SNMPv2-TC, SNMPv2-TM, and SNMPv2-CONF should be included with the SNMP manager.*

2. MIB COMPILATION ORDER FOR TDM UNITS

IANAifType-MIB

PerfHist-TC-MIB

SNMPv2-MIB (if not included with SNMP manager)

IF-MIB

IP-MIB

IP-FORWARD-MIB

FRAME-RELAY-DTE-MIB

DS1-MIB

DS0-MIB

DS0BUNDLE-MIB

EtherLike-MIB

ADTRAN-MIB

ADTRAN-IADSYS-MIB

ADTRAN-IADROUTER-MIB

3. TRAPS SUPPORTED BY TDM UNITS

From RFC1215-MIB:	coldStart
	linkDown
	linkUp
	authenticationFailure
From ADTRAN-IADSYS-MIB:	adIadWanDown - 1003203
	adIadWanUp - 1003204
	adIadBatteryAlarmAct - 1003207
	adIadBatteryAlarmDeact - 1003208
(T1 WAN interface only):	adIadDs1RedAlarmON - 1003209
	adIadDs1YellowAlarmON - 1003210
	adIadDs1BlueAlarmON - 1003211
	adIadDs1RedAlarmOFF - 1003212
	adIadDs1YellowAlarmOFF - 1003213
	adIadDs1BlueAlarmOFF - 1003214
	adIadDs1SEF - 1003215
	adIadDs1FS - 1003216
(T1 WAN interface only):	adIadDs1CRC - 1003217
	adIadDs1LCV - 1003218
	adIadDs1SLP - 1003219
From ADTRAN-IADVOICE-MIB:	adIadVoiceaLifeLineActivated - 1003407
	adIadVoiceaLifeLineDeactivated - 1003408

4.   MIB VARIABLES SUPPORTED BY TDM UNITS

SNMPv2 states the supported MIB variables by the following method:

The unit will have a MIB called TA 6XX.mi2 that will describe the SNMP variables supported. This MIB will contain an Agent Capabilities module that will describe the SNMP variables supported.

5.   MIBS SUPPORTED BY ATM UNITS

> **NOTE**
>
> *This section is currently being revised to include new SNMP information for SNMP v2. Please visit the ADTRAN website at: http://www.adtran.com for the latest documentation.*

tcp:

tcpRtoAlgorithm	RO
tcpRtoMin	RO
tcpRtoMax	RO
tcpMaxConns	RO
tcpActiveOpens	RO
tcpPassiveOpens	RO
tcpAttemptFails	RO
tcpEstabResets	RO
tcpCurrEstab	RO
tcpInSegs	RO
tcpOutSegs	RO
tcpRetransSegs	RO

tcpConnTable

tcpConnEntry

tcpConnState	RO
tcpConnLocalAddress	RO
tcpConnLocalPort	RO
tcpConnRemAddress	RO
tcpConnRemPort	RO

tcpInErrs	RO
tcpOutRsts	RO

udp:

udpInDatagrams	RO
udpNoPorts	RO
udpInErrors	RO
udpOutDatagrams	RO
udpLocalAddress	RO
udpLocalPort	RO

udpTable

udpEntry

udpEntryLocalAddress	RO
udpLocalPort	RO

egp:

egpInMsgs	RO
egpInErrs	RO
egpOutMsgs	RO
egpOutErrors	RO
egpNeighState	RO
egpNeighAddr	RO
egpNeighAs	RO
egpNeighInMsgs	RO
egpNeighInErrs	RO
egpNeighOutMsgs	RO
egpNeighOutErrs	RO
egpNeighInErrMsgs	RO
egpNeighOutErrMsgs	RO
egpNeighStateUps	RO
egpNeighStateDowns	RO
egpNeighIntervalHello	RO
egpNeighIntervalPoll	RO
egpNeighMode	RO

dsx1:

dsx1ConfigTable

dsx1ConfigEntry

dsx1LineIndex	RO
dsx1IfIndex	RO
dsx1TimeElapsed	RO
dsx1ValidIntervals	RO
dsx1LineType	RO
dsx1LineCoding	RO
dsx1SendCode	RO
dsx1CircuitIdentifier	RO
dsx1LoopbackConfig	RO
dsx1LineStatus	RO
dsx1SignalMode	RO
dsx1TransmitClockSource	RO
dsx1Fdl	RO

