ADTRAN

TOTAL ACCESS 600R

System Manual

4200600L1#TDM Total Access 600R TDM

61200600L1-1A
December 2002

Trademarks

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

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.

ADTRAN

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

About this Manual

This manual provides a complete description of the Total Access 600R 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 600R. This manual is arranged so that needed information can be quickly and easily found. The following is an overview of the contents.

Revision History

This is the first issue of this manual.

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

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

1. This equipment complies with Part 68 of FCC rules. On the back of the equipment housing is a label showing the FCC registration number and ringer equivalence number (REN). 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. 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 to be connected to the telephone network or premises wiring using an FCC compatible modular jack, which is Part 68 compliant.
7. The following information may be required when applying to the local telephone company for leased line facilities.

Product	Reg. Number	Service Type	REN/SOC	FIC	USOC
Total Access 600R	HDCUSA-44556-DE-N	1.544 Mbps - SF 1.544 Mbps - SF and B8ZS 1.544 Mbps - ESF 1.544 Mbps - ESF and B8ZS	6.0N	04DU9-BN 04DU9-DN 04DU9-1KN 04DU9-1SN	RJ-48C

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.

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 voiceband analog signals 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 for filing an affidavit with the local exchange carrier when connecting unprotected customer premise equipment (CPE) to 1.544 Mbps or subrate digital services.

Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirement for subrate services is 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:

____

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.*

Industry Canada Compliance Information

Notice: The Industry Canada label applied to the product (identified by the Industry Canada logo or the “IC:” in front of the certification/registration number) signifies that the Industry Canada technical specifications were met.

Notice: The Ringer Equivalence Number (REN) for this terminal equipment is supplied in the documentation or on the product labeling/markings. The REN assigned to each terminal device indicates the maximum number of terminals that can be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices should not exceed five (5).

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.

Warranty and Customer Service

ADTRAN will repair and return this product within ten years from the date of shipment if it does not meet its published specifications or fails while in service. For detailed warranty, repair, and return information refer to the ADTRAN Equipment Warranty and Repair and Return Policy Procedure.

Return Material Authorization (RMA) is required prior to returning equipment to ADTRAN.

For service, RMA requests, or further information, contact one of the numbers listed at the end of this section.

LIMITED PRODUCT WARRANTY

ADTRAN warrants that for ten years from the date of shipment to Customer, all products manufactured by ADTRAN will be free from defects in materials and workmanship. ADTRAN also warrants that products will conform to the applicable specifications and drawings for such products, as contained in the Product Manual or in ADTRAN's internal specifications and drawings for such products (which may or may not be reflected in the Product Manual). This warranty only applies if Customer gives ADTRAN written notice of defects during the warranty period. Upon such notice, ADTRAN will, at its option, either repair or replace the defective item. If ADTRAN is unable, in a reasonable time, to repair or replace any equipment to a condition as warranted, Customer is entitled to a full refund of the purchase price upon return of the equipment to ADTRAN. This warranty applies only to the original purchaser and is not transferable without ADTRAN's express written permission. This warranty becomes null and void if Customer modifies or alters the equipment in any way, other than as specifically authorized by ADTRAN.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE FOREGOING CONSTITUTES THE SOLE AND EXCLUSIVE REMEDY OF THE CUSTOMER AND THE EXCLUSIVE LIABILITY OF ADTRAN AND IS IN LIEU OF ANY AND ALL OTHER WARRANTIES (EXPRESSED OR IMPLIED). ADTRAN SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING (WITHOUT LIMITATION), ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.   SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THIS EXCLUSION MAY NOT APPLY TO CUSTOMER.

In no event will ADTRAN or its suppliers be liable to the Customer for any incidental, special, punitive, exemplary or consequential damages experienced by either the Customer or a third party (including, but not limited to, loss of data or information, loss of profits, or loss of use). ADTRAN is not liable for damages for any cause whatsoever (whether based in contract, tort, or otherwise) in excess of the amount paid for the item. Some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to the Customer.

Customer Service, Product Support Information, and Training

ADTRAN will repair and return this product if within ten years from the date of shipment the product does not meet its published specification or the product fails while in service.

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

SYSTEM DESCRIPTION

This section of ADTRAN's Total Access 600R System Manual is designed for use by network engineers, planners, and designers for overview information about the Total Access 600R.

It contains general information and describes the L2 protocol support, routing capability, security, and testing features. This section should be used in conjunction with Section 2, Engineering Guidelines, of this system manual.

CONTENTS

1. SYSTEM OVERVIEW

The Total Access 600R is a cost-effective T1/FT1 access router designed for small and medium businesses, branch offices and campuses. The unit provides 1.54 Mbps for dedicated Internet access or remote office connectivity. With its integrated CSU/DSU, the Total Access 600R provides wide area network access over a standard T1 or fractional T1 circuit.

Multiple users can share network access over a single T1 connection. For simultaneous access to both a corporate network and the public Internet, the unit offers the ability to configure multiple frame relay PVCs. In addition, the unit includes NAT/NAPT and IP filtering which provides security from unauthorized access to the user's network.

The Total Access 600R also provides a cost-effective campus connectivity solution. When used with private dry copper, the unit delivers up to 1.54 Mbps to cross-campus network elements. This solution is ideal for extending LAN segments to other buildings.

Other features include a DHCP server, TELNET support, SNMP support, ping utility, and software upgrades via TFTP and XMODEM.

Until now, the Total Access 600R unit has been running firmware version A.03.XX. Recently, A.04.XX has been released. 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. There are two possible upgrade paths: (1) Upgrading from A.03 to A.04 directly (2) Upgrading from A.03 to A.03.9X (Transition Build) to A.04.

Upgrading from A.03 to A.03.9X (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-015, A.03 to A.04 Firmware Upgrade, for more details.

2. FEATURES AND BENEFITS

Below is a list of unit features and benefits.

Configuration and Management

- VT100 emulation via the **CRAFT** port
- Telnet
- SNMP
- LAN and WAN status LEDs
- Text-based configuration file support
- Syslog client
- ICMP Ping utility
- Trace route utility

Software Upgradeable

- TFTP download
- XMODEM via **CRAFT** port

Network Interface

- Line Rate: T1 1.544 Mbps +/-75 bps
- Physical Interface: RJ-48C (Modular, 8-pin)
- Framing: D4 (SF)/ESF
- Line Code: AMI/B8ZS
- Input Signal: 0 to -36 dB
- DS0 Assignment: User selectable
- Timing: Loop and local

LAN Interface

- 10/100 BaseT
- Half or Full Duplex
- RJ-45
- Secondary IP address
- DHCP server
- IEEE 802.3

Protocol Support

- IP
- DNS
- TCP
- RIP V1, V2 and static routes
- UDP, UDP Relay
- ICMP
- ARP
- PPP
- Frame Relay

Frame Relay

- Support for both point-to-point and point-to-multipoint networks using up to 10 PVCs
- RFC 1490 Encapsulation (Multiprotocol over Frame Relay)
- Signaling Types: LMI, Annex D (ANSI), Annex A (Q933A), and Static (No Signal)

PPP

- LCP, IPCP, BCP, CCP
- Van Jacobson (VJ) header compression

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 (NAT)

Security

- PAP, CHAP, EAP, and Radius
- NAT/NAPT
- Packet filtering by source and destination IP address, source and destination port number, MAC address, protocol or pattern
- Multi-layer password protection
- Telnet security: Access list and password protection

Integrated Components

- IP router
- Network connection
- 10/100BaseT connection
- **CRAFT** port

Testing

- Local Loopbacks: Line and Payload
- Remote Loopbacks: Line, Payload, CSU Loopbacks, and Fractional T1 loopback per ANSI T1.403-1995 (Annex B)
- Error Counts: ES, SES, SEF, FS, LCV, SLP, and UAS
- Alarm Status: Loss of signal, Red Alarm, Yellow Alarm, and Blue Alarm

ENGINEERING GUIDELINES

CONTENTS

FIGURES

TABLES

1. EQUIPMENT DIMENSIONS

The Total Access 600R measures 11.25” W, 7.5” D, and 2” H and comes equipped for table top or wall mount use.

2. POWER REQUIREMENTS

The Total Access 600R has a maximum power consumption of 90-125 VAC 60 Hz and a maximum current draw of 300 mA.

3. REVIEWING THE FRONT PANEL DESIGN

Figure 1 shows the front panel of the Total Access 600R which contains the LAN, WAN, and power LEDs. These LEDs and their functions are described in Table 1.

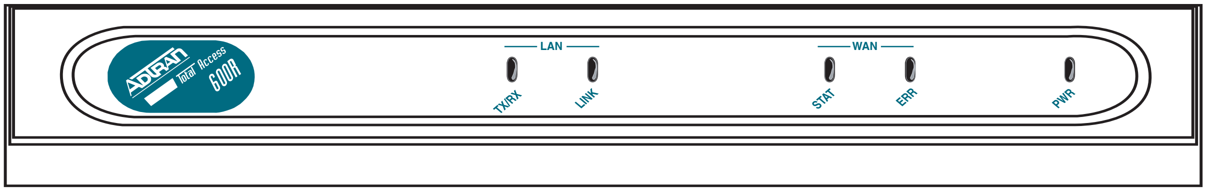


Figure 1. Total Access 600R Front Panel

Front Panel LEDs

The front panel provides five status LEDs to monitor operation and activity. The following table provides LED activity explanations.

Table 1. 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.
	Yellow (solid)	The T1 is in yellow alarm.
	Green (solid)	The unit is not in alarm.

Table 1. Total Access 600R Front Panel LEDs (Continued)

For these LEDs...	This color light...	Indicates that...
WAN ERR	Red (flashing)	The T1 is down.
	Yellow (solid)	Errors are present on the WAN link.
	Red (solid)	Severe errors are present on the WAN link.
	Off	WAN link is up and error-free.
PWR	Green (solid)	Power is supplied to the unit.
	Off	Power is not supplied to the unit.

4. REVIEWING THE REAR PANEL DESIGN

The Total Access 600R rear panel is shown in Figure 2.

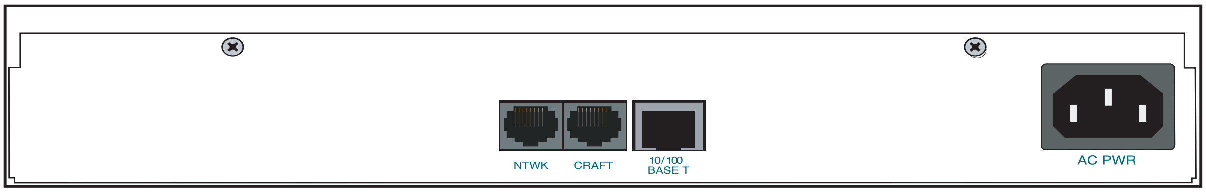


Figure 2. Total Access 600R Rear Panel

NTWK Connection

The **NTWK** connection pinout is a T1 connection. Table 2 shows the pinout for this connection.

Connector type RJ-48C

Table 2. T1 NTWK Connection Pinout

PIN	NAME		DESCRIPTION
1	R1	RXDATA-RING	Receive data from the network
2	T1	RXDATA-TIP	Receive data from the network
3	—	UNUSED	—
4	R	TXDATA-RING	Transmit data toward the network
5	T	TXDATA-TIP	Transmit data toward the network
6, 7, 8	—	UNUSED	—

Craft Port

The **CRAFT** port connects to a computer or modem. The **CRAFT** port input provides the following functions:

- Accepts input from a PC or a modem for controlling the unit.
- Operates at 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bps.
- Acts as input for either VT100 or PC control.
- Acts as an interface for flash memory software downloads using XMODEM.

Table 3 shows the **CRAFT** port pinout.

Connector type	RJ-48C

Table 3. CRAFT Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis
2	RTS	Request to send - flow control
3	RXDATA	Data received by the unit.
4	DTR	Data terminal ready
5	TXDATA	Data transmitted by the unit.
6	CD	Carrier detect
7	UNUSED	—
8	CTS	Clear to send - flow control

10/100BaseT Connection

The **10/100BASET** port (RJ-48C) provides a 10/100BaseT Ethernet LAN connection, which is used for IP Routing, TFTP, SNMP, and Telnet connections. Table 4 shows the **10/100BASET** port pinout.

Connector type	RJ-48C

Table 4. 10/100BaseT 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	—

AC Power Connection

Each unit includes an auto ranging 90-125 VAC, 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.

5. DB-9 TO RJ ADAPTER

The DB-9 to RJ adapter is used to connect a PC or VT100 terminal to the **CRAFT** port. The adapter pinout is shown in Table 5.

Table 5. DB-9 to RJ Adapter Pinout

DB-9	RJ-45	DESCRIPTION
2	5	TX Data
3	3	RX Data
5	1	GND
Note: All other pins are unused.		

6. AT-A-GLANCE SPECIFICATIONS

Table 6 lists the unit specifications.

Table 6. Specifications

Application	Feature	Specification
T1 Network Interface		
	Physical Interface	RJ-48C
	Line Rate	1.544 Mbps +/- 75 bps
	Framing	D4 (SF)/ESF
	Line Code	AMI/B8ZS
LAN Interface		
	Data Rate	10/100 Base
	Duplex Type	Half or full duplex
Frame Relay Support		
	Specifications	RFC 1490 Encapsulation (Multiprotocol over Frame Relay)
	Signaling Types	LMI Annex D (ANSI) Annex A (Q933A) Static (No Signaling)
Protocol Support		
	Protocols	IP DNS TCP RIP V1, V2 and static routes UDP, UDP Relay ICMP ARP PPP Frame Relay
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 (NAT)

Table 6. Specifications (Continued)

Application	Feature	Specification
Management		
	Craft Interface	EIA 232, Physical RJ-48C
	Ethernet 10/100BaseT Interface	SNMP V2 support Syslog client ICMP Ping Utility Full menu-driven Telnet access Software download via TFTP
Security		
	Authentication	PAP, CHAP, EAP, and Radius
	Telnet	Telnet access list and Password protection
	Filtering	Packet filtering by IP address, port number, MAC address, protocol or pattern
WAN Testing and Troubleshooting		
	Loopbacks	Local Loopbacks (line and payload) Remote Loopbacks (line, payload, and CSU) Fractional T1 loopback per ANSI T1.403-1995 (Annex B)
	Status	Error Counts Alarm Status

NETWORK TURNUP PROCEDURE

CONTENTS

1. INTRODUCTION

This section discusses the unit installation process.

2. TOOLS REQUIRED

The tools required for unit installation are:

- Screws (customer-provided for wallmount installation)
- Screwdriver (for wall or rackmount installation)

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 modules can be damaged by static electrical discharge. Before handling modules, wear an antistatic discharge wrist strap to prevent damage to electrical components. Place modules in antistatic packing material when transporting or storing. When working on modules, always place them 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 the contact information in the front of this manual).

Contents of ADTRAN Shipment

Your ADTRAN shipment of the Total Access 600R includes the following items:

- Mounting Instructions (P/N 64200600L1#T-19A)
- CD (P/N 32536146@B)
- Cable Tie (P/N 3292032)
- Silver Satin Cable (P/N 3127004)
- Four Rubber Feet (P/N 3270BF003)
- Power Cord (P/N 3127009)

- 2 Mounting Brackets (P/N 3265421@C)
- 4 Screws (P/N 3276003003)
- RJ-45 to DB-9 Adapter (P/N 3196ADPT001)
- The Total Access 600R base unit.

NOTE *Customers must supply the Ethernet cable.*

4. GROUNDING INSTRUCTIONS

The following provides grounding instruction information from the Underwriters' Laboratory UL 60950 Standard for Safety of Information Technology Equipment Including Electrical Business Equipment, with revisions dated March 15, 2002.

AC Power

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.

5. SUPPLYING POWER TO THE UNIT

AC Powered Systems

The AC powered unit comes equipped with a detachable power cord with a 3-prong plug for connecting to a grounded power receptacle. As shipped, the unit is set to factory default conditions. After installing the chassis, the unit is ready for power-up. To power-up the unit, ensure that the unit 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 unit's AC system must be from a grounded 90-125 VAC, 60 Hz source.*
- *The power receptacle uses double-pole, neutral fusing.*
- *Maximum recommended ambient operating temperature is 45 ºC.*

6. MOUNTING OPTIONS

The Total Access 600R comes equipped for table top or wallmount use. The unit is shipped with two wall-mount brackets (P/N 326542@C) and four screws (P/N 3276003003) which the customer must attach to the base unit for wallmount use.

WARNING

If wallmounted, the Total Access 600R must be mounted with the LEDs pointing down or sideways as shown in the mounting instructions (P/N 64200600L1#T-19A).

USER INTERFACE GUIDE

The User Interface Guide (UIG) section of the ADTRAN Total Access 600R 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.

SECTION INDEX

FIGURES

TABLES

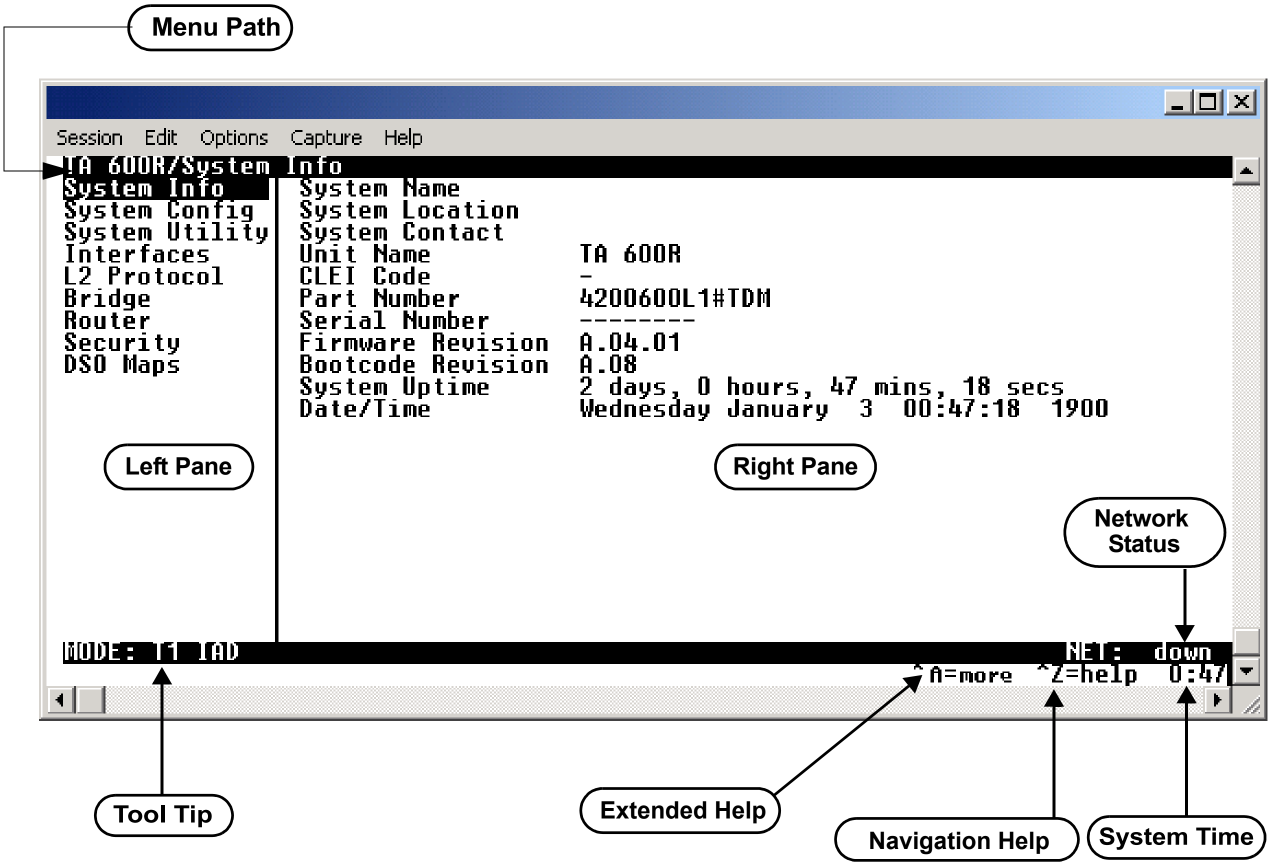
1. NAVIGATING THE TERMINAL MENU

Log in to the unit by connecting one end of the supplied silver cable to the RJ-45 interface labeled **CRAFT** (located on the rear of the unit) and the other to a RJ-45 to DB-9 adapter. Connect the DB-9 (female) to a VT100 terminal or PC with VT100 emulator software. 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. The default condition for the unit is no password, so the user can just press enter at the Login prompt. (Refer to *DLP-002*, *Logging in to the System,* for detailed instructions.)