dsx1CurrentTable

dsx1CurrentEntry

dsx1CurrentIndex	RO
dsx1CurrentESs	RO
dsx1CurrentSESs	RO
dsx1CurrentSEFs	RO
dsx1CurrentUASs	RO
dsx1CurrentCSSs	RO
dsx1CurrentPCVs	RO
dsx1CurrentLESs	RO
dsx1CurrentBESs	RO
dsx1CurrentLCVs	RO

dsx1IntervalTable

dsx1IntervalEntry

dsx1IntervalIndex	RO
dsx1IntervalNumber	RO
dsx1IntervalESs	RO
dsx1IntervalSESs	RO
dsx1IntervalSEFs	RO
dsx1IntervalUASs	RO
dsx1IntervalCSSs	RO
dsx1IntervalPCVs	RO
dsx1IntervalLESs	RO
dsx1IntervalBESs	RO
dsx1IntervalLCVs	RO

dsx1TotalTable

dsx1TotalEntry

dsx1TotalIndex	RO
dsx1TotalESs	RO
dsx1TotalSESs	RO
dsx1TotalSEFs	RO
dsx1TotalUASs	RO
dsx1TotalCSSs	RO
dsx1TotalPCVs	RO
dsx1TotalLESs	RO
dsx1TotalBESs	RO
dsx1TotalLCVs	RO

dsx1FracTable

dsx1FracEntry

	dsx1FracIndex	RO
	dsx1FracNumber	RO
	dsx1FractIfIndex	RO

snmp:

snmpInPkts	RO
snmpOutPkts	RO
snmpInBadVersions	RO
snmpInBadCommunityNames	RO
snmpInBadCommunityUses	RO
snmpInASNParseErrs	RO
snmpInTooBigs	RO
snmpInNoSuchNames	RO
snmpInBadValues	RO
snmpInReadOnlys	RO
snmpInGenErrs	RO
snmpInTotalReqVars	RO
snmpInTotalSetVars	RO
snmpInGetRequests	RO
snmpInSetRequests	RO
snmpInGetRequests	RO
snmpInTraps	RO
snmpOutTooBigs	RO
snmpOutNoSuchNames	RO
snmpOutBadValues	RO
snmpOutGenErrs	RO
snmpOutGetRequests	RO
snmpOutGetNexts	RO
snmpOutSetRequests	RO
snmpOutGetRepsonses	RO
snmpOutTraps	RO
snmpEnableAuthenTraps	RO

atm:

atmInterfaceTable

atmInterfaceEntry		
	atmInterfaceMaxVpcs	RO
	atmInterfaceMaxVccs	RO
	atmInterfaceConfVpcs	RO
	atmInterfaceConfVccs	RO
	atmInterfaceMaxActiveVpiBits	RO
	atmInterfaceMaxActiveVciBits	RO
	atmInterfaceIlmiVpi	RO
	atmInterfaceIlmiVci	RO
	atmInterfaceAddressType	RO
	atmInterfaceAdminAddress	RO
	atmInterfaceMyNeighborIpAddress	RO
	atmInterfaceMyNeigherIfName	RO

atmInterfaceTCTable		
atmInterfaceTCEntry		
	atmInterfaceOCDEvents	RO
	atmInterfaceTCAlarmState	RO

atmTrafficDescrParamTable		
atmTrafficDescrParamEntry		
	atmTrafficDescrParamIndex	RO
	atmTrafficDescrType	RO
	atmTrafficDescrParam1	RO
	atmTrafficDescrParam2	RO
	atmTrafficDescrParam3	RO
	atmTrafficDescrParam4	RO
	atmTrafficDescrParam5	RO
	atmTrafficDescrQosClass	RO
	atmTrafficDescrRowStatus	RO

atmVclTable		
atmVclEntry		
	atmVclVpi	RO
	atmVclVci	RO
	atmVclAdminStatus	RO
	atmVclOperStatus	RO
	atmVclLastChange	RO
	atmVclReceiveTrafficDescrIndex	RO

atmVclTransmitTrafficDescrIndex	RO
atmVccAalType	RO
atmVccAal5CpcsTransmitSduSize	RO
atmVccAal5CpcsReceiveSduSize	RO
atmVccAal5EncapsType	RO
atmVclCrossConnectIdentifier	RO
atmVclRowStatus	RO

aal5VccTable

    aal5VccEntry

aal5VccVpi	RO
aal5VccVci	RO
aal5VccCrcErrors	RO
aal5VccSarTimeOuts	RO
aal5VccOverSizedSDUs	RO

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com