Terminal Menu Window

The unit uses a multi-level menu structure that contains both menu items and data fields. All menu items and data fields display in the terminal menu window (see Figure 1), through which you have complete control of the unit.



```
TA 600R/System Info
System Info      System Name
System Config    System Location
System Utility   System Contact
Interfaces       Unit Name          TA 600R
L2 Protocol      CLEI Code          -
Bridge           Part Number        4200600L1#TDM
Router           Serial Number      --------
Security         Firmware Revision  A.04.01
DS0 Maps         Bootcode Revision  A.08
                 System Uptime      2 days, 0 hours, 47 mins, 18 secs
                 Date/Time          Wednesday January  3  00:47:18  1900

MODE: T1 IAD                                                  NET:  down
                                               ^A=more  ^Z=help   0:47
```

Figure 1. Top-Level Terminal Menu Window

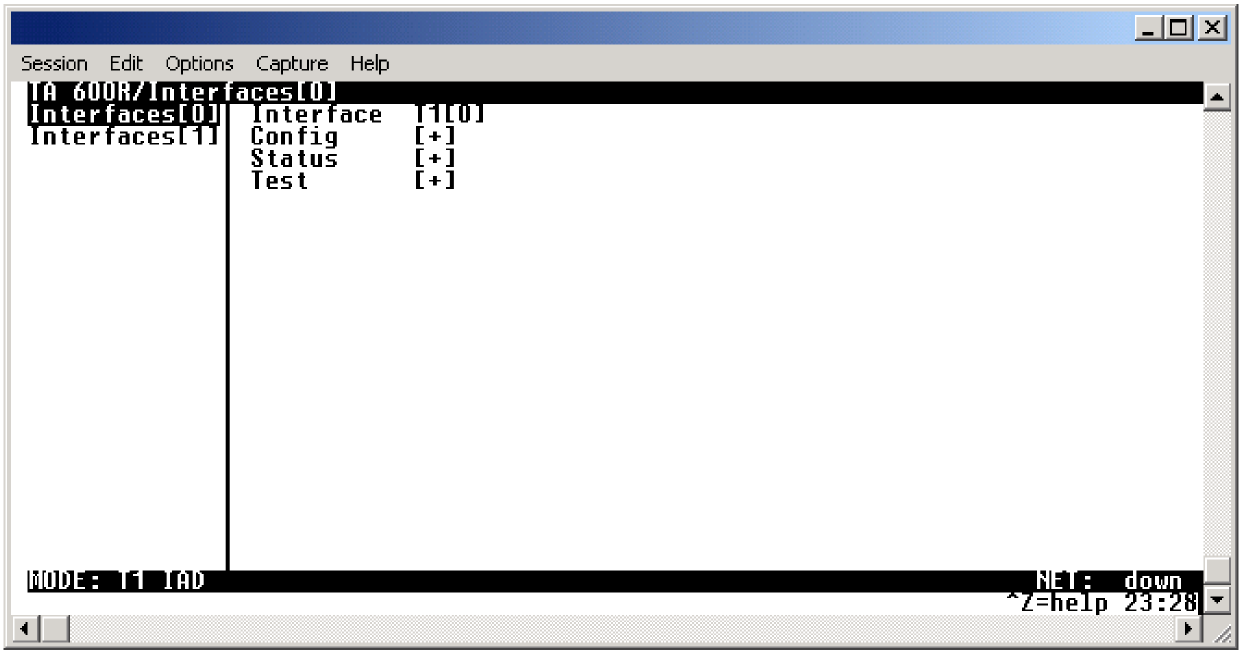
Menu Path

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 Info** submenu; therefore, the menu path reads **TA 600R/System Info**.

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 shows this alternate view. Fields and submenu names may vary slightly in this view.



```
TA 600R/Interfaces[0]
Interfaces[0]  Interface   T1[0]
Interfaces[1]  Config      [+]
               Status      [+]
               Test        [+]

MODE: T1 IAD                                              NET:  down
                                                       ^Z=help 23:28
```

Figure 2. Alternate Window 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, or Right arrow
Move from right pane to left pane	Tab, Escape, Left arrow, or Backspace
Move within each pane	Up/Down or Left/Right arrows

Right Window Pane Notation

The right window pane shows the contents of the currently selected menu. These contents can 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
<+>	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

- Tool Tip - provides a brief description of the currently selected mode
- Network Status - displays network status information, Up or Down
- Extended Help - displays information about selected commands (CTRL+A)
- Navigation Help - lists characters used for navigating the terminal menu and session management (CTRL+Z)
- System Time - displays current time

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

To do this...	Press this key...
Move between the left and right panes	Tab Arrows
Move to the top of a screen	A
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
Return to Login prompt (**CRAFT** port connection only)	Ctrl + L
Return to Login prompt (**CRAFT** port connection only)	Ctrl + S

Session Management Keystrokes

To do this...	Press this key...
Log out of a session (Telnet Connection)	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.	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.	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 **DS0** field in the **EDIT/VIEW MAP** screen, all of the information associated with the **DS0** is copied.	C

To do this...	Press this key...
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.	<
Insert a new list item. For example, add a new item to the **TELNET USER LIST** connection list by pressing <I> while the cursor is over the index number.	I
Delete a list item. For example, delete an item from the **TELNET USER LIST** connection list by pressing **<**D**>** while the index number is active.	D

2. TERMINAL MENU AND SYSTEM CONTROL

Selecting the Appropriate Menu

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

To do this...	Go to this menu...
Review and monitor general system information	**SYSTEM INFO**
Set up the management, syslog, and network time	**SYSTEM CONFIG**
Upgrade firmware, do config transfers, ping, traceroute, reset unit, and access terminal mode	**SYSTEM UTILITY**
Configure and monitor the T1 and Ethernet interfaces.	**INTERFACES**
Configure and monitor the L2 Protocol for the T1 and Ethernet interfaces	**L2 PROTOCOL**
Configure and monitor bridging parameters	**BRIDGE**
Define, configure, and monitor all router functions	**ROUTER**
Configure the filter defines and Radius server	**SECURITY**
Configure and apply DS0 maps	**DS0 MAPS**

Telnet Security Levels

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

Table 1. Telnet Password Security Levels

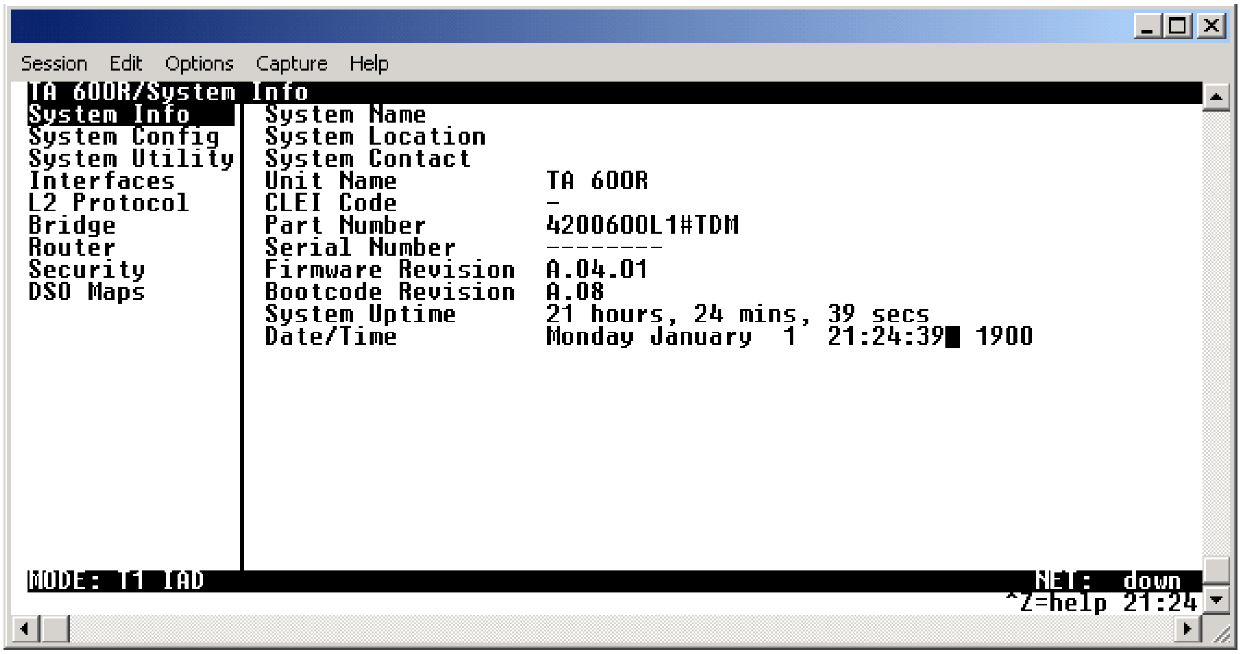
Security Level	**Description**
Full	The user has all access to view and configure all menus (same as logging in to the **CRAFT** port)
Support	The user has access to view **SYSTEM INFO**. The user has privileges to view and change everything under the **SYSTEM CONFIG** menu except for the **CRAFT** port 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 view only privileges of **SYSTEM INFO**. 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.
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.

3. MENU DESCRIPTIONS

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.

NOTE *All figures in this section will be representative of A.04.01 firmware or later.*



```
TA 600R/System Info
System Info     System Name
System Config   System Location
System Utility  System Contact
Interfaces      Unit Name          TA 600R
L2 Protocol     CLEI Code          -
Bridge          Part Number        4200600L1#TDM
Router          Serial Number      ---------
Security        Firmware Revision  A.04.01
DS0 Maps        Bootcode Revision  A.08
                System Uptime      21 hours, 24 mins, 39 secs
                Date/Time          Monday January  1  21:24:39█ 1900



MODE: T1 IAD                                              NET: down
                                                      ^Z=help 21:24
```

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 31 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. The factory default is to have no entry in the system name field.

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 31 alphanumeric characters in this field, including spaces and special characters (such as an underscore). The factory default is to have no entry in the system location field.

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 31 alpha-numeric characters in this field, including spaces and special characters (such as an underscore). The factory default is to have no entry in the system contact field.

System Info > Unit Name

Product-specific name for the unit.

System Info > CLEI Code

The CLEI code for the unit.

System Info > Part Number

ADTRAN part number for the unit.

System Info > Serial Number

The serial number field will reflect serial number located on bottom of the unit's chassis.

System Info > Firmware Revision

Displays the current firmware revision level of the unit.

System Info > Bootcode Revision

Displays the bootcode revision.

System Info > System Uptime

Displays the length of time since the last reboot of the unit.

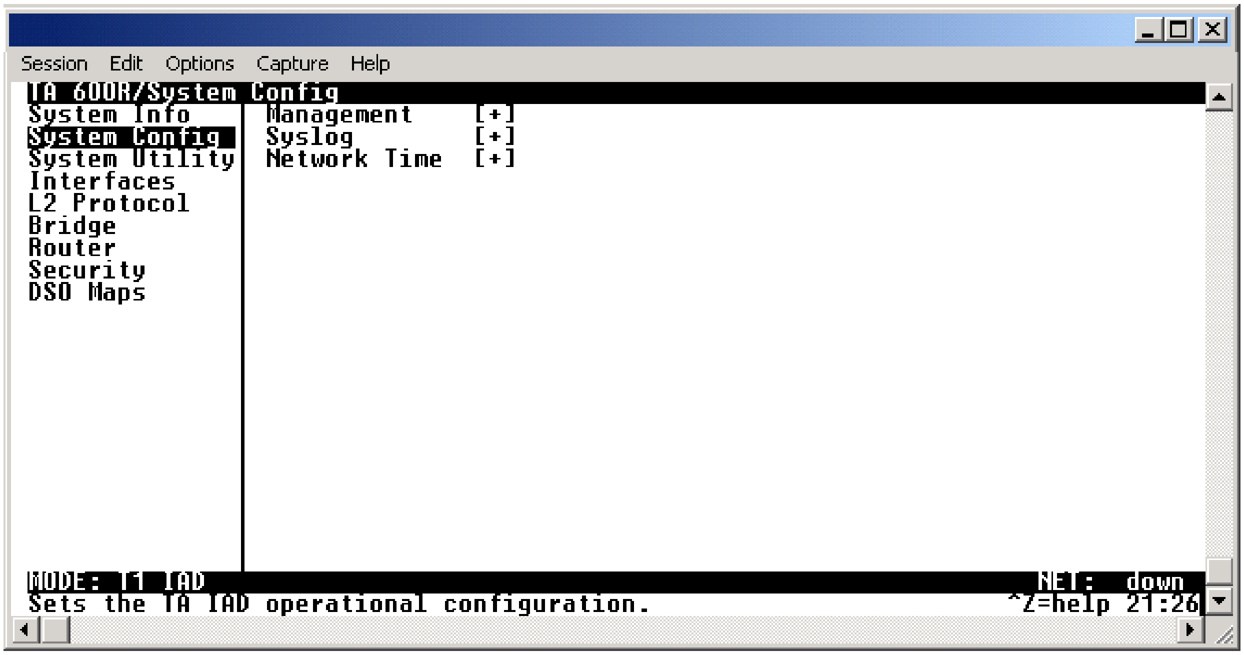
> NOTE *Each time you reset the system, this value resets to 0 days, 0 hours, 0 min. and 0 secs.*

System Info > Date/Time

Displays the current date and time, including seconds. This field can be edited. Enter the time in 24-hour format (such as 23:00:00 for 11:00 pm). Enter the date in mm-dd-yyyy format (for example, 10-30-1998).

SYSTEM CONFIG

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



```
TA 600R/System Config
System Info     Management     [+]
System Config   Syslog         [+]
System Utility  Network Time   [+]
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD                                                   NET:  down
Sets the TA IAD operational configuration.                ^Z=help 21:26
```

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.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PASSWORD PROTECT

The unit's VT100 **CRAFT** port can be accessed via an RJ-48 connector located on the rear of the unit.

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

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PASSWORD

This is the text string that is used for comparison when password protecting the **CRAFT** port. By default, no password is entered. You can enter up to 30 characters in this field. Table 2 provides instructions for changing the password.

*The security level for the **CRAFT** port is always set to **FULL**. This gives full access to all menus.*

Passwords are case-sensitive and can contain up to 30 alphanumeric characters (including spaces and special characters).

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 > 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**.

SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > DATA BITS

This is the asynchronous bit rate that the **CRAFT** port will run. The possible values are **7** or **8** (def) 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**.

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**.

SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS

Activate the Telnet access and set up the various Telnet parameters from this menu.

Firmware A.03.XX or previous supports one Telnet session active at a time. Firmware A.04.XX supports five simultaneous Telnet sessions.

SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > ACCESS

Sets **ACCESS** to **ON** or **OFF.** 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 **PASSWORD**, **RADIUS**, **PASSWORD/RADIUS**, and **RADIUS/PASSWORD**. **PASSWORD/RADIUS** indicates that the unit will try Password Authentication first, and if that fails it will try Radius Authentication. **RADIUS/PASSWORD** indicates that the unit will try Radius authentication first, and if that fails it will try Password authentication. The default is **PASSWORD**.

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. You can enter up to 15 characters in this field. The factory default is no entry in the **NAME** field.

PASSWORD

When the authenticating method is password, or password 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 1-255 minutes.

LEVEL

This is the security level granted to the user. Table 3 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 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.
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 > IP ACCESS LIST

Set up the list of allowed Telnet managers.

NETWORK ADDRESS AND MASK

Enter a network address and subnet mask 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 subnet mask of 0.0.0.0 will allow any host Telnet access, regardless of the network address. A network address of 0.0.0.0 with corresponding netmask 255.255.255.255 will not allow any host Telnet access.

The factory default is **0.0.0.0.** for both parameters, which will allow all users Telnet IP 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. The factory default is **ON**.

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 eight 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 **GET**.

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. 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. 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 is 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 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 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 255.255.255.252 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 > 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 53.*

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 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 and be one of the following names:

FATAL
ALERT
CRITICAL
ERROR
WARNING
NOTICE
INFO
DEBUG

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.

SYSTEM CONFIG > SYSLOG > DHCP LEVEL

Minimum required level for sending DHCP log messages.

SYSTEM CONFIG > SYSLOG > NTP LEVEL

Minimum required level for sending NTP log messages.

SYSTEM CONFIG > SYSLOG > TFTP LEVEL

Minimum required level for sending TFTP log messages.

SYSTEM CONFIG > SYSLOG > TELNET LEVEL

Minimum required level for sending TELNET log messages.

SYSTEM CONFIG > SYSLOG > IP LEVEL

Minimum required level for sending IP log messages.

SYSTEM CONFIG > SYSLOG > PPP LEVEL

Minimum required level for sending PPP log messages.

SYSTEM CONFIG > SYSLOG > NAT LEVEL

Minimum required level for sending NAT log messages.

SYSTEM CONFIG > SYSLOG > ARP LEVEL

Minimum required level for sending ARP log messages.

SYSTEM CONFIG > SYSLOG > UDP LEVEL

Minimum required level for sending UDP log messages.

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.

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.

SYSTEM CONFIG > SYSLOG > ROUTER LEVEL

Minimum required level for sending router log messages.

SYSTEM CONFIG > SYSLOG > NONVOL LEVEL

Minimum required level for sending nonvolatile memory log messages.

SYSTEM CONFIG > SYSLOG > NOKIA LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > AUTOBAUD LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > TOLLBRG LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > CMCP LEVEL

(This parameter is not applicable for the Total Access 600R.)

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.

SYSTEM CONFIG > SYSLOG > ETH LEVEL

Minimum required level for sending log messages about Ethernet physical connection.

SYSTEM CONFIG > SYSLOG > ICMP LEVEL

Minimum required level for sending ICMP log messages.

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 DS0 mapping.

SYSTEM CONFIG > SYSLOG > SELFTEST LEVEL

Minimum required level for sending log messages about selftest.

SYSTEM CONFIG > SYSLOG > VOICE LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > JETSTREAM LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > POTS LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > LESCAS LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > ATM LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > COPPERCOM LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > VOFR LEVEL

(This parameter is not applicable for the Total Access 600R.)

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.

SYSTEM CONFIG > SYSLOG > BRIDGE LEVEL

Minimum required level for sending bridge mode log messages.

SYSTEM CONFIG > SYSLOG > MAINT LEVEL

Minimum required level for sending **CRAFT** port log messages.

SYSTEM CONFIG > SYSLOG > HDLC LEVEL

Minimum required level for sending low level HDLC log messages.

SYSTEM CONFIG > SYSLOG > VOATM LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > PPPOA LEVEL

(This parameter is not applicable for the Total Access 600R.)

SYSTEM CONFIG > SYSLOG > FDL LEVEL

Minimum required level for sending FDL 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

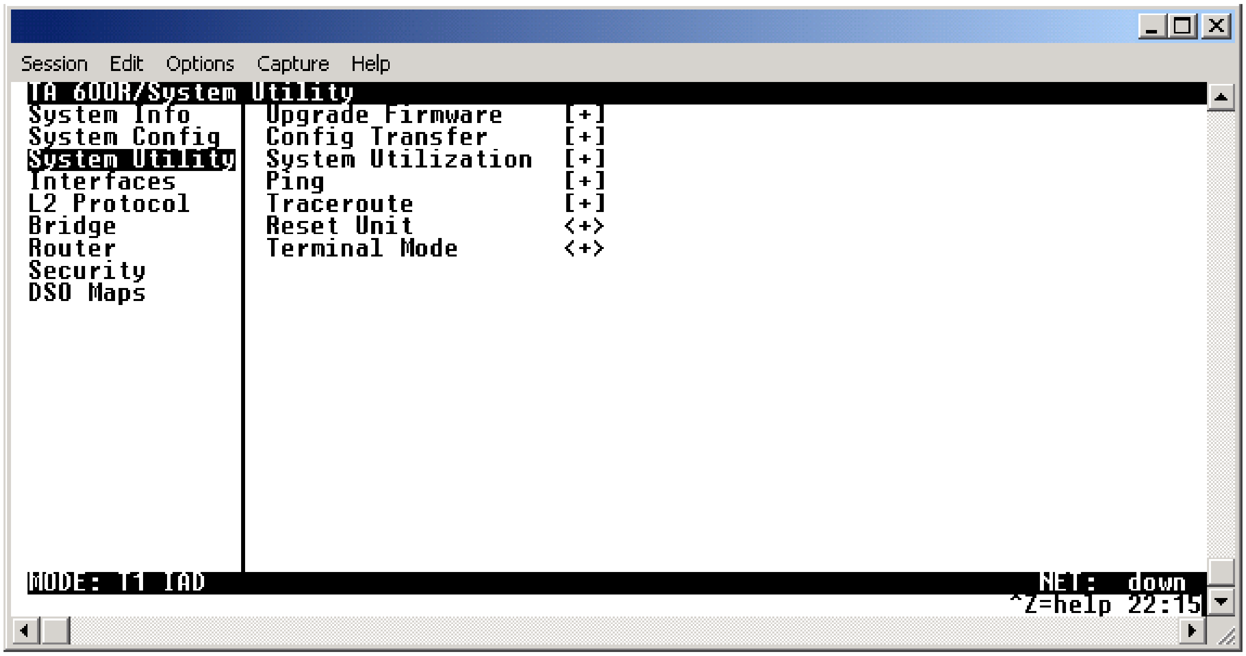
This is the interval of time between each request the unit sends out to the time server. A smaller refresh time guarantees that the unit receives the correct time from the server and corrects possible errors more quickly. This may be more taxing on the machine. A range of refresh times is available for 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.



```
TA 600R/System Utility
System Info      Upgrade Firmware     [+]
System Config    Config Transfer      [+]
System Utility   System Utilization   [+]
Interfaces       Ping                 [+]
L2 Protocol      Traceroute           [+]
Bridge           Reset Unit           <+>
Router           Terminal Mode        <+>
Security
DS0 Maps

MODE: T1 IAD                                           NET:  down
                                                    ^Z=help 22:15
```

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.

> *Before using* **Start Transfer***, the unit should have a valid IP address, subnet mask, and default gateway (if required). See DLP-004, Setting Ethernet 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.

System Utility > Config Transfer > Transfer Method

Sends a 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 default gateway (if required). See DLP-004, Setting Ethernet 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 > 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.

> CAUTION
>
> *If you execute this command, the unit retrieves the configuration file, the WAN link is reset, and the unit starts using the new configuration.*

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.

> CAUTION
>
> *Before using this command, you must have identified a valid TFTP server in* **TFTP Server 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 > Total Avg CPU Utilization

Total Avg CPU Utilization is a running total of CPU utilization since the last reset.

System Utility > System Utilization > Performance > Current Avg CPU Utilization

Current Avg CPU Utilization is the running total of CPU utilization since the last clear.

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.*

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 > Source Address

Selects whether the ping packet should use the **Interface** address or the **NAPT** (if that interface uses NAT) as the source address of the ping packet. This is the address that is used for ICMP requests. **Interface** means it will use the IP address associated with the WAN for outgoing packets and the Ethernet IP address for ICMP requests made on the LAN. **NAPT Address** will replace the WAN IP address with the NAPT address for outgoing ICMP requests. Default is **Interface**.

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 every 2 seconds. 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

Activator to begin the traceroute process by sending a probe datagram with a Time To Live (TTL) value of 1.

SYSTEM UTILITY > RESET UNIT

Selecting this activator will power reset the unit.

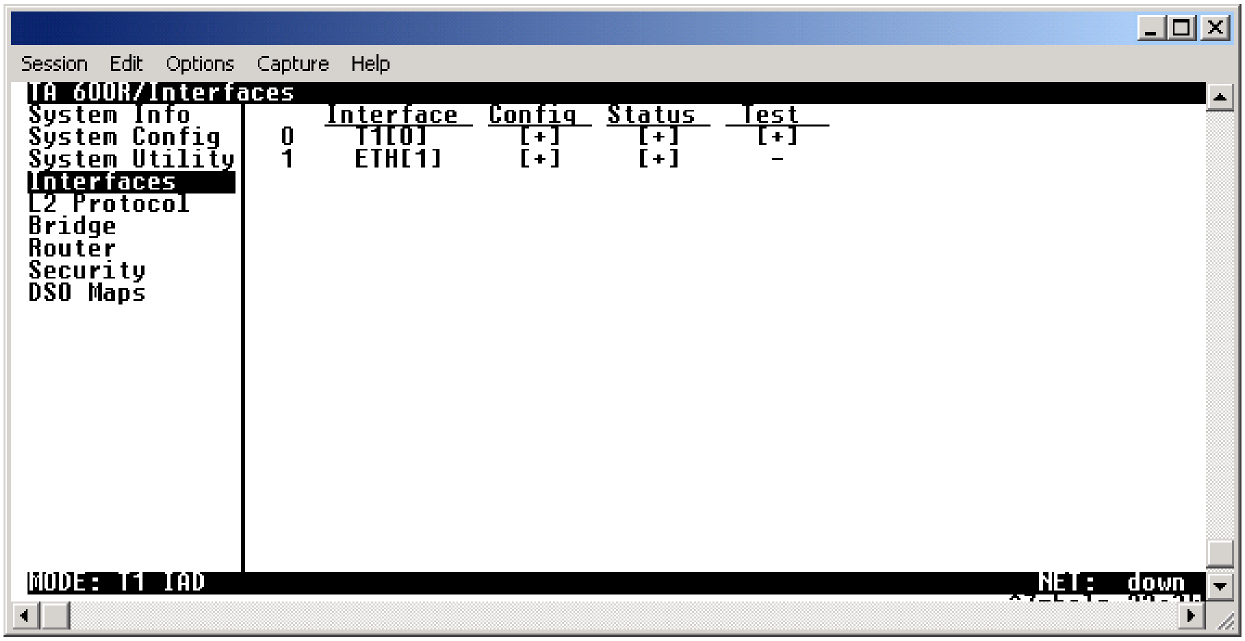
SYSTEM UTILITY > TERMINAL MODE

The terminal mode gives the user a command-line prompt. From this prompt, you can:

- Perform a reset with the command "reset"
- Perform a 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-013, *Saving and Loading Text Configuration Using the 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, (*See* DLP-014, *Unit Installation Using The Auto-Config Feature* for details.)

INTERFACES

Use the **INTERFACES** menu to view and configure parameters for the T1 and Ethernet interfaces as shown in Figure 6.



```
TA 600R/Interfaces
System Info          Interface  Config  Status   Test
System Config     0    T1[0]     [+]     [+]     [+]
System Utility    1    ETH[1]    [+]     [+]      -
Interfaces
L2 Protocol
Bridge
Router
Security
DSO Maps

MODE: T1 IAD                                             NET:  down
```

Figure 6. Interfaces Menus

INTERFACES (T1[0])

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

The 0 in T1[0] represents a physical port. The T1 physical port is always 0.

INTERFACES (T1[0]) > CONFIG

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

INTERFACES (T1[0]) > CONFIG > TIMING MODE

Choices are **NETWORK** and **INTERNAL**. Select **NETWORK** when the unit will receive timing from the network. Select **INTERNAL** when the unit will generate the timing. Default is **NETWORK**.

INTERFACES (T1[0]) > 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**, **SF**, **SLC96 ALARM-16**, and **SLC96 ALARM-13**. Extended Superframe (**ESF**) provides a non-disruptive means of full-time monitoring on the facility datalink (FDL). Default is **ESF**.

> NOTE **SF** *is equivalent to the D4 frame format.*

INTERFACES (T1[0]) > 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[0]) > 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[0]) > CONFIG > CSU LPBK

Choices are **ENABLE**, **DISABLE**, and **DISABLE ALL**. Default is **ENABLE**. This allows the unit to either respond or not respond to CSU loop up commands.

INTERFACES (T1[0]) > STATUS

Displays the T1 status including performance data and alarm histories.

INTERFACES (T1[0]) > STATUS > PERFORMANCE

Displays the T1 performance data.

INTERFACES (T1[0]) > STATUS > PERFORMANCE > TIME FRAME

Choices are **CURRENT**, **15 MIN**, and **24 HR**. Default is **CURRENT**. The performance fields -- either **CURRENT**, **15 MIN**, or **24 HR**. -- provide status on key performance measures as specified in ANSI T1.403 and AT&T TR 54016 for each of the T1 ports. When **CURRENT** is chosen, the performance data for the current 15 minute window is shown.

INTERFACES (T1[0]) > STATUS > PERFORMANCE > CLEAR

Clears information for the selected port. Press **<Enter>** when the cursor is over this field to clear the data.

INTERFACES (T1[0]) > STATUS > PERFORMANCE > 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[0]) > STATUS > PERFORMANCE > 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[0]) > STATUS > PERFORMANCE > SEF

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

INTERFACES (T1[0]) > STATUS > PERFORMANCE > FS

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

INTERFACES (T1[0]) > STATUS > PERFORMANCE > 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[0]) > STATUS > PERFORMANCE > 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[0]) > STATUS > PERFORMANCE > UAS

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

INTERFACES (T1[0]) > STATUS > ALARMS

Displays current alarms and alarm history for T1 interface.

INTERFACES (T1[0]) > 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).
YELLOW	Remote alarm indicator (RAI) being received on port.
BLUE	Receiving unframed all ones from the port alarm indicator signal (AIS).

INTERFACES (T1[0]) > 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.

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).
YELLOW	Remote alarm indicator (RAI) being received on port.
BLUE	Receiving unframed all ones from the port alarm indicator signal (AIS).

INTERFACES (T1[0]) > STATUS > ALARMS > CLEAR HISTORY

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

INTERFACES (T1[0]) > TEST

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

INTERFACES (T1[0]) > 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. **PAYLOAD** Loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

INTERFACES (T1[0]) > TEST > REM LB

Loopback of remote 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. **PAYLOAD** Loopback is similar to line loopback except that the framing is extracted from the received data and then regenerated for the transmitted data. **NONE** disables the loopback test. Default is **NONE**.

INTERFACES (T1[0]) > TEST > TEST STATUS

Indicates whether a test is in progress.

INTERFACES (ETH[1])

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

> NOTE *The 1 in ETH[1] represents a physical port. The Ethernet physical port is always 1.*

INTERFACES (ETH[1]) > CONFIG

Enable the **AUTONEGOTIATION** and configure the Ethernet rate from this menu.

INTERFACES (ETH[1]) > CONFIG > AUTONEGOTIATION

If set to **ON**, **AUTONEGOTIATION** automatically detects 10 or 100 Mb Ethernet and negotiates the duplex setting. **ON** is the default setting.

INTERFACES (ETH[1]) > CONFIG > DATA RATE

(This option is only available if ***AUTONEGOTIATION*** *is set to* ***OFF****.)* **DATA RATE** sets the speed of the Ethernet interface. Choices are **10BASET** and **100BASET**. The default value is **10BASET**.

INTERFACES (ETH[1]) > CONFIG > DUPLEX TYPE

(This option is only available if ***AUTONEGOTIATION*** *is set to* ***OFF****.)* **DUPLEX TYPE** configures the Ethernet interface for **FULL DUPLEX** or **HALF DUPLEX**. **FULL DUPLEX** allows the Ethernet interface to send and receive simultaneously. **HALF DUPLEX** allows the Ethernet interface to either send or receive at any given moment, but not simultaneously. The default is **HALF DUPLEX**.

> NOTE *If the* **DATA RATE** *is set to* **10BASET** *or* **100BASET***, the* **DUPLEX TYPE** *must be configured as* **FULL DUPLEX** *or* **HALF DUPLEX**.

INTERFACES (ETH[1]) > STATUS

Displays the **MAC ADDRESS**, **DATA LINK**, **DATA RATE**, and **DUPLEX TYPE**.

INTERFACES (ETH[1]) > STATUS > MAC ADDRESS

This is a read-only field which displays the unique MAC address programmed at ADTRAN.

INTERFACES (ETH[1]) > STATUS > DATA LINK

Displays the status of the data link as up or down. This is a read-only field.

INTERFACES (ETH[1]) > STATUS > DATA RATE

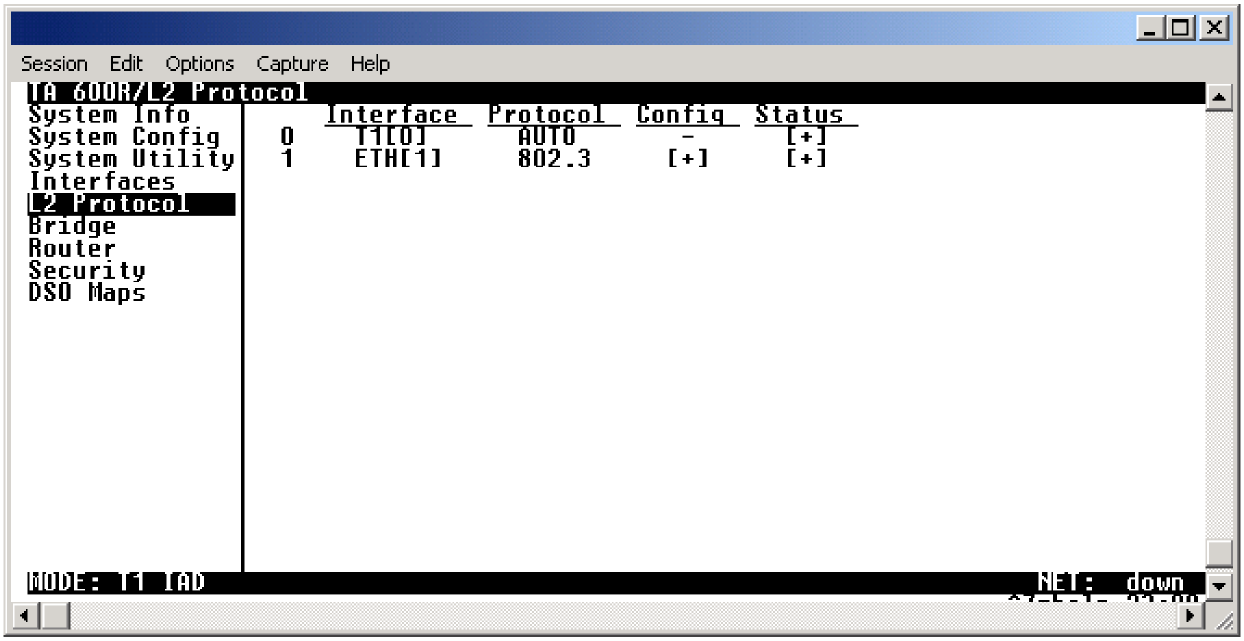
Displays the data rate present on the Ethernet interface. The possibilities are **10BASET**, **100BASET**, and **N/A**. **N/A** indicates the **AUTONEGOTIATION** is set to **ON** and there is no Ethernet connection. This is a read-only field.

INTERFACES (ETH[1]) > STATUS > DUPLEX TYPE

Displays the duplex type present on the Ethernet interface. The possibilities are **FULL DUPLEX** and **HALF DUPLEX**. This is a read-only field.

L2 PROTOCOL

Use the L2 Protocol menu to select the L2 Protocol, configure the protocol specific parameters, and view the status as shown in Figure 7.



```
TA 600R/L2 Protocol
System Info       Interface  Protocol  Config  Status
System Config  0    T1[0]      AUTO      -      [+]
System Utility 1    ETH[1]     802.3    [+]     [+]
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD                                          NET: down
```

Figure 7. L2 Protocol Menu

L2 PROTOCOL (T1[0])

Configure the L2 Protocol and view the status parameters from this menu.

The 0 in T1[0] represents a physical port. The T1 physical port is always 0.

L2 PROTOCOL (T1[0]) > PROTOCOL

Configure the L2 Protocol mode. Choices are **PPP**, **FRE**, and **AUTO**. The default is **AUTO**. Selecting **AUTO** enables the Auto-config feature. Reference *DLP-014, Unit Installation Using The Auto-Config Feature*, for more information.

L2 PROTOCOL (T1[0]) > 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 detection while Serial Line Internet Protocol (SLIP) and other protocols do not.

L2 PROTOCOL (T1[0]) > 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 cyclic redundancy check (CRC) for detecting bad data, but leaves the error correction algorithms to be performed by the 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 (T1[0]) > 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. Reference DLP-014, Unit Installation Using The Auto-Config Feature, for more information.*

L2 PROTOCOL (T1[0] - PPP)

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

L2 PROTOCOL (T1[0] - PPP) > CONFIG

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

L2 PROTOCOL (T1[0] - 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 (T1[0] - 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 (T1[0] - 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 (T1[0] - PPP) > Config > Authentication > Tx Username

*(This option is not available when the **TX Method** is set to **None**.)*

This is the username that is used when being authenticated by the PPP peer. You can enter up to 31 characters in this field. Default is no entry in the **TX Username** field.

L2 Protocol (T1[0] - PPP) > Config > Authentication > Tx Password

*(This option is not available when the **TX Method** is set to **None**.)*

This is the password or secret that is used when being authenticated by the PPP peer. You can enter up to 30 characters in this field. Default is no password.

L2 PROTOCOL (T1[0] - PPP) > CONFIG > AUTHENTICATION > RX 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	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.

L2 PROTOCOL (T1[0] - PPP) > CONFIG > AUTHENTICATION > RX USERNAME

(This option is not available when the ***RX METHOD*** *is set to none.)*
This is the username used to authenticate the PPP peer. You can enter up to 31 characters in this field. Default is no entry in the **RX USERNAME** field.

L2 PROTOCOL (T1[0] - PPP) > CONFIG > AUTHENTICATION > RX PASSWORD

(This option is not available when the ***RX METHOD*** *is set to none.)*
This is the password or secret that is used to authenticate the PPP peer. You can enter up to 30 characters in this field. Default is no password.

L2 PROTOCOL (T1[0] - 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 (T1[0] - 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** (default).

L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > 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 (DEFAULT) 5 SECS**, and **10 SECS**.

L2 PROTOCOL (T1[0] - 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 (DEFAULT)**, **10**, **15**, and **20**.

L2 PROTOCOL (T1[0] - PPP) > CONFIG > PPP > FORCE PEER IP ADDRESS

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

L2 PROTOCOL (T1[0] - PPP) > STATUS

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

L2 PROTOCOL (T1[0] - PPP) > STATUS > LCP

Link Control Protocol. Reflects LCP layer active.

L2 PROTOCOL (T1[0] - PPP) > STATUS > BCP

Shows UP if PPP Bridge Control Protocol has negotiated successfully.

L2 PROTOCOL (T1[0] - PPP) > STATUS > IPCP

Shows UP if PPP IP Control Protocol has negotiated successfully.

L2 PROTOCOL (T1[0] - PPP) > STATUS > UP TIME

Displays how long the PPP session has been connected.

L2 PROTOCOL (T1[0] - PPP) > STATUS > TX PKTS

Number of packets transmitted.

L2 PROTOCOL (T1[0] - PPP) > STATUS > RX PKTS

Number of packets received.

L2 PROTOCOL (T1[0] - PPP) > STATUS > TX BYTES

Number of bytes transmitted.

L2 PROTOCOL (T1[0] - PPP) > STATUS > RX BYTES

Number of bytes received.

L2 PROTOCOL (T1[0] - PPP) > STATUS > CLEAR STATS

Selecting this activator will clear the PPP stats.

L2 PROTOCOL (T1[0] - FRE)

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

L2 PROTOCOL (T1[0] - FRE) > CONFIG

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

L2 PROTOCOL (T1[0] - 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) This is 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 Data Link Connection Identifiers (DLCIs) are assigned in the DLCI Mapping and must be the same for the device it will communicate with.

The default value is **ANNEX D (ANSI)**.

L2 PROTOCOL (T1[0] - 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 (T1[0] - 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 static is used, the unit will poll the switch to determine which DLCIs are active. These active DLCIs will attempt to determine the IP addresses on the other end of the virtual circuit using Inverse ARP (IARP). If there is a response, the network learned will be added to the router tables and the virtual circuit will be treated as an unnumbered interface. Bridge connections are made using bridge group 1. When more than one DLCI mapping is listed, the unit will try to match the DLCIs learned from the Frame Relay switch with the DLCI values in the map. If there is a match, the protocols specified in the map are used. However, if an active DLCI is not in the list, the unit looks for an entry that has 0 in the DLCI field. This entry is considered the default entry to use when no match occurs. If this default entry is not present, the unit falls back to using IARP to determine the protocols to use with that particular virtual circuit. If a static maintenance protocol is used, at least one DLCI mapping must be specified.

> 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 (T1[0] - FRE) > CONFIG > DLCI MAPPING > NUM

Displays the index number in the DLCI mapping table.

L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING > 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 (T1[0] - 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 (T1[0] - FRE) > CONFIG > DLCI MAPPING > DLCI

The DLCI number identifies the virtual circuit being configured.

L2 PROTOCOL (T1[0] - FRE) > CONFIG > DLCI MAPPING > MODE

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

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

The default is **ROUTE IP.**

L2 PROTOCOL (T1[0] - FRE) > CONFIG > 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** msec.

L2 PROTOCOL (T1[0] - FRE) > STATUS

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

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT

View the Frame Relay statistics on the WAN port.

L2 PROTOCOL (T1[0] - 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 (T1[0] - FRE) > STATUS > PORT > SIGNAL STATE

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

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > TX FRAMES

Total frames transmitted out the WAN port.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > RX FRAMES

Total frames received on the WAN port.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > TX BYTES

Total bytes transmitted out the WAN port.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > RX BYTES

Total bytes received on the WAN port.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > FULL STATUS TX FRAMES

Number of full status frames transmitted out the WAN port.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > FULL STATUS RX FRAMES

Number of full status frames received on the WAN port.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > LINK INTEGRITY STATUS TX FRAMES

Number of Link-Integrity (LI) only frames transmitted out the WAN port.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > LINK INTEGRITY STATUS RX FRAMES

Number of LI only frames received on the WAN port.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > DROP UNKNOWN DLCI

Number of frames received that were not associated with any known PVC.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > DROP INVALID DLCI

Number of frames received that had illegal DLCIs.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PORT > CLEAR STATS

Selecting this activator will clear the port Frame Relay Statistics.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S

View the Frame Relay status on a per-PVC basis.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > DLCI

The DCLI number identifies the virtual circuit being monitored.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > STATE

The state of the virtual circuit:

INACTIVE	The circuit exists but has been deactivated by the Frame Relay switch.
EXISTS	The circuit exists at this point and should be activated soon.
ACTIVE	The circuit is fully active.
OFF	The circuit has been turned off by the DLCI mapping active selection.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > TX FRAMES

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

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > RX FRAMES

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

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > TX BYTES

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

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > RX BYTES

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

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > DE COUNT

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

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > CR COUNT

Number of packets received on this DLCI with the command response (CR) bit set.

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > BECN COUNT

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

L2 PROTOCOL (T1[0] - FRE) > STATUS > PVC'S > FECN COUNT

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

L2 PROTOCOL (T1[0] - 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 (T1[0] - AUTO)

View the status of the T1 interface with the **L2 PROTOCOL** set to **AUTO** (using Auto-config feature). Reference *DLP-014, Unit Installation Using The Auto-Config Feature,* for further details.

L2 PROTOCOL (T1[0] - 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 (T1[0] - AUTO) > STATUS > STATE

This field represents the state of the auto-detect/configuration function. The possible states 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 (T1[0] - AUTO) > STATUS > TX PKTS

Number of packets transmitted out of the WAN port.

L2 PROTOCOL (T1[0] - AUTO) > STATUS > RX PKTS

Number of packets received on the WAN port.

L2 PROTOCOL (T1[0] - AUTO) > STATUS > TX BYTES

Number of bytes transmitted out of the WAN port.

L2 PROTOCOL (T1[0] - AUTO) > STATUS > RX BYTES

Number of bytes received out the WAN port.

L2 PROTOCOL (T1[0] - AUTO) > STATUS > CLEAR STATS

Selecting this activator will clear the statistics.

L2 PROTOCOL (ETH[1])

Configure the **L2 PROTOCOL** parameters and view the status of the Ethernet interface from this menu.

> NOTE *The 1 in ETH[1] represents a physical port. The Ethernet physical port is always 1.*

L2 PROTOCOL (ETH[1]) > PROTOCOL

Displays the L2 Protocol for the **10/100BASET** Ethernet port. Currently only 802.3 is supported.

L2 PROTOCOL (ETH[1]) > CONFIG

Configure the mode for this **10/100BASET** Ethernet port from this menu.

L2 PROTOCOL (ETH[1]) > CONFIG > MODE

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

ROUTE IP	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.

The default is **ROUTE IP.**

L2 PROTOCOL (ETH[1]) > STATUS

View the L2 Protocol statistics for the **10/100BASET** Ethernet port from this menu.

L2 PROTOCOL (ETH[1]) > STATUS > TX PACKETS

Total number of packets transmitted out the Ethernet port.

L2 PROTOCOL (ETH[1]) > STATUS > RX PACKETS

Total number of packets received from the Ethernet port.

L2 PROTOCOL (ETH[1]) > STATUS > TX ERRORS

Total number of transmit errors encountered on Ethernet port.

L2 PROTOCOL (ETH[1]) > STATUS > SINGLE COLLISIONS

Total number of single collisions before successful transmission.

L2 PROTOCOL (ETH[1]) > STATUS > MULTIPLE COLLISIONS

Total number of multiple collisions before successful transmission.

L2 PROTOCOL (ETH[1]) > STATUS > EXCESSIVE COLLISIONS

Total number of collisions that resulted in packet being dropped.

L2 PROTOCOL (ETH[1]) > STATUS > DEFERRED TRANSMISSIONS

Total number of packets deferred due to collisions.

L2 PROTOCOL (ETH[1]) > STATUS > CARRIER SENSE ERRORS

Total number of carrier sense errors encountered (no link integrity).

L2 PROTOCOL (ETH[1]) > STATUS > RX ERRORS

Number of packets received in error and dropped.

L2 PROTOCOL (ETH[1]) > STATUS > CRCS

Number of packets detected with CRC errors.

L2 PROTOCOL (ETH[1]) > STATUS > RX COLLISIONS

Number of collisions which occurred during reception.

L2 PROTOCOL (ETH[1]) > STATUS > NON-ALIGNED

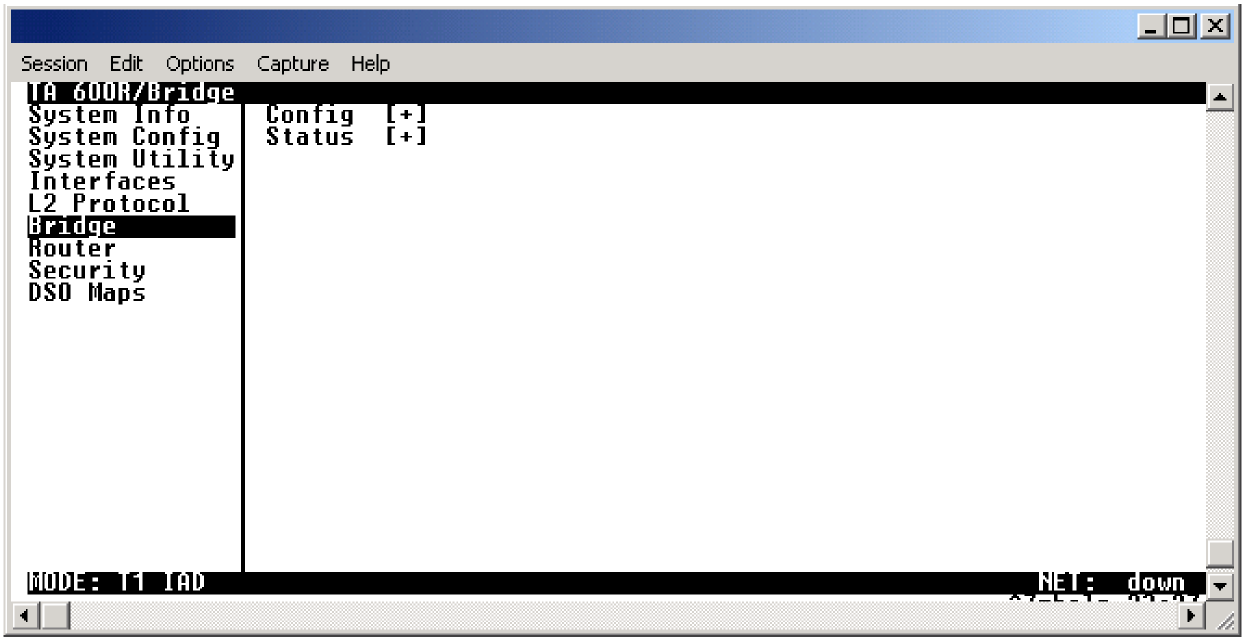
The **NON-ALIGNED** parameter is set when the number of bits received is not divisible by 8.

L2 PROTOCOL (ETH[1]) > 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 8.



```
TA 600R/Bridge
System Info        Config   [+]
System Config      Status   [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD                                                    NET:  down
```

Figure 8. Bridge Menu

BRIDGE > CONFIG

Configure the interfaces and bridge table parameters from this menu.

BRIDGE > CONFIG > INTERFACES (T1[0])

Configure the T1 interface bridging parameters from this menu.

> NOTE
>
> *The T1[0] interface will not appear as a bridge interface entry if the mode is set to route IP.*

BRIDGE > CONFIG > INTERFACES (T1[0]) > SUB-INTERFACE

The T1 sub-interface is PPP [0.0] if the **L2 PROTOCOL** is set for **PPP**. The [0.0] represents the T1 physical and logical ports, respectively. This is a read-only field. The T1 sub-interface is **FRE [0.X]** if the **L2 PROTOCOL** is set for **FRAME RELAY**. The [0.X] represents the T1 physical and logical ports, respectively. The T1 physical port is always 0. The X represents the Frame Relay logical port and will be a number between 0-9 corresponding to the interface number under **L2 PROTOCOL > CONFIG > DLCI MAPPING**. This is a read-only field.

BRIDGE > CONFIG > INTERFACES (ETH[1])

Configure the Ethernet Bridging parameters from this menu.

> NOTE *The ETH[1] interface will not appear as a bridge interface entry if the mode is set to route IP.*

BRIDGE > CONFIG > INTERFACES (ETH[1]) > SUB-INTERFACE

The Ethernet sub-interface is 802.3[1.0]. The [1.0] represents the Ethernet physical and logical ports, where 1 is the physical port and 0 is the logical port assigned to the Ethernet interface. This is a read-only field.

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

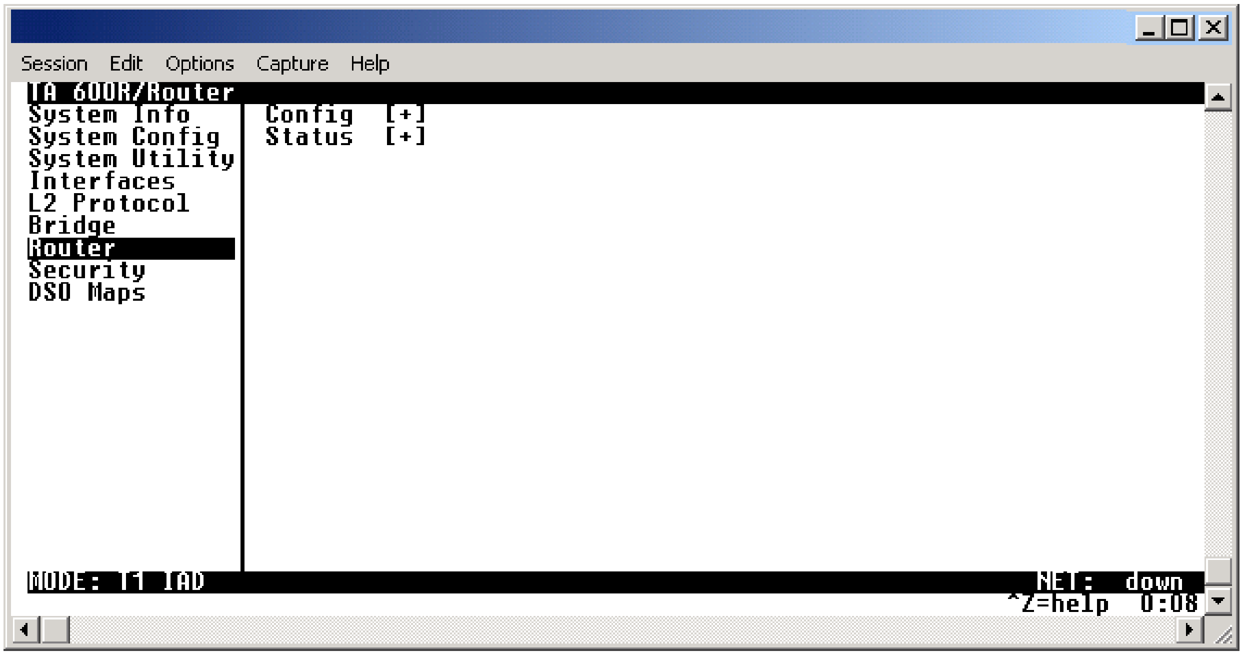
Location indicates if it is LAN or WAN. This is a read-only field.

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 9.



```
TA 600R/Router
System Info      Config   [+]
System Config    Status   [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security
DSO Maps

MODE: T1 IAD                                  NET:  down
                                            ^Z=help  0:08
```

Figure 9. 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 T1 interfaces from this menu.

ROUTER > CONFIG > INTERFACES (ETH[1])

Configure the layer 3 options for the Ethernet parameters from this menu.

NOTE *The 1 in ETH[1] represents a physical port. The Ethernet physical port will always be 1.*

NOTE *The Ethernet port will always appear in the* **ROUTER > CONFIG > INTERFACES** *table regardless of the L2 Protocol mode setting.*

ROUTER > CONFIG > INTERFACES (ETH[1]) > SUB-INTERFACE

The Ethernet sub-interface is 802.3[1.0]. The [1.0] represents the Ethernet physical and logical ports, where 1 is the physical port and 0 is the logical port assigned to the Ethernet interface. This is a read-only field.

ROUTER > CONFIG > INTERFACES (ETH[1])> SETUP

Configure the Ethernet addressing, RIP, and Proxy ARP from this menu.

PRIMARY IP

This is used to set up 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.

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 IP

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**.

ROUTER > CONFIG > INTERFACES (T1[0])

Configure the T1 interface parameters from this menu.

> *The 0 in T1[0] represents a physical port. The T1 physical port will always be 0.*

> *The T1 interface will not appear in the **ROUTER > CONFIG > INTERFACES** table if the **L2 PROTOCOL MODE** is set for **BRIDGE ALL**. The T1 interface will not appear if a DLCI is not entered in the **DLCI MAPPING** table (**L2 PROTOCOL (T1[0]-FRE) > CONFIG > DLCI MAPPING**) when the **L2 PROTOCOL** is set to Frame Relay (**FRE**).*

ROUTER > CONFIG > INTERFACES (T1[0])> SUB-INTERFACE

The T1 sub-interface is PPP [0.0] if the L2 Protocol is set for **PPP**. The [0.0] represents the T1 physical and logical ports, respectively. This is a read-only field.

The T1 sub-interface is FRE [0.X] if the L2 Protocol is set for **FRAME RELAY**. The [0.X] represents the T1 physical and logical ports, respectively. The T1 physical port is always 0. The X represents the Frame Relay logical port and will be a number between 0-9 corresponding to the interface number under **L2 PROTOCOL** > **CONFIG** > **DLCI MAPPING**. This is a read-only field.

ROUTER > CONFIG > INTERFACES (T1[0]) > SET-UP

Configure the addressing, address mode, MTU, NAT, and RIP parameters from this menu.

ACTIVE

This option allows this DLCI to be assumed as active (set to **YES**) and begin transmitting data packets. If set to **NO**, the interface will not be put in the route table and will not be seen by other devices on the network. This can be set to **NO** if waiting on future turnup from Frame Relay provider. Default is set to **YES**.

DLCI

*(This option is only available when the **L2 PROTOCOL** is set to **FRAME RELAY**.)* This DLCI is the number associated with the virtual circuit on the T1 interface. This number corresponds to the DLCI number in the **L2 PROTOCOL > CONFIG > DLCI MAPPING** table.

ADDRESS MODE

This option determines how the WAN interface receives its IP address. **USER SPECIFIED** is the normal mode of operation.

- The choices are **USER SPECIFIED** (default) and **IPCP ASSIGNED** if the **L2 PROTOCOL** is set to **PPP**.
- The choices are **USER SPECIFIED** (default), **IARP**, and **DHCP CLIENT** if the **L2 PROTOCOL** is set to **FRAME RELAY**. **IARP** can be used to learn the far-end IP address.
- If using the Auto-config option and the **L2 PROTOCOL** is **PPP**, the default is **IPCP ASSIGNED**. This means the unit will learn its IP address from a router on the WAN during IPCP negotiation. It is the same mechanism used by the auto-detection algorithm.
- If using the Auto-config option and the **L2 PROTOCOL** is **FRAME RELAY**, the default is **DHCP CLIENT**. This means a DHCP Server from the service provider will issue this unit an IP address using DHCP.
- If the Auto-config option is not used, the **USER SPECIFIED** option for both **PPP** and **FRAME RELAY** allows the IP addresses to be statically programed into the unit.

LOCAL IP ADDRESS

*(This option is only applicable in **USER SPECIFIED** address mode.)* For **PPP**, this IP address is the local WAN IP address and can be statically assigned if using numbered interfaces. For **FRAME RELAY**, this is the numbered IP associated with this DLCI interface. This address is used by the unit to respond to Inverse ARP requests. If this IP address is left as **0.0.0.0**, the link is treated as unnumbered and the unit responds to the Inverse ARP with its Ethernet IP address. Default is **0.0.0.0.**

IP NETMASK

*(This option is not available for **FRAME RELAY DHCP CLIENT ADDRESS MODE**.)* For Frame Relay, the IP netmask which is applied to the **FAR-END IP ADDRESS** and **LOCAL IP ADDRESS** is specified here. Default is **0.0.0.0.** For the PPP protocol, this network mask is applied to the **FAR-END IP ADDRESS** for determining the PPP peer's network. If left as **0.0.0.0**, a standard network mask is used. Default is **0.0.0.0.**

FAR-END IP ADDRESS

*(This option is not available for **FRAME RELAY DHCP CLIENT ADDRESS MODE, FRAME RELAY IARP ADDRESS MODE**, or **PPP IPCP ASSIGNED ADDRESS MODE**.)* For Frame Relay, this is the IP address of the device on the other end of the virtual circuit. When this DLCI becomes active, the unit will add a route in the IP routing table. Default is **0.0.0.0.** For the PPP protocol, the PPP peer's IP address or network can be set here, if known. Leaving this at **0.0.0.0** means that the unit will determine the PPP peer's IP and network (if unnumbered) using the PPP IPCP. Default is **0.0.0.0.**

MTU

(This option is not available if the ***L2 Protocol*** *is set to* ***PPP****.)* The Maximum Transmission Unit (MTU) is the largest possible data unit that can be transmitted. The range is **64** to **1500**. The default is **1500**.

NAT

The unit can perform Network Address Translation (NAT). This feature is most widely used when connecting to the Internet. The Ethernet network can consist of private network numbers. When this profile is enabled, all IP addresses on the Ethernet side are translated into the one real IP address. Multiple stations on the Ethernet side can access the Internet simultaneously.

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. Default is **Disabled.** When disabled, the unit will route across the connection normally.

Public IP Address Mode

(This option is only available when ***NAT Port Translation*** *is enabled.)* The port translation requires at least a single real IP address for translating. This value can use the IP assigned to the interface (or assigned via layer 2 protocol like PPP), obtained using DHCP client, or statically specified on this menu. If the address cannot be learned, it must be specified in order for the translation to work. Choices are **Interface, Specified,** and **DHCP Client.** Default is **Interface.**

Public IP Address

(This option is only available when ***NAT Port Translation*** *is enabled and the* ***Public IP Address Mode*** *is set to* ***Specified****.)* This is the specified address used as the NAT address. Default is **0.0.0.0.**

Translate Body of Unmapped Ports

If this option is set to **Disabled**, the user must add an entry in the translation table for every port which needs to be translated. If set to **Enabled**, every port will be translated. The default is **Disabled**, which is sufficient for most circuits.

Translation Table

(This option is only available when ***NAT Port Translation*** *is enabled.)* Add translation entries to specify port address translations or to setup 1:1 translations.

PUBLIC ADDRESS MODE

*(This option is only available when **NAT PORT TRANSLATION** is enabled.)* The public IP address used for this translation entry can be the NAPT IP address assigned to the link or can be specified. You specify an address to direct packets with certain protocols to different servers. Choices are **NAPT ADDR** and **SPECIFIED**. Default is **NAPT ADDR**.

PUBLIC ADDRESS

*(This option is only available when **NAT PORT TRANSLATION** is enabled and the **PUBLIC ADDRESS MODE** is set to **SPECIFIED**.)* Default is **0.0.0.0**.

PROTOCOL MODE

*(This option is only available when **NAT PORT TRANSLATION** is enabled.)* This is the upper layer protocol that is to be monitored for translation. For **TCP** and **UDP**, a port number must also be specified. Choices are **TCP; UDP; ICMP; ANY (TCP, UDP,** or **ICMP); ALL; SPECIFIED;** and **NONE.** Default is **NONE.**

PROTOCOL

*(This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to **SPECIFIED.)*** Default is **0** (decimal).

PROTOCOL TYPE

*(This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to **SPECIFIED**.)* For well known protocols, this status will populate with the protocol. This is a read-only field.

PUBLIC TYPE MODE

*(This option is only available when **NAT PORT TRANSLATION** is enabled and **PROTOCOL MODE** is set to either **TCP** or **UDP**.)* The public destination port associated with this entry can be specified to add more control over certain types of traffic. Choices are **SPECIFIED** and **ANY PORT**. The default, **ANY PORT**, covers all port types.

PUBLIC PORT

*(This option is only available when **NAT PORT TRANSLATION** is enabled and **PUBLIC PORT MODE** is set to **SPECIFIED.)*** However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP,** or **ICMP); ALL; SPECIFIED;** or **NONE**. Default is **0** (decimal).

PUBLIC PORT TYPE

*(This option is only available when **NAT PORT TRANSLATION** is enabled and **PUBLIC PORT MODE** is set to **SPECIFIED**.)* However, it will not be available if **PROTOCOL MODE** is set to **ICMP; ANY (TCP, UDP,** or **ICMP); ALL; SPECIFIED;** or **NONE**. Read-only.

PRIVATE ADDRESS MODE

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* The private IP address can be specified to steer 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 matching this entry's public parameters will be dropped if this mode is set to **ANY INTERNAL.** Choices are **SPECIFIED** and **ANY INTERNAL.** Default is **ANY INTERNAL.**

PRIVATE ADDRESS

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled and* ***PRIVATE ADDRESS MODE*** *is set to* ***SPECIFIED****.)* Default is **0.0.0.0.**

PRIVATE PORT MODE

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled. However, it will not be available if* ***PROTOCOL MODE*** *is set to* ***ICMP; ANY (TCP, UDP,*** *or* ***ICMP); ALL; SPECIFIED;*** *or* ***NONE****.)* The private destination port associated with this entry can be specified to add more control over certain types of traffic. Leave as **ANY PORT** to cover all port types. Choices are **ANY PORT** and **SPECIFIED**. Default is **ANY PORT.**

PRIVATE PORT

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled and* ***PRIVATE PORT MODE*** *is set to* ***SPECIFIED****. However, it will not be available if* ***PROTOCOL MODE*** *is set to* ***ICMP; ANY (TCP, UDP,*** *or* ***ICMP); ALL; SPECIFIED;*** *or* ***NONE****.)* Default is **0** (decimal).)

TRANSLATE BODY

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* When 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** (default) for applications where this will cause problems.

NAT VIEW

Shows the protocols that are actively being translated.

ENTRY

Indicates the entry number in the **NAT VIEW** table.

PRIV ADDR

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This shows the private address of the host that the entry is used for.

PUB ADDR

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This shows the public address this entry is using for its NAPT.

SERV ADDR

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This is the destination of the packet.

PROTO

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This shows the protocol used (**TCP, UDP, ICMP**, etc.).

PRIV PORT

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This is the private port used for the entry.

SPOOF PORT

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* If the same private port is already used in the table, it will spoof a different port for the entry.

SERVER PORT

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This port is used on the public side.

TIME

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This is the time since the entry was last used.

IN CNT

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This is the number of packets that came in.

OUT CNT

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This is the number of packets sent out.

NAPT ADDRESS

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This represents the public address that is being used as the NAPT address. Read-only.

ENTRY COUNT

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This is the number of entries in the NAT table. Maximum is 1500.

ENTRY OVERFLOW COUNT

(This option is only available when ***NAT PORT TRANSLATION*** *is enabled.)* This is a count of the dropped entries due to entry count being 1500 or greater; i.e., the NAT table is full.

RIP

Routing Information Protocol (RIP) is based on the shortest path (hops) between two IP addresses on a network. Each router maintains and broadcasts a routing table of known addresses/routes.

VERSION

The RIP protocol can be specified per DLCI. The possible selections are **OFF** (default) (meaning no RIP packets are listened to or sent), **V1** (RIP version 1), or **V2** (which is RIP version 2).

METHOD

This specifies the way the RIP protocol sends out its advertisements. The default is **SPLIT HORIZON**.

SPLIT HORIZON	Only routes not learned from this particular virtual circuit are advertised.
POISON REVERSE	All routes are advertised, but the routes learned from this port are “poisoned” with an infinite metric.

DIRECTION

This parameter specifies the direction at which RIP advertisements are sent and listened.

TX AND RX (DEF)	RIP advertisements are periodically transmitted and are listened to on this virtual circuit.
TX ONLY	RIP advertisements are periodically transmitted but are not listened to on this virtual circuit.
RX ONLY	RIP is not transmitted on this virtual circuit, but they are listened to.

V2 SECRET

Enter the secret used by RIP version 2 here.

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. Default is **0.0.0.0.** This is a default gateway for the entire unit, not just for the Ethernet port.

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 MODE

When set to **ON**, the unit acts as a DHCP server and will dynamically assign IP, network mask, default gateway, and DNS addresses to any device which transmits a broadcast DHCP request. The addresses assigned are based on the unit’s own IP address and will be within the same network. Default is **OFF.**

ROUTER > CONFIG > DHCP SERVER > DHCP RENEWAL TIME (HOURS)

The number of hours that the DHCP server should allow the device to keep its previous IP assignment, before it is required to send a new DHCP request. The default is **15 HOURS**.

ROUTER > CONFIG > DHCP SERVER > DOMAIN NAME

Text string used to represent the domain name used by the unit.

ROUTER > CONFIG > DHCP SERVER > PRIMARY DNS

IP address of first server to which domain name requests are sent. Default is **0.0.0.0**.

ROUTER > CONFIG > DHCP SERVER > SECONDARY DNS

IP address of server used as a backup, in case the primary address does not respond to the request. Default is **0.0.0.0**.

ROUTER > CONFIG > DHCP SERVER > PRIMARY NBNS/WINS

Primary address of the NBNS/WINS server. Default is **0.0.0.0**.

ROUTER > CONFIG > DHCP SERVER > SECONDARY NBNS/WINS

Secondary address of the NBNS/WINS server. Default is **0.0.0.0**.

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**, and **ARP CACHE** 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 ICMP messages this 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 UBOUND 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 > IP STATS > ARP CACHE

This lists the contents of the units'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.

IP ADDRESS

IP address used for resolving MAC address.

MAC ADDRESS

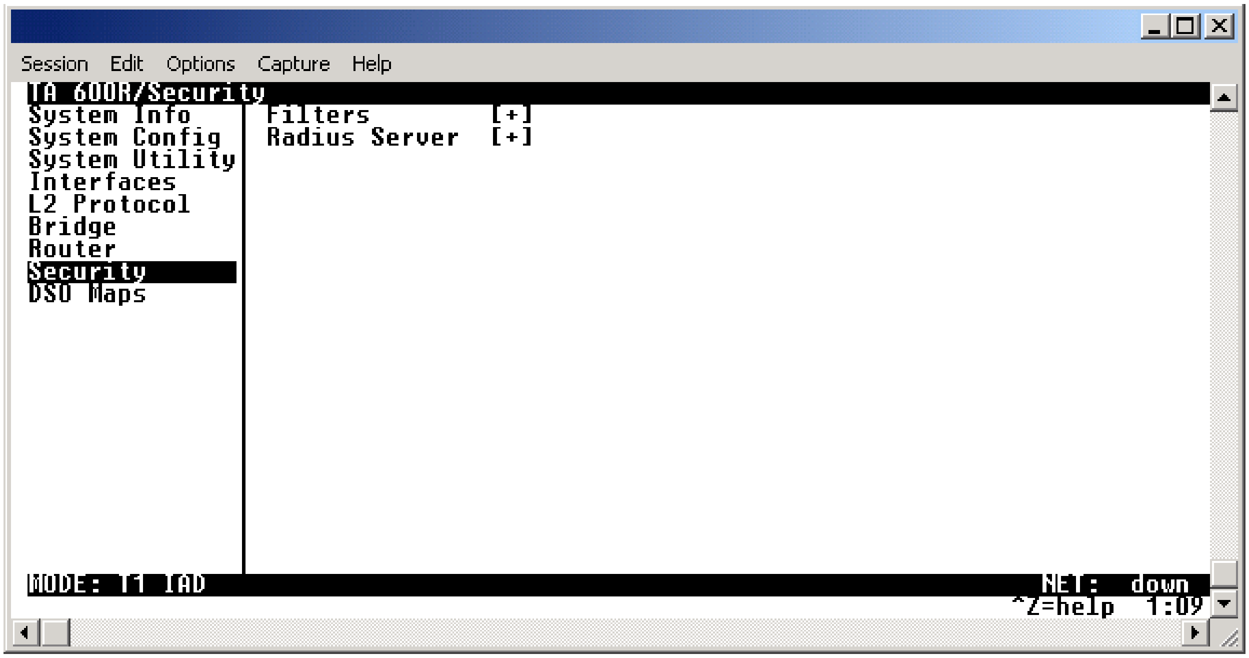
Ethernet address resolved (0=no resolution).

TIME

Minutes since entry was first entered.

SECURITY

Configure the **SECURITY FILTERS** and **RADIUS SERVER** parameters from this menu as shown in Figure 10.



```
TA 600R/Security
System Info     Filters        [+]
System Config   Radius Server  [+]
System Utility
Interfaces
L2 Protocol
Bridge
Router
Security
DS0 Maps

MODE: T1 IAD                                        NET:  down
                                                 ^Z=help  1:09
```

Figure 10. Security Menu

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 a list under the PVC or PPP configuration. This menu is used to define the individual filter defines based on packet type.

NOTE *The Filter Defines option works for Frame Relay and PPP.*

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.

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.

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.

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 TO 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 TO 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

PROTO PORT

Protocol used for comparison. Value is in decimal format. Range: **0 TO 255**. Default is **0**.

PROTO 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

TCP ESTAB

Yes - only when TCP established
No - only when TCP not established
Ignore - ignore TCP flags (default)

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 (T1[0])

Define the filters for the T1 interfaces from this menu.

> NOTE *The T1 interface will only appear in the* **SECURITY > FILTERS > INTERFACE** *list if the* **L2 PROTOCOL** *is set to* **FRAME RELAY** *or* **PPP**.

SECURITY > FILTERS > INTERFACES (T1[0]) > SUB-INTERFACE

If the **L2 PROTOCOL** is **FRAME RELAY**, the **SUB-INTERFACE** will be **FRE [0.X]**, where the [0.X] represents the T1 physical and logical ports, respectively. The T1 physical port is always 0. The X represents the Frame Relay logical port and will always be a number 0-9 corresponding to the interface number under **L2 PROTOCOL > CONFIG > DLCI MAPPING**. This is a read-only field.

If the **L2 PROTOCOL** is **PPP**, the **SUB-INTERFACE** is **PPP [0.0]**. The [0.0] represents the T1 physical and logical ports, respectively. This is a read-only field.

SECURITY > FILTERS > INTERFACES (T1[0]) > SET-UP

Enable the T1 interface filtering and define filters from this menu.

IN FROM VC

The packets which come into the unit 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 WAN are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > IN EXCEPTIONS** list.

FORWARD ALL No incoming packets from the WAN are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > IN EXCEPTIONS** list.

IN EXCEPTIONS

This is a list of up to 32 filter entries which can be combined using the operations field. The operations 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.

OUT TO VC

The packets which come from the unit to the WAN can be filtered in three ways:

DISABLE (DEF)	Turns off packet output filtering. No outgoing packets are blocked.
BLOCK ALL	All outgoing packets to the WAN are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > OUT EXCEPTIONS** list.
FORWARD ALL	No outgoing packets to the WAN are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > OUT EXCEPTIONS** list.

OUT EXCEPTIONS

This is a list of up to 32 filter entries which can be combined using the operations field. The operations 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.

SECURITY > FILTERS > INTERFACES (ETH[1])

Define the filters for the Ethernet interface from this menu.

SECURITY > FILTERS > INTERFACES (ETH[1]) > SUB-INTERFACE

The Ethernet sub-interface is 802.3[1.0]. This is a read-only field.

SECURITY > FILTERS > INTERFACES (ETH[1]) > SET-UP

Enable the Ethernet interface filtering and define filters from this menu.

IN FROM VC

The packets which come into the unit 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 WAN are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > IN EXCEPTIONS** list.
FORWARD ALL	No incoming packets from the WAN are blocked except as defined in the **SECURITY > FILTERS > INTERFACES > SETUP > IN EXCEPTIONS** list.

IN EXCEPTIONS

This is a list of up to 32 filter entries which can be combined using the operations field. The operations 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.

Out to VC

The packets which come from the unit to the WAN can be filtered in three ways:

Disable (def) Turns off packet output filtering. No outgoing packets are blocked.

Block All All outgoing packets to the WAN are blocked except as defined in the **Security > Filters > Interfaces > Setup > Out Exceptions** list.

Forward All All outgoing packets to the WAN are not blocked except as defined in the **Security > Filters > Interfaces > Setup > Out Exceptions** list.

Out Exceptions

This is a list of up to 32 filter entries which can be combined using the operations field. The operations 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.

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** 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** 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** the unit should attempt to communicate with when authenticating a Telnet session. 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 is the commonly used port.

SECURITY > RADIUS SERVER > SECRET

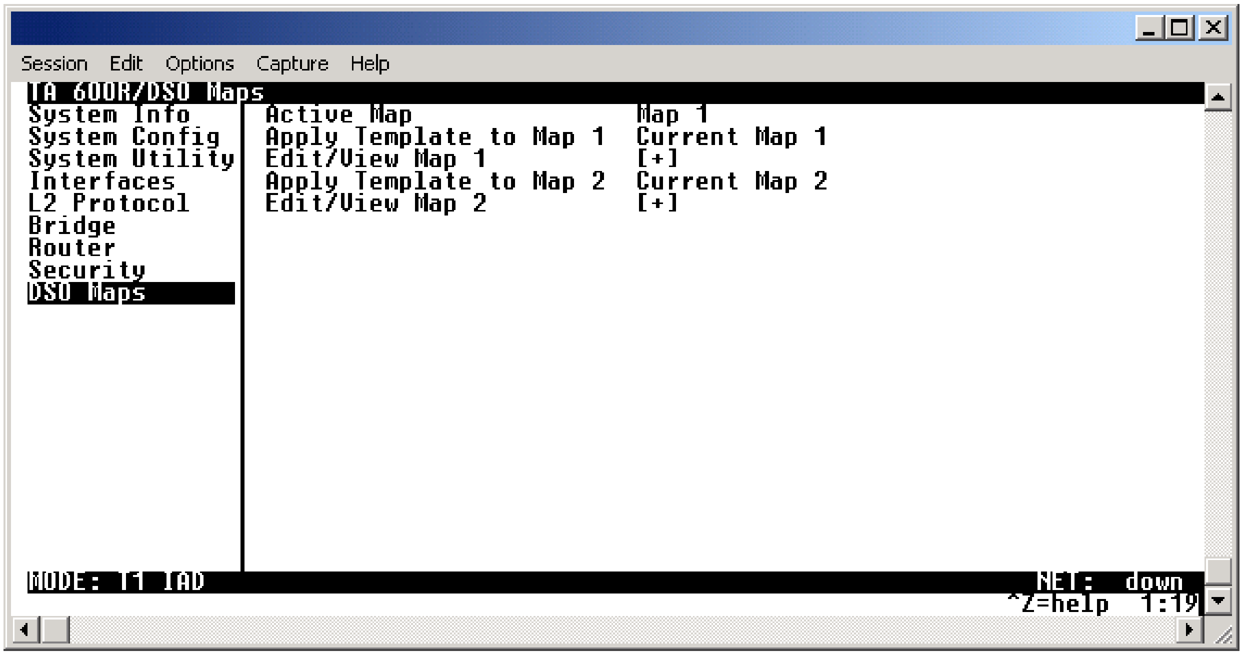
The **RADIUS SERVER** and unit share this text string. It is used by the **RADIUS SERVER** to authenticate the unit, the RADIUS client. The factory default is not to use a secret.

SECURITY > RADIUS SERVER > RETRY COUNT (1-10)

This is the number of times the unit should send a request packet to 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

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 11.



```
TA 600R/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                                              NET:  down
                                                       ^Z=help  1:19
```

Figure 11. DS0 Maps Menu.

DS0 MAPS > ACTIVE MAP

Activates one of the two dedicated maps (**MAP 1** or **MAP 2**). Default is **MAP 1**.

DS0 MAPS > APPLY TEMPLATE TO MAP 1

Choices are **CURRENT MAP 1, CURRENT MAP 2,** and **CLEAR MAP**. Default is **CURRENT MAP 1**. **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 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 all of the slots and the modules displays. The first option is **OPEN**, which unassigns the slot if selected. Use **TA 600R** to map network timeslots to the router. Pick the appropriate **SERVICE** and press **<Enter>**. Default is **OPEN**.

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.

Once a **SERVICE** is assigned, the TA 600R port choices are **N/A**, **UNASSIGNED, ROUTER 64K,** and **ROUTER 56K**. Default is **N/A**.

DS0 MAPS > EDIT/VIEW MAP 1 > RBS

Robbed Bit Signaling. The **RBS** parameter remains at **N/A** for the TA 600R, because **RBS** is not applicable to data connections.

DS0 MAPS > APPLY TEMPLATE TO MAP 2

Choices are **CURRENT MAP 1, CURRENT MAP 2,** and **CLEAR MAP**. Default is **CURRENT MAP 2**. **CLEAR MAP** clears the entire map.

DS0 MAPS > EDIT/VIEW MAP 2

Define map 2. The map allows the user to assign services and ports to individual DS0s 1-24.

DS0 MAPS > EDIT/VIEW MAP 2 > DS0

Displays the network T1 time slot to be assigned.

DS0 MAPS > EDIT/VIEW MAP 2 > SERVICE

When you select this option, a list of all of the slots and the modules displays. The first option is **OPEN**, which unassigns the slot if selected. Use **TA 600R** to map network timeslots to the router. Pick the appropriate **SERVICE** and press **<Enter>**. Default is **OPEN**.

DS0 MAPS > EDIT/VIEW MAP 2 > 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.

Once a **SERVICE** is assigned, the TA 600R port choices are **N/A**, **UNASSIGNED, ROUTER 64K,** and **ROUTER 56K**. Default is **N/A**.

DS0 MAPS > EDIT/VIEW MAP 2 > RBS

Robbed Bit Signaling. The **RBS** parameter remains at **N/A** for the TA 600R because **RBS** is not applicable to data communications.

Appendix A. Configuring the Unit for Routing

Initial Setup

Before the unit can be configured for routing, the DS0s must be mapped.

DS0 Mapping

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 T1 line entering the unit is broken up into 24 DS0s or channels. At least one DS0 needs to be mapped to the router in order to use the unit 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 600R**.
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.

Setting up Routing Options

The unit can support IP routing and bridging. These procedures are described on the pages that follow.

IP Routing

After completing the DS0 mapping, there are three remaining steps required for the unit to be used for IP Routing: (1) Ethernet Interface Configuration, (2) T1 Interface Configuration, and (3) Default Gateway Configuration. All of these procedures are described in the pages that follow.

Router Ethernet Interface Setup

Router Ethernet Interface Setup Instructions

Step	Action
1	From the Main menu, select **ROUTER**, select **CONFIG**, select **INTERFACES** and then select **ETH [1] SETUP** and press **ENTER**.
2	Press **Enter** on the **PRIMARY IP [+]** option to enter primary Ethernet configuration.
3	Set the **IP ADDRESS** of the Ethernet port.
4	Set the **SUBNET MASK** of the Ethernet port.
5	**RIP** on the Ethernet is disabled by default. If **RIP** needs to be enabled, press **Enter** on **RIP** [+].
6	Press **ENTER** on **VERSION** and select **V1** or **V2** to activate **RIP**.
7	Press the down arrow and select the appropriate **RIP METHOD**, **DIRECTION**, and **V2 SECRET** (where applicable).
8	Press the left arrow key to return to the Ethernet menu showing **PRIMARY IP** and **SECONDARY IPS**.
9	If the unit needs additional secondary IP addresses, press **Enter** on **SECONDARY IPS** [+].The unit supports up to 5 additional LAN segments. Enter each additional secondary IP address and subnet mask. Press "I" to insert additional entries.

Router T1 Interface Setup

Before configuring the Router T1 Interface, choose **L2 PROTOCOL** and select **PPP**, **FRE**, or **AUTO**. Setup instructions for the **PPP** and **FRE** are described on the following pages. For information on setting the **L2 PROTOCOL** to **AUTO**, reference DLP-014, *Unit Installation Using The Auto-Config Feature*.

Router T1 Interface Setup Instructions when L2 Protocol = PPP

Step	Action
1	From the Main menu, select **L2 PROTOCOL** and press **ENTER**.
2	Set the T1 [0] interface protocol to **PPP.**
3	Press **Enter** on the **CONFIG [+]** option. Verify mode is **ROUTE IP**.
4	Press **Enter** on the **AUTHENTICATION [+]** option if you wish 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 will appear.
5	Left arrow back to the Main menu.
6	Select router, select **CONFIG**, select **INTERFACES**, and select **T1 [0] SETUP**. Enter WAN information: • Far-End IP Address The far-end WAN IP address from the unit. • IP Netmask The subnet mask for this WAN link • Local IP Address The local WAN IP address for the unit. The other config items can be left at the defaults.
7	For **NAT** configuration, please see the **IP Routing with NAT** section of this appendix. On page 123.

Router T1 Interface Setup Instruction when L2 Protocol = Frame Relay (FRE)
(required if the unit is to be used for Frame Relay IP Routing on the WAN interface)

Step	Action
1	From the Main menu, select **L2 PROTOCOL** and press **ENTER**.
2	Set the **T1 [0]** interface protocol to **FRE**.
3	Press **Enter** on the **CONFIG [+]** option.
4	Set the **MAINTENANCE PROTOCOL** to **ANNEX D** (ANSI)**, ANNEX A** (q 933a)**, 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 [+]**. Right arrow one time to create an entry.
6	Set **ACTIVE** to **YES**.
7	Set **DLCI** to the DLCI number.
8	Set mode to **ROUTE IP**.
9	Left arrow back to the main menu. Select **ROUTER**, select **CONFIG**, select **INTERFACES**, and select **T1 [0] SETUP**. Set **ACTIVE** to **YES**.
10	Set **ADDRESS MODE** to **USER SPECIFIED** and enter a **FAR-END IP ADDRESS**. This will force the unit to not use IARP.
11	Enter the **IP NETMASK**.
12	Enter the **LOCAL IP ADDRESS** for the unit. The other config items can be left at the default values.
13	For **NAT** configuration, please see the **IP Routing with NAT** section of this appendix, on page 133.

Router T1 Interface Setup Instructions - IP Routing with NAT	
Step	**Action**
1	The **NAT** menu is found under **ROUTER >CONFIG >INTERFACES (T1 [0]) > SETUP**. The **NAT** menu can be easily accessed by pressing **<Ctrl><N>**.
NOTE	*The T1 interface will not appear if a DLCI is not entered in the DLCI mapping table (***L2 PROTOCOL T1[0]-FRE > CONFIG > DLCI MAPPING***) when the L2 Protocol is set to Frame Relay (FRE).*
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** is the default and will use the WAN IP address for the NAPT address. • **SPECIFIED** allows you to enter another 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.
5	Create specific **NAT** translations based on your application. **PUBLIC ADDRESS MODE** **NAPT ADDR** (Address) or **SPECIFIED**. Choice of using the NAPT address or specifying a different public address to be used for this translation. **PUBLIC ADDRESS MODE** **NAPT ADDR** (Address) or **SPECIFIED**. Choice of using the NAPT address or specifying a different public address to be used for this translation. **PROTOCOL** Protocol for this translation. **PUBLIC PORT MODE** **SPECIFIED** or **ANY PORT**. Choosing **SPECIFIED** brings up the **PUBLIC PORT** and **PUBLIC PORT TYPE** (read-only) settings. **PUBLIC PORT** Numeric Public Port number to be translated (e.g., 23, 80). **PUBLIC PORT TYPE** Read-only port type chosen by the user setting of the **PUBLIC PORT** option. **PRIVATE ADDRESS MODE** **SPECIFIED** or **ANY INTERNAL**. Choosing **SPECIFIED** brings up the **PRIVATE ADDRESS** option. **PRIVATE PORT MODE** **SPECIFIED** or **ANY PORT**. Choosing **SPECIFIED** brings up the **PRIVATE PORT** option. **PRIVATE PORT** Numeric Private Port number to be translated to (e.g. 23, 80). **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.

Default Gateway Setup

In A.04 TDM code, the default gateway is for the entire unit, not just for the Ethernet Port.

Default Gateway Setup Instructions	
1	From the Main menu, select **ROUTER**, select **CONFIG**, and select **ROUTES**.
2	Press Enter on the **DEFAULT GATEWAY** and set the corresponding IP address for the **DEFAULT GATEWAY**.

Appendix B. Configuring the Unit for Bridging

Initial Setup

Before the unit can be configured for bridging, DS0s must be mapped. Reference the DS0 Mapping section on page 119.

Setting up Bridging Options

If the unit will be used for bridging, continue with the steps below.

Bridging

Bridging is supported by the PPP and Frame Relay protocols. The following procedures describe the bridging configuration for those two protocols.

PPP Bridging Setup Instructions	
1	From the Main menu, select **L2 PROTOCOL (T1[0])>PROTOCOL** and select **PPP**.
2	Select **CONFIG** and press **<Enter>**. Then select **MODE** and select **BRIDGE ALL**.
3	Use the left arrow to return to the Main menu; select **BRIDGE**.
4	The user may confirm that Bridging is activated by selecting **CONFIG** and **INTERFACES**. If the T1[0] interface appears in the list, the Bridging is active on the WAN link.
5	The time (in minutes) it takes an entry to age out of the Bridge table may be set by down arrowing to **BRIDGE TABLE** and then using the right arrow to select **BRIDGE TABLE AGING**.

Frame Relay Bridging Setup Instructions	
1	From the Main menu, select **L2 PROTOCOL (T1[0])>PROTOCOL** and select **FRE**.
2	Select **CONFIG** and press **<Enter>**.
3	Set the **MAINTENANCE PROTOCOL TO ANNEX D (ANSI), ANNEX A** (q**933**a**), LMI**, or **STATIC (NO SIG)**.
NOTE	*The* ***MAINTENANCE PROTOCOL*** *should be set based on the Frame Relay switch.*
4	Select **DLCI MAPPING** and press **<Enter>**. Then select **MODE** and select **BRIDGE ALL** for all DLCIs which will use bridging.
5	Use the left arrow to return to the Main menu; select **BRIDGE**.
6	The user may confirm that Bridging is activated by selecting **CONFIG** and **INTERFACES**. If the T1[0] interface appears in the list, the Bridging is active on the WAN link.
7	The time (in minutes) it takes an entry to age out of the Bridge table may be set by down arrowing to **BRIDGE TABLE** and then using the right arrow to select **BRIDGE TABLE AGING**.

DETAIL LEVEL PROCEDURES

CONNECTING THE TERMINAL OR PC TO THE CRAFT PORT

Introduction

Provisioning is 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 **CRAFT** port on the rear of the unit allows access to the menus and management features of the unit. This section specifies how to connect the VT100 terminal or PC to the unit.

Access to the unit is through the port labeled **CRAFT**, an RJ-45 connector on the back of the unit. A special ADTRAN adapter is required for access to this port.

Prerequisite Procedures

The unit must be powered for terminal communication to function.

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-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is provided with the unit.

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

DLP-001

Perform Steps Below in the Order Listed

1. Connect a VT100 terminal to the unit.

   - Set the parameters of the VT100 terminal 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 serial port.
   - Plug the RJ-45 male end of the data cable into the **CRAFT** port on the rear of the unit by using the ADTRAN-proprietary DB-9 to RJ-45 adapter. Make the connection to the VT100 terminal as appropriate for your equipment.

2. Connect a PC emulating a VT100 terminal to the unit.
3. Most personal computers or laptops can run communications software that will emulate a VT100 terminal. Windows programs such as Terminal© or Hyperterminal© are two such examples in the Windows format. However, there are many other adequate, commercially available software packages which will allow your PC or laptop to emulate a VT100 terminal. Certain configuration items must be set on a PC or laptop for it to act as a VT100 terminal for the unit.

   - Set the PC for direct connect on the appropriate com port (instead of dial-up connection).
   - Set the parameters of the communications software to:
     - 9600 baud rate
     - 8 data bits
     - No parity
     - 1 stop bit
     - No flow control
   - Plug the RJ-45 male end of the data cable into the **CRAFT** port on the rear of the unit by using the ADTRAN-proprietary DB-9 to RJ-45 adapter. Make connection to the PC or laptop as appropriate for your equipment.

4. Press <Enter> or <Ctrl + R> until the Login menu appears on screen.

   You are now ready to log in to the unit, as described in DLP-002*, Logging in to the System.*

NOTE *A VT100 terminal program is provided with the ADTRAN Utilities.*

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

LOGGING IN TO THE SYSTEM

Introduction

Once connected to the unit via either a VT100 terminal or PC configured as a VT100 terminal, it is necessary to log in to the system to gain access to the management and provisioning functions. This DLP provides specific steps for logging in to the system and accessing the various management and provisioning functions.

Prerequisite Procedures

Complete DLP-001, *Connecting the Terminal or PC to the CRAFT Port*, before logging in to a unit.

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-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is provided with the unit.

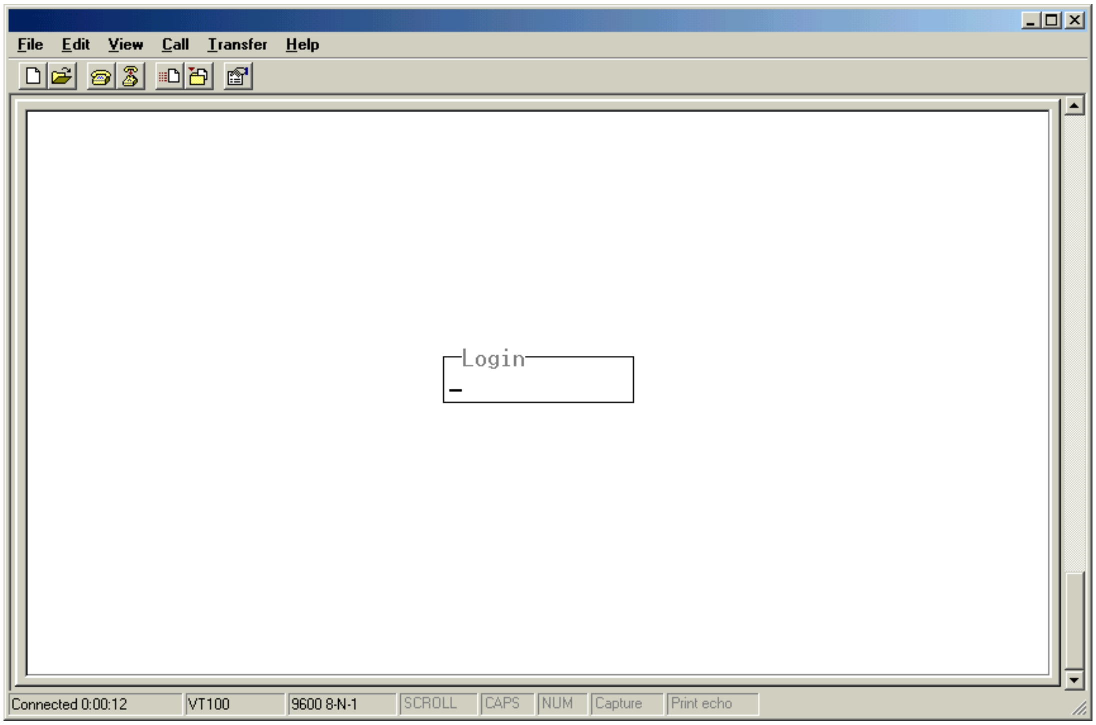
WARNING	*To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.*

DLP-002

Perform Steps Below in the Order Listed

1. After connecting to the system, a blank screen will appear.

   Pressing any key will display the login screen shown below.



   The cursor will blink at the **LOGIN** field, waiting for a password to be entered.

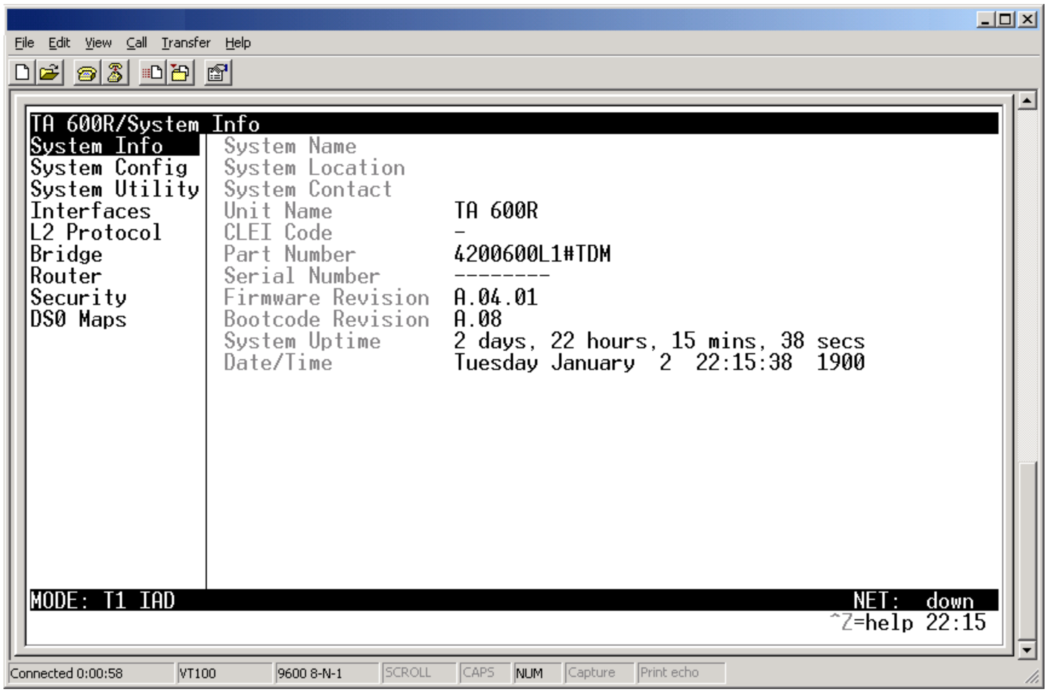
2. At the **LOGIN** field, enter the password for the unit.

   Passwords are case sensitive. There is not a manufacturer's password by default. Press <Enter> to enter the menu.

NOTE

If a customer forgets the password, they can contact ADTRAN Technical Support at 888-4ADTRAN for instructions on how to access the unit.

3. Upon entering the correct password, the **MAIN MENU** is displayed as shown below.



```
TA 600R/System Info
System Info      System Name
System Config    System Location
System Utility   System Contact
Interfaces       Unit Name          TA 600R
L2 Protocol      CLEI Code          -
Bridge           Part Number        4200600L1#TDM
Router           Serial Number      --------
Security         Firmware Revision  A.04.01
DS0 Maps         Bootcode Revision  A.08
                 System Uptime      2 days, 22 hours, 15 mins, 38 secs
                 Date/Time          Tuesday January  2  22:15:38  1900

MODE: T1 IAD                                               NET:  down
                                                        ^Z=help 22:15
```

You are now logged in to the menu system.

NOTE *CONTROL L or CONTROL S will return to the login prompt shown in Step 1.*

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

ADDING/REMOVING TELNET USERS AND CHANGING PASSWORD SECURITY LEVELS

Introduction

All menu items in the unit are protected by passwords of varying security levels. By assigning different passwords to different security levels, the 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 unit.

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-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is provided with the unit.
- Ethernet cable from the **10/100BASET** port on the unit to a hub (customer-provided)
- Use Ethernet crossover if going from the unit to a PC (customer-provided).

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

DLP-003

Perform 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 a VT100 compatible terminal or with a PC running VT100 emulation software), follow the procedure in DLP-001 *Connecting the 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-004 and DLP-006 to connect to the **10/100BASET** interface.

2. Log in to the unit.

   Log in to the unit (see DLP-002, *Logging in to the System* for details).

3. Go to the **SYSTEM CONFIG** menu and select the **MANAGEMENT** menu and press <Enter>.
4. Go to the **TELNET ACCESS** menu and press <Enter>.
5. Go to the **AUTHEN METHOD** menu and press <Enter>. Select the appropriate authentication method. The choices are **PASSWORD, RADIUS, PASSWORD/RADIUS**, and **RADIUS/PASSWORD**.
6. Go to the **USER LIST** menu and press <Enter>.
7. To add a new user profile and password, right arrow over to the right pane.
8. Give the new user profile a name by selecting the **NAME** field, pressing <Enter>, and typing the user defined name.
9. Personalize the password for the appropriate level by selecting the **PASSWORD** field, pressing <Enter>, then typing the desired password. You will have to type the new password again to confirm it.

   Passwords for the unit 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 (********).

10. Select the **IDLE TIME (MINS)** 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**. The default value is **10**.
11. Assign the password level by selecting the **LEVEL** field and choosing from the following level descriptions.

The unit contains six different password levels. The table below gives a brief description of each level.

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 access to view **SYSTEM INFO**. 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 view-only privileges of **SYSTEM INFO**. 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.
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.

In the A.03 firmware, only one Telnet session can be active at a time. The A.04 firmware will support five simultaneous Telnet sessions.

In the A.03 firmware, the default conditions for the username and password fields are to have no entries in these fields.

*In the A.04 firmware, the default username and password are **guest** and **password**, respectively.*

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

SETTING ETHERNET IP PARAMETERS

Introduction

If the unit is connected to an IP network for Telnet, TFTP, or SNMP management, several IP parameters 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 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 unit (customer-provided)
- DB-9 female to RJ-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is provided with the unit.
- Ethernet cable from the **10/100BASET** port on the unit to a hub (customer-provided)
- Use Ethernet crossover if going from the unit to a PC (customer-provided).

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

DLP-004

Perform Steps Below in the Order Listed

1. Connect the unit to your VT100 system (details found in DLP-001, *Connecting the Terminal or PC to the CRAFT Port*).
2. Log in to the system with maximum rights (details for logging in are in DLP-002 and DLP-003).
3. From the **ROUTER/CONFIG/INTERFACES (ETH[1])** menu, select the **SETUP** option and press <Enter>.
4. Select the **PRIMARY IP** option and press <Enter>. Select **IP ADDRESS** and press <Enter>.

   Enter the appropriate IP address.
5. From the **ROUTER/CONFIG/INTERFACES (ETH[1])/SETUP/PRIMARY IP** menu, select the **SUBNET MASK** option and press <Enter>.

   Enter the appropriate Subnet Mask.
6. From the **ROUTER/CONFIG/ROUTES** menu, select the **DEFAULT GATEWAY** option and press <Enter>.

   Enter the appropriate Default Gateway.
7. Escape out to the **ROUTER** menu and log off by pressing <Ctrl + L>.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

VERIFYING COMMUNICATIONS OVER AN IP LAN

Introduction

When an **ETHERNET** port is connected to a local area network (LAN), test steps must be performed on the unit to ensure that it 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-004, *Setting Ethernet IP Parameters* should be complete.

Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect the terminal to the unit (customer-provided)
- DB-9 female to RJ-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is provided with the unit.
- Ethernet cable from the **10/100BASET** port on the unit to a hub (customer-provided)
- Use Ethernet crossover if going from the unit to a PC (customer-provided).

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

DLP-005

Perform Steps Below in the Order Listed

1. Ascertain the unit IP address.

   If you do not already have the IP Address for the unit, obtain it from the Network Administrator or manually check for the address in the **ROUTER/CONFIG/INTERFACES (ETH[1])/SETUP/PRIMARY IP/IP ADDRESS** menu.

NOTE *You must log in with a security level of* **CONFIG, SUPPORT***, or* **FULL** *to modify the IP parameters on the unit.*

2. Ping the 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 unit. Verify that the unit responds properly.

   If the unit fails to respond, try the following:

   - Verify that the proper IP Address, Subnet Mask, and Default Gateway are provisioned in the unit (see DLP-004, *Setting Ethernet IP Parameters* for details).
   - Verify that the unit is properly cabled into the LAN and that the Ethernet cable is properly seated in the RJ-45 **10/100BASET** port on the rear of the unit.
   - Verify the LAN link light on the front of the unit is lit. If not lit, check the cabling between the hub and the unit.
   - If the unit 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 unit is connected is lit. If this light is not lit, check the cabling between the hub and the unit.
   - 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 to a PC.

   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, type* **<Ctrl+C>** *to get the program to stop.*

3. Telnet to the unit.

   From the same computer used in the previous step, Telnet to the unit and verify that the Telnet session is properly opened (see DLP-006*, Telnetting to the Unit*). Once the Telnet session is established, press **<Ctrl+L>** to log out 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.*

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

TELNETTING TO THE UNIT

Introduction

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. This procedure details the steps which must be performed to Telnet into the unit.

Prerequisite Procedures

Complete DLP-004 and DLP-005 (Steps 1 and 2 only).

Tools and Materials Required

- Access to a PC or other computer connected to the LAN.
- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the unit (customer-provided)
- DB-9 female to RJ-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is provided with the unit.
- Ethernet cable from **10/100BASET** port on the unit to a hub (customer-provided)
- Use Ethernet crossover if going from the unit to a PC (customer-provided).

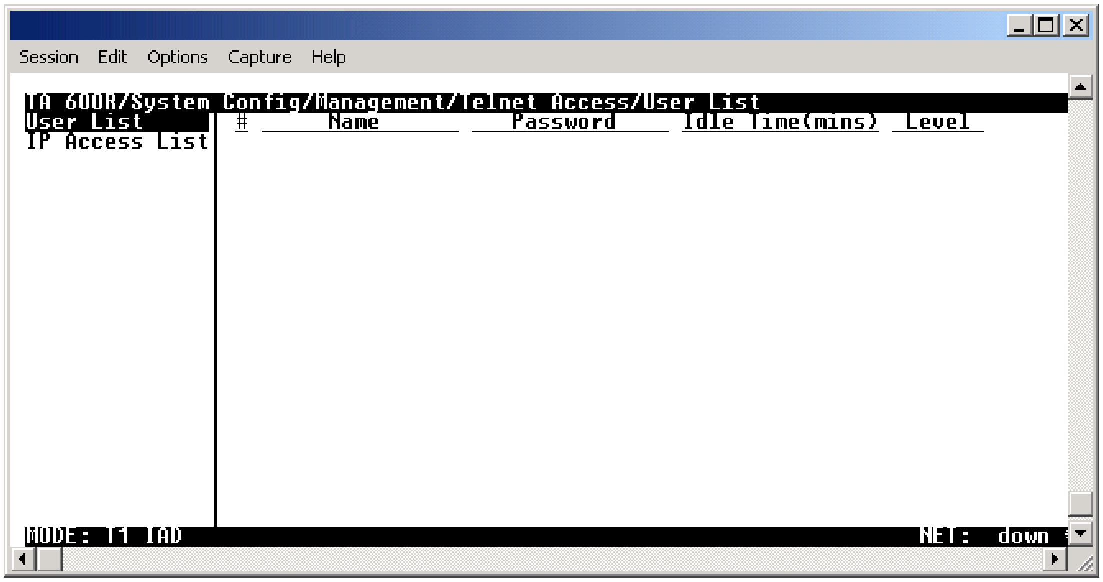
NOTE *The A.03.XX firmware supports one Telnet session at a time. The A.04 firmware supports five simultaneous Telnet sessions.*

DLP-006

Perform Steps Below in the Order Listed

1. Connect the computer to the unit's **CRAFT** port as shown in DLP-001, *Connecting the Terminal or PC to the CRAFT Port*.
2. Log in to the unit as shown in DLP-002, *Logging in to the System*.
3. Select **SYSTEM CONFIG**, **MANAGEMENT**, and **TELNET ACCESS**.
4. Right arrow to **AUTHEN METHOD** and press <Enter>. Select **PASSWORD, RADIUS, PASSWORD/RADIUS,** or **RADIUS/PASSWORD** and press <Enter>.
5. Verify the **TELNET ACCESS** is set to **ON**. Down arrow to select **USER LIST** and press <Enter>.

   The following screen will appear.



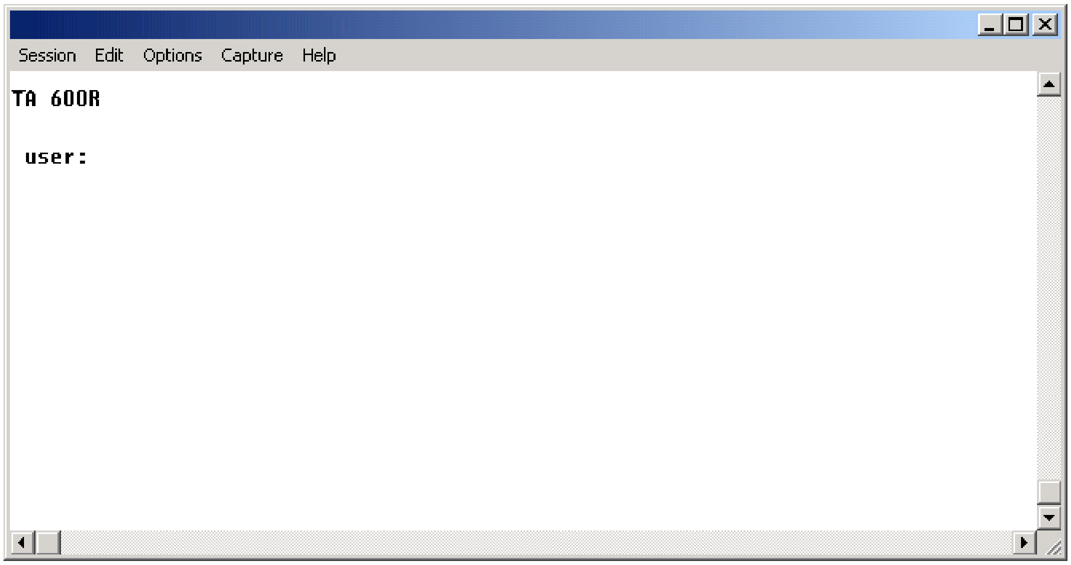
```
TA 600R/System Config/Management/Telnet Access/User List
User List      #      Name          Password      Idle Time(mins)  Level
IP Access List

MODE: T1 IAD                                                    NET:  down
```

6. Use the right arrow key to select the **NAME** field; press <Enter>. Enter a username to be used for Telnet logins.
7. If **PASSWORD** was selected for the **AUTHEN METHOD** in Step 4, right arrow over to **PASSWORD**; press <Enter>. Enter a password to be used for Telnet logins.
8. 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**. The default value is **10** minutes. Enter the appropriate **IDLE TIME**.
9. Use the right arrow key to select **LEVEL**. Select the appropriate security level. For security level definitions, reference DLP-003 *Adding/Removing Telnet Users and Changing Password Security Levels*.
10. This completes the addition of one Telnet user. Repeat Steps 1-9 for each user needing Telnet access.

11. Press <Ctrl + L> to log out of the unit.
12. From a remote computer system connected to the LAN, Telnet to the unit.

> 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.*

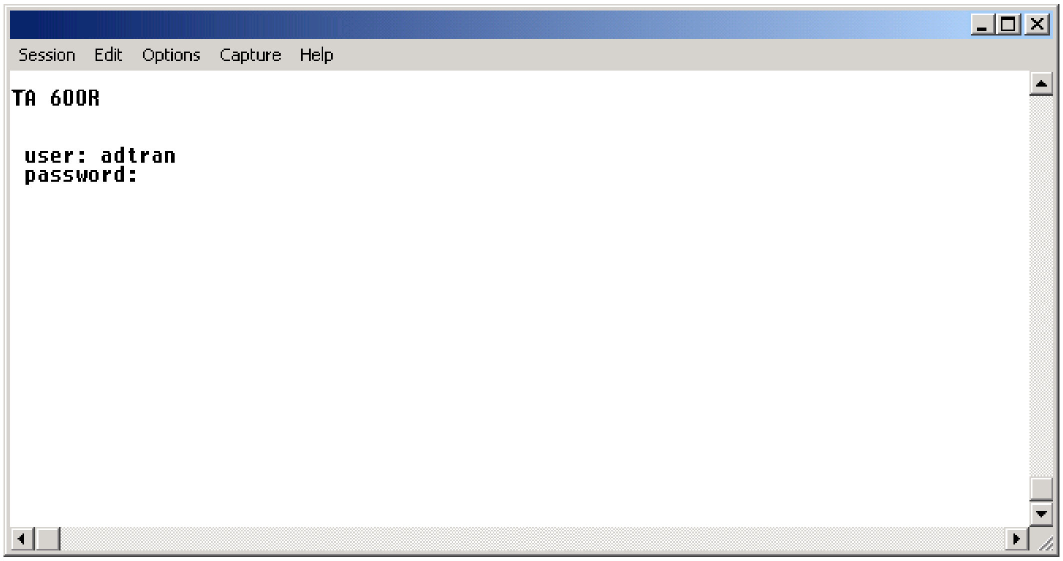
The following screen will appear.



```
TA 600R

 user:
```

13. Enter the user name assigned in Step 7 and press <Enter>.

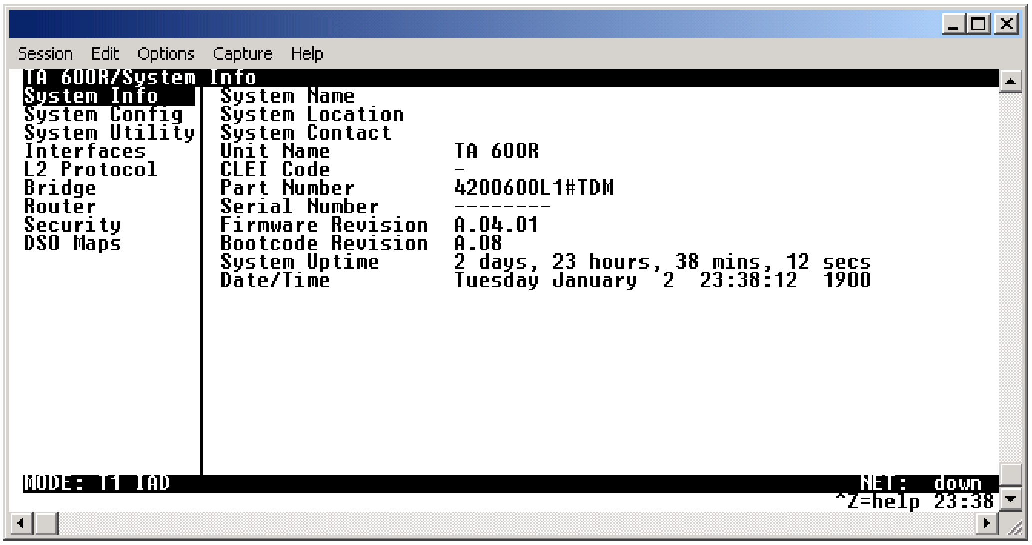
The following screen will appear.



```
TA 600R

 user: adtran
 password:
```

14. Enter the password assigned in Step 7.

    Upon entering the correct password, the unit's Main Menu is displayed as shown below:



```
TA 600R/System Info
System Info     System Name
System Config   System Location
System Utility  System Contact
Interfaces      Unit Name          TA 600R
L2 Protocol     CLEI Code          -
Bridge          Part Number        4200600L1#TDM
Router          Serial Number      --------
Security        Firmware Revision  A.04.01
DS0 Maps        Bootcode Revision  A.08
                System Uptime      2 days, 23 hours, 38 mins, 12 secs
                Date/Time          Tuesday January  2  23:38:12  1900







MODE: T1 IAD                                                  NET:  down
                                                          ^Z=help 23:38
```

    You are now Telnetted into the unit's menu system.

15. When you complete your configuration changes and save the changes (when prompted), press <Ctrl+L> to log out and close the session.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

UPGRADING THE FIRMWARE USING XMODEM

Introduction

The unit supports firmware updates via the **10/100BASET** port using either TFTP from a network server or the **CRAFT** interface using XMODEM. XMODEM is found in the VT100 terminal application in the ADTRAN Utilities package and in most PC VT100 communications software packages. This procedure outlines the steps for a successful firmware upgrade using the **CRAFT** interface and XMODEM software. Firmware may be obtained from the ADTRAN website at www.adtran.com. Select **Support** and then **Post-Sales Technical Support**.

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-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is provided with the unit.
- ADTRAN-provided file containing upgraded code
- XMODEM software

WARNING

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

DLP-007

Perform the Steps Below in the Order Listed

1. Connect to the unit using the **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-001, *Connecting the 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.

   Log in to the unit (see DLP-002, *Logging in to the System* for details).

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**.
5. Select **START TRANSFER** to start the update. 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 unit 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 has successfully completed, the following messages will display:

   Verifying downloaded FLASH image...

   Erasing FLASH...

   Programming FLASH...

   FLASH programmed successfully.

   The unit 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 **10/100BASET** port, the unit may be quickly upgraded using TFTP provided there is a TFTP server on the local network. The unit can also be upgraded across the WAN using TFTP provided there is a TFTP server accessible to the unit. The unit ships with ADTRAN Utilities software, which includes a TFTP server. See DLP-008, *Upgrading the Firmware Using TFTP*, for more details.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

UPGRADING THE FIRMWARE USING TFTP

Introduction

The unit supports firmware updates via the **10/100BASET** Ethernet port using either TFTP from a network server or the **CRAFT** interfaces using XMODEM. The unit also supports TFTP updates across the WAN using the data/router channels. This DLP provides the steps to follow for a successful firmware upgrade using the **10/100BASET** Ethernet port and a TFTP Server.

Tools and Materials Required

- A TFTP Server accessible on the local network (a TFTP server is provided with the unit as part of the ADTRAN Utilities software) or a TFTP server accessible across the WAN
- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the unit (customer-provided)
- DB-9 female to RJ-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is shipped with the unit.
- Ethernet cable from **10/100BASET** port on the unit to a hub (customer-provided)
- Use Ethernet crossover if going from the unit to a PC (customer-provided).

WARNING

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

DLP-008

Perform Steps Below in the Order Listed

For LAN Upgrades

1. Connect to the unit 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-006, *Telnetting to the Unit*, to connect to the unit.

2. Verify the TFTP server is running on the network. The user may ping the TFTP server from the unit to verify communication.

> *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.*

3. Download the firmware upgrade file to your computer.

> *If using ADTRAN utilities, save the upgrade file to the "**ADTNUTIL**" directory on your hard drive.*

4. Go to the **SYSTEM UTILITY** menu and select the **UPDATE FIRMWARE** menu; press <Enter>.
5. Go to the **TRANSFER METHOD** menu and select **TFTP**.
6. Set the **TFTP SERVER ADDRESS** to the IP address of the machine running the TFTP server program.

> *If using ADTRAN utilities, this will be the IP address that appears in the* ***TFTP SERVER STATUS*** *window.*

7. Enter the filename of the update file into the **TFTP SERVER FILENAME** field.
8. 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, various status messages display in **TRANSFER 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 unit 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.
Host Timeout	Unit will display this message if TFTP server address is incorrect.
idle	The upgrade has not yet been initiated.

9. When the update has successfully completed, **FLASH PROGRAMMED SUCCESSFULLY** will display 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 will display **RESETTING...**

   The unit 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.

For WAN Upgrades

1. Telnet into the unit using **FULL** or **SUPPORT** levels (refer to DLP-003, *Adding/Removing Telnet Users and Changing Password Security Levels*).
2. Verify the TFTP server is running on the network. Verify that the unit can ping the TFTP server.
3. Go to the **SYSTEM UTILITY** menu and select the **UPDATE FIRMWARE** menu; press **<Enter>**.
4. Go to the **TRANSFER METHOD** menu and select **TFTP**.
5. 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.*

6. Enter the filename of the update file into the **TFTP SERVER FILENAME** field.
7. 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, various status messages display in **TRANSFER 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 unit 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.
Host Timeout	Unit will display this message if TFTP server address is incorrect.
idle	The upgrade has not yet been initiated.

8. When the update has successfully completed, **FLASH PROGRAMMED SUCCESSFULLY** will display 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 will display **RESETTING...**

   The unit 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.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

SAVING THE CURRENT CONFIGURATION USING TFTP

Introduction

The unit supports configuration transfers from the unit (via the **10/100BASET** Ethernet port) to a TFTP server located on the network or a TFTP server accessible across the WAN. 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) or a TFTP server accessible across the WAN.
- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the unit (customer-provided)
- DB-9 female to RJ-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is shipped with the unit.
- Ethernet cable from the **10/100BASET** port on the unit to a hub (customer-provided)
- Use Ethernet crossover if going from the unit to a PC (customer-provided).

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

DLP-009

Perform Steps Below in the Order Listed

Saving Configuration using TFTP Server on Local Network

1. Connect to the unit 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-006, *Telnetting to the Unit*, to connect to the unit.

2. Verify the TFTP server is running on the network.

> *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.*

3. Go to the **SYSTEM UTILITY** menu and select the **CONFIGURATION TRANSFER** menu; press <Enter>.
4. Verify the **TRANSFER METHOD** is set to **TFTP**.
5. Set the **TFTP SERVER IP ADDRESS** to the IP address of the machine running the TFTP Server Program.

> *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.*

6. Change **TFTP SERVER FILENAME** to a unique filename. This will be the name of the configuration file saved to the remote server. An example filename would be **ta_iad.cfg**.

   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).

7. Select the **SAVE CONFIG REMOTELY** menu field and press <Enter>.

   Enter **Y** to confirm the request.

8. 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....**
9. When the transfer has successfully completed, **Idle** displays in the **Current Transfer Status** field.

> CAUTION *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.*

Saving Configuration using TFTP Server Accessible Across the WAN

1. Telnet into the unit using **Full** or **Support** levels (refer to DLP-003, *Adding/Removing Telnet Users and Changing Password Security Levels*).
2. Verify the TFTP server is running on the network. Verify that the unit can ping the TFTP server.
3. Go to the **System Utility** menu and select the **Configuration Transfer** menu; press <Enter>.
4. Verify the **Transfer Method** is set to **TFTP**.
5. Set the **TFTP Server IP Address** to the IP address of the machine running the TFTP Server Program.

> NOTE *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.*

6. Change **TFTP Server Filename** to a unique filename. This will be the name of the configuration file saved to the remote server. An example filename would be **ta_iad.cfg**.

   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).
7. Select the **Save Config Remotely** menu field and press <Enter>.

   Enter **Y** to confirm the request.
8. 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....**
9. When the transfer has successfully completed, **Idle** displays in the **Current Transfer Status** field.

> CAUTION *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.*

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

LOADING THE CURRENT CONFIGURATION USING TFTP

Introduction

The unit supports configuration uploads from a unit (via the **10/100BASET** Ethernet port) to a TFTP server located on the network or a TFTP server accessible across the WAN. This DLP provides the steps 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) or a TFTP server accessible across the WAN
- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the unit (customer-provided)
- DB-9 female to RJ-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is shipped with the unit.
- Ethernet cable from **10/100BASET** port on the unit to a hub (customer-provided)
- Use Ethernet crossover if going from the unit to a PC (customer-provided).

WARNING

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

DLP-010

Perform Steps Below in the Order Listed

Loading Configuration using TFTP Server on Local Network

1. Connect to the unit 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-006, *Telnetting to the Unit*, to connect to the unit.

2. Log in to the unit using a **FULL** or **SUPPORT** level password (see DLP-003, *Adding/Removing Telnet Users and Changing Password Security Levels* 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.

NOTE *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 including path. This will be the name of the configuration file retrieved from the remote server. An example filename would be **ta_iad.cfg**.

   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>.

   Enter **Y** to confirm the request.

9. View **CURRENT TRANSFER STATUS** to verify the progress of the current upload.

10. When the upload has successfully completed, **IDLE** displays in the **CURRENT TRANSFER STATUS** field.

CAUTION *The unit is rebooted immediately after a configuration is successfully loaded. Any online sessions will be terminated.*

11. After an appropriate length of time, the user may Telnet back into the unit.

> CAUTION
>
> *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.*

Loading Configuration using TFTP Server Accessible Across the WAN

1. Telnet into the unit using **FULL** or **SUPPORT** levels (refer to DLP-003, *Adding/Removing Telnet Users and Changing Password Security Levels*).
2. Verify the TFTP server is running on the network. Verify that the unit can ping the TFTP server.
3. Go to the **SYSTEM UTILITY** menu and select the **CONFIGURATION TRANSFER** menu; then press **<Enter>**.
4. Verify the **TRANSFER METHOD** is set to **TFTP**.
5. 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.*

6. Change **TFTP SERVER FILENAME** to a unique filename including path. This will be the name of the configuration file retrieved from the remote server. An example filename would be **ta_iad.cfg**.

   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).

7. Select the **LOAD AND USE CONFIG** menu field and press <Enter>.

   Enter **Y** to confirm the request.

8. View **CURRENT TRANSFER STATUS** to verify the progress of the current upload.
9. When the upload has successfully completed, **IDLE** displays in the **CURRENT TRANSFER STATUS** field.

> CAUTION
>
> *The unit is rebooted immediately after a configuration is successfully loaded. Any online sessions will be terminated.*

10. After an appropriate length of time, the user may Telnet back into the unit.

> CAUTION
>
> *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.*

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

SAVING THE CURRENT CONFIGURATION USING XMODEM

Introduction

The unit supports configuration transfers from the unit using a VT100 terminal or terminal emulator (with XMODEM) and the **CRAFT** interface. This DLP provides the steps to follow 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

WARNING

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

DLP-011

Perform Steps Below in the Order Listed

1. Connect to the unit using the RJ-45 **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-001, *Connecting the Terminal or PC to the CRAFT Port*. Connecting to the **CRAFT** port interface limits the config transfer procedure to XMODEM only.
2. Log in to the unit. (See DLP-002, *Logging in to the System*, for details.)
3. Go to the **SYSTEM UTILITY** menu and select **CONFIG 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 unit for the transfer download. The following message is displayed: **"This will begin sending a copy of the current system configuration."**

   When the unit is ready to send the configuration file, "**XMODEM/CRC: Receive CONFIG file now...**" is displayed in the bottom left corner of the terminal window. While this message is visible the menus are not available.
6. Configure the VT100 terminal or terminal emulation software to **RECEIVE** (you are prompted for filename).
7. From the terminal evaluation 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. Also, when specifying the filename, ensure that the filed save a .cfg extension. Otherwise, the file may not be available for uploading into the other units.

   Because XMODEM data is being transferred in-band through the menu interface, the VT100 menus of the unit 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).
8. When the transfer has successfully completed, **IDLE** displays in the **CURRENT TRANSFER STATUS** field and **UPLOAD COMPLETE** displays in the **PREVIOUS TRANSFER STATUS** field.

Follow-up Procedure

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

LOADING THE CURRENT CONFIGURATION USING XMODEM

Introduction

The unit supports configuration uploads from a unit using a VT100 terminal or terminal emulator (with XMODEM) and the **CRAFT** interface. This DLP provides the steps for a successful configuration upload using the **CRAFT** port and XMODEM.

Prerequisite Procedures

Obtain the configuration file (see for DLP-011, *Loading the Current Configuration Using XMODEM*, for details).

Tools and Materials Required

- VT100 terminal or PC with VT100 terminal emulation software
- XMODEM software

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

DLP-012

Perform Steps Below in the Order Listed

1. Connect to the unit using the RJ-45 **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-001, *Connecting the Terminal or PC to the CRAFT Port*. Connecting to the **CRAFT** interface limits the config transfer procedure to XMODEM Only.
2. Log in to the unit. (See DLP-002, *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 unit for the transfer download.

CAUTION *The following message is displayed: "Warning: WAN link may be reset after transfer complete!"*

   When the unit is ready to receive the XMODEM configuration file, the menu screen will clear and display **XMODEM/CRC: Transmit CONFIG file now...** If this does not appear, please review the 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**. Configuration files should have a .cfg extension.

   If necessary, refer to the terminal emulation software documentation for help.

   Because XMODEM data is being transferred in-band through the menu interface, the VT100 menus of the unit 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. After the config transfer is complete, the **CONFIG TRANSFER** menu will be displayed.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

SAVING AND LOADING TEXT CONFIGURATION USING THE TERMINAL COMMAND LINE

Introduction

The unit has the ability to download a text file which contains the configuration of the entire unit. This configuration may be altered in a text editor and then uploaded to the unit.

This DLP will explain how to save and load the configuration.

Prerequisite Procedures

You must connect to the unit with a VT100 terminal session (reference DLP-001 and DLP-002) or via a Telnet session (reference DLP-006, *Telnetting to the Unit*).

Tools and Materials Required

- Access to a PC or other computer connected to the LAN (Telnet access only).
- VT100 compatible terminal or computer with terminal emulation software.
- Appropriate cable to connect terminal to the unit (customer-provided).
- DB-9 female to RJ-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN-proprietary and is shipped with the unit.
- Ethernet cable from the **10/100BASET** port on the unit to a hub (customer-provided).
- Use Ethernet crossover if going from the unit to a PC (customer-provided).

WARNING

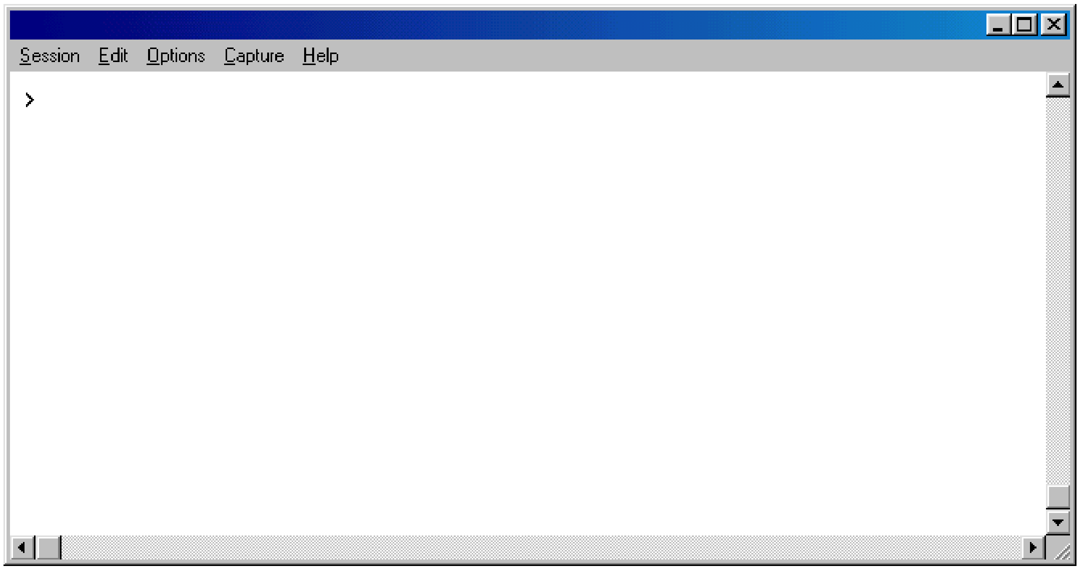
To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

DLP-013

Perform Steps Below in the Order Listed

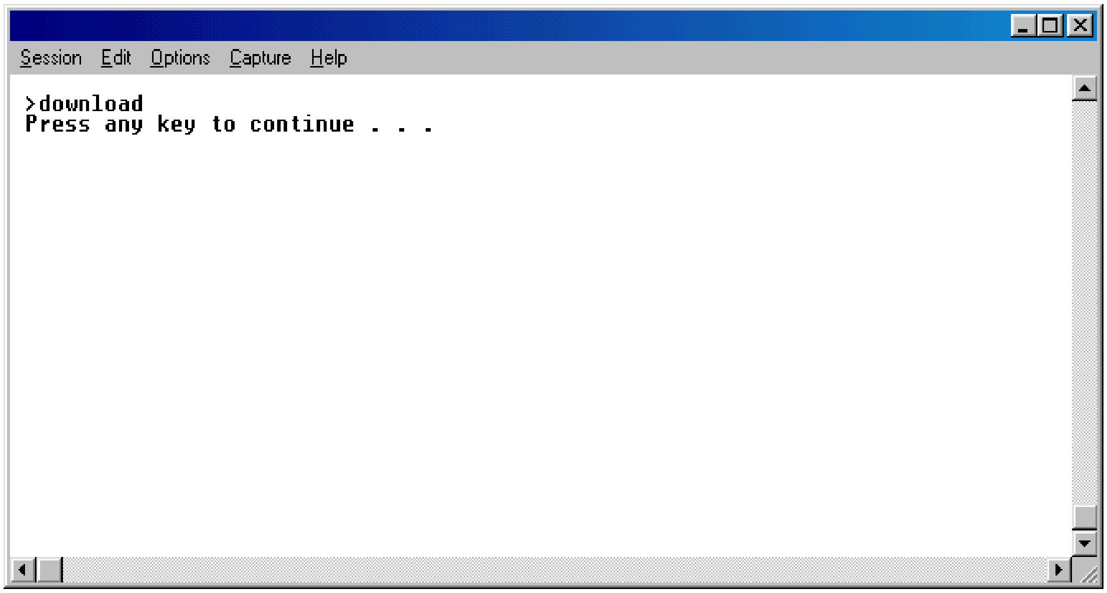
Saving the Router's Configuration

1. Establish a connection to the router with the terminal software either through the **CRAFT** port or via a Telnet session.
2. From the Main Menu, select **SYSTEM UTILITY**, then **TERMINAL MODE**, and then press <Enter>.
3. The following screen will appear.



```
>
```

4. At the terminal prompt, type download and then press <Enter>. The following screen will appear.



```
>download
Press any key to continue . . .
```

5. Don’t press another key yet!
6. Enable "capture" or "logging" in the terminal software, saving it to a file on your computer.
7. Press the SPACE BAR to continue. The router will then print its configuration to the terminal screen. (With capture enabled, the terminal software will capture the configuration and write it to the file that you designated.)
8. When the configuration stops printing, end the capture. The router's configuration is now saved to the file that you designated.
9. At the terminal prompt, type **exit** to go back into the configuration menu of the router.
10. Always use <Ctrl + L> to exit the configuration menu before closing the Telnet or terminal software.

Loading a Configuration into the Router

Follow the steps below to upload the text file back into the unit. These text files can be the entire configuration, or just partial commands that affect specific configuration changes. The uploading steps are the same, no matter the size of the file.

1. Establish a connection to the router with the terminal software either through the **CRAFT** port or via a Telnet session.
2. From the Main Menu, select **SYSTEM UTILITY**, then **TERMINAL MODE**, and then 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. Then type **exit** to go back into the configuration menu of the router.
5. Always use <Ctrl + L> to exit the configuration menu before closing the Telnet or terminal software.

Entering Commands at the Command Prompt

To do this manually from the prompt, precede each instruction with a ">". **After uploading, to apply and save changes, you must issue the command "save" from the prompt.** The command will apply ALL changes to the unit (the same as escaping all the way out of the terminal menu). To do a save to flash only, but not apply the changes, you can go back to the menu system and press <Ctrl + W>. A **!exit** command executes a do not save and a do not ask function (i.e., changes will not be saved and the user will not be prompted to save the changes).

The commands are based on string comparisons with the menu system (with spaces replaced with underscores). This means that the config command will appear exactly as it appears in the terminal menus. To change a configuration, type in the option desired exactly as it appears on the menu. For example, to change the T1 timing mode, the command line would read

```
>sysconfig t1_timing_mode network    or
>sysconfig t1_timing_mode internal   or
>sysconfig t1_timing_mode dsx-1.
```

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

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, 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-009*, Saving the Current Configuration Using TFTP*.
- A script obtained via the terminal mode. See DLP-013 (*Saving the Router's Configuration* section only).

> NOTE *The service provider's access network Layer 1 must be provisioned to map a single 64K 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-45 female adapter for connecting to the **CRAFT** port on the rear of the unit (only required if unit has to be factory defaulted)
- Silver Satin Cable for **CRAFT** access (P/N 3127004 provided with unit, only required if unit has to be factory defaulted)

WARNING

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

DLP-014

Perform 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. The unit begins 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 64K 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-009*, Saving the Current Configuration Using TFTP*.
   - A script obtained via the terminal mode. See DLP-013 (*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.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

A.03 TO A.04 FIRMWARE UPGRADE

Introduction

Until now, the Total Access 600R has been running firmware version A.03.xx. Recently, A.04.xx has been released. 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-009 and DLP-011 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.03.9X (Transition Build) firmware from the ADTRAN website (http://www.ADTRAN.com).

NOTE *For the Total Access 600R, select* **SERVICE/SUPPORT>TECHNICAL SUPPORT>TOTAL ACCESS PRODUCTS>TOTAL ACCESS 600R>FIRMWARE**.

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-45 female adapter for connecting to the **CRAFT** port on the rear of the unit. This adapter is ADTRAN proprietary and is shipped with the unit.

DLP-015

Perform Steps Below in the Order Listed

Upgrade From A.03 to A.03.9X (Transition Build) to A.04

1. Upgrade the firmware from A.03 to A.03.9X (Transition Build) firmware. See DLP-007 or DLP-008 for instructions on how to perform this upgrade.
2. Once the upgrade to A.03.9X is complete, immediately upgrade the unit to A.04. See DLP-007 or DLP-008 for instructions on how to perform this upgrade.

Upgrading from A.03 to A.03.9X (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-007 or DLP-008 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.
   - 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.
3. Reconfigure the unit for the specific application.

Upgrading from A.03 to A.04 directly (or from A.04 to A.03 directly) will erase the unit's configuration.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

ADTRAN UTILITIES

ADTRAN delivers several PC software utilities with the unit. These utilities are located on the CD-ROM that came with your shipment. They also include MIB files (located in the MIB directory).

Review the readme file (Readme.txt) for the latest information about the utilities.

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 Telnet, VT100, and TFTP Server utilities.

CONTENTS

FIGURES

1. TELNET UTILITY

The Telnet utility delivered with the unit provides enhancements to standard Telnet programs that make it easier to work with unit options.

Access the Telnet program remotely through the **10/100BASET** Ethernet port. For a detailed description of how to work with the Telnet program, refer to *Navigating the Terminal Menus* in the User Interface Guide section of this manual. If you need help setting up the unit for a Telnet session, refer to the Detailed Level Procedures section of this manual.

The Telnet menus include **SESSION**, **EDIT**, **OPTIONS**, **CAPTURE**, and **HELP** (see the menu tree in Figure 1).

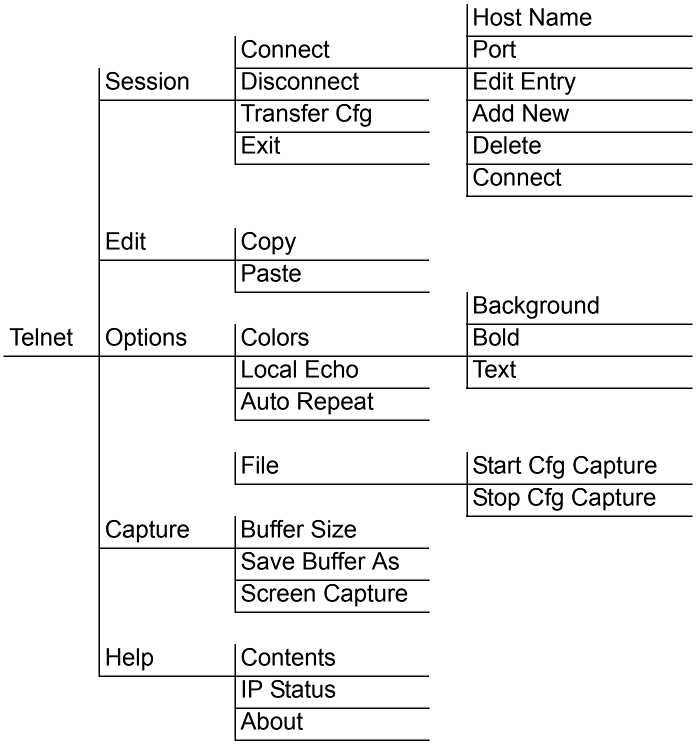


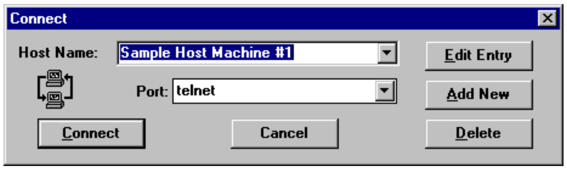
Figure 1. Telnet Menu Tree

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: Sample Host Machine #1

Port: telnet

Host Name

Accepts and stores host names. You may enter 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.

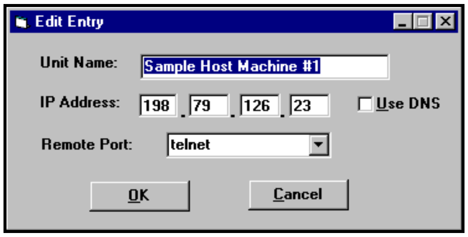
PORT

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 **(.)** while the cursor is located in each IP field, that field entry is deleted.



Unit Name: Sample Host Machine #1

IP Address: 198 . 79 . 126 . 23

□ Use DNS

Remote Port: telnet

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; simply 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 primarily for sending 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. 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 on-line help for using the ADTRAN Utilities.

Contents

Opens the on-line 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 Menus* in the User Interface Guide section of this manual. If you need help setting up the unit for a VT100 session, refer to the Detailed Level Procedures section of this manual.

VT100 menus include **SESSION**, **EDIT**, **PORT**, **OPTIONS**, **CAPTURE**, and **HELP** (see the menu tree in Figure 2).

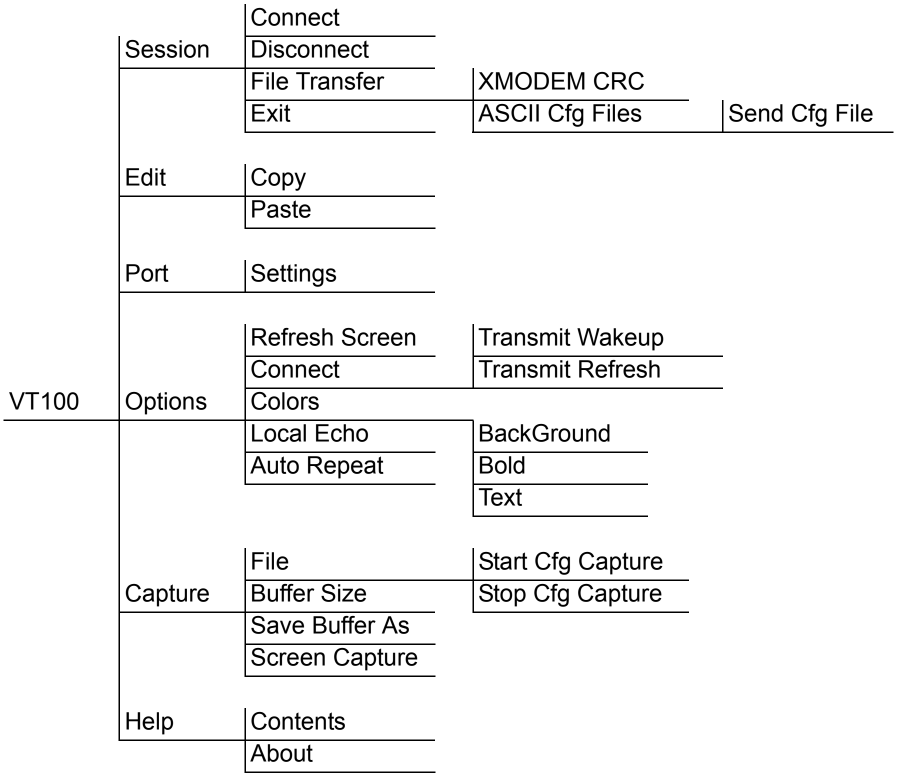


Figure 2. VT100 Menu Tree

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 the unit.

XMODEM CRC

Selects the XMODEM file transfer protocol.

ASCII Cfg Files

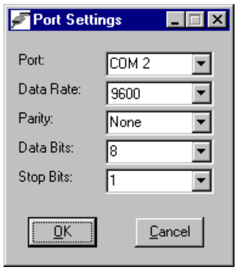
Selects ASCII transfer mode. Primarily useful for configuration transfers for the ADTRAN products.

Edit Menu

Identical to the Telnet **EDIT MENU** (see *Edit Menu* on page 183).

Port Menu

Changes serial COM **PORT SETTINGS**. Provides data rate settings from 300 - 57600 bps.



Port Settings

Port: COM 2

Data Rate: 9600

Parity: None

Data Bits: 8

Stop Bits: 1

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 **CRAFT** port online in terminal mode.

Transmit Refresh

Provides a control sequence to refresh the screen automatically when connecting. This is the default setting.

Colors

Identical to Telnet **COLORS** Menu (see *Colors* on page 184).

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 184).

Help Menu

Provides on-line help and information about the version number.

Contents

Opens on-line help.

About
Displays version and owner information.

3. TFTP SERVER

The TFTP Server utility transfers configuration files to and from a TFTP server. You can install this program on a PC running any version of Microsoft Windows. The configuration of the 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 **10/100BASET** 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 3 shows the TFTP Sever Interface Menu Tree. Figure 4 shows the TFTP server interface. For information on transferring and saving configurations using TFTP, refer to the Detailed Level Procedures section of this manual.

NOTE *Files must be placed in the Application directory where you installed the product. Received files are also placed here.*

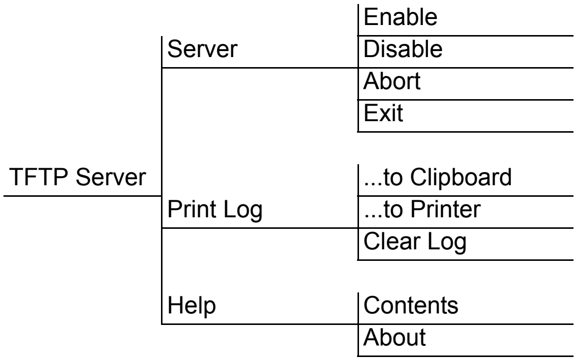
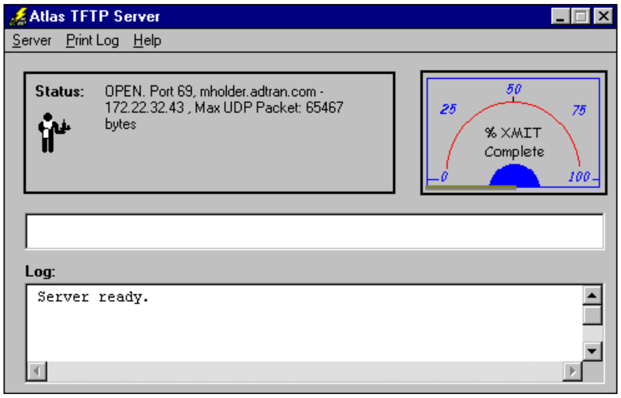


Figure 3. TFTP Server Interface Menu Tree



Status: OPEN. Port 69, mholder.adtran.com - 172.22.32.43 , Max UDP Packet: 65467 bytes

Log:

```
Server ready.
```

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 the 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 **Port Closed** displays 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 on-line help and version information.

Contents
Opens on-line 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 process.

6. LOG FIELD

This field displays a record of all of the events that occur while 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.

MIB

This section details the Management Information Bases (MIBs) supported, MIB Compilation Order, Traps Supported, and MIB Variables supported.

CONTENTS

The Total Access 600R supports SNMP Version 2.

As the MIBs are used for multiple Total Access 600 units, various voice options will appear in SNMP. If a voice option is selected for the 600R, SNMP will return an error.

1. MIBs Supported by the Total Access 600R

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
RFC3201.mi2	CIRCUIT-IF-MIB

Enterprise MIBs:

adtran.mi2	ADTRAN-MIB
adIadSys.mi2	ADTRAN-ADIADSYS-MIB
adIadRtr.mi2	ADTRAN-ADIADROUTER-MIB

NOTE *SNMPv2-SMI, SNMPv2-TC, SNMPv2-TM, SNMPv2-CONF should be included with the SNMP manager.*

NOTE *All MIBs for the Total Access 600R are SNMPv2.*

2. MIB COMPILATION ORDER

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

CIRCUIT-IF-MIB

ADTRAN-MIB

ADTRAN-IADSYS-MIB

ADTRAN-IADROUTER-MIB

3. TRAPS SUPPORTED BY THE TOTAL ACCESS 600R

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 adIadDs1CRC - 1003217 adIadDs1LCV - 1003218 adIadDs1SLP - 1003219

4. MIB VARIABLES SUPPORTED BY THE TOTAL ACCESS 600R

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.