## TOTAL ACCESS 850
### System Manual

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1200375L1</td>
<td>Total Access 850 Chassis</td>
</tr>
<tr>
<td>1200373L1</td>
<td>T1 Bank Controller Unit (BCU)</td>
</tr>
<tr>
<td>1200373L2</td>
<td>T1 BCU with DSX Port</td>
</tr>
<tr>
<td>4203376L1#TDM</td>
<td>T1 Router Control Unit (RCU) with TDM Software</td>
</tr>
<tr>
<td>4203376L1#ATM</td>
<td>T1 RCU with ATM Software</td>
</tr>
<tr>
<td>1203376L1</td>
<td>3rd Generation T1 RCU</td>
</tr>
<tr>
<td>1200377L1</td>
<td>SDSL RCU</td>
</tr>
<tr>
<td>1200377L2</td>
<td>2nd Generation SDSL RCU</td>
</tr>
<tr>
<td>1203384L2</td>
<td>Echo Canceller with ADPCM</td>
</tr>
<tr>
<td>1175006L2</td>
<td>Power Supply Unit</td>
</tr>
<tr>
<td>1175043L3</td>
<td>AC Supply/Battery Charger</td>
</tr>
</tbody>
</table>
Trademarks
Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

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

To the Holder of the Manual
The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.
In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

About this Manual
This manual provides a complete description of the Total Access 850 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 850. This manual is arranged so that needed information can be quickly and easily found.
Revision History

<table>
<thead>
<tr>
<th>Document Revision</th>
<th>Date</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>April 2004</td>
<td>This is the first issue of this manual. The previous version of this product was covered under document 64200376L1-1.</td>
</tr>
<tr>
<td>B</td>
<td>August 2004</td>
<td>Update licensing and warranty agreement; correct third generation part numbers.</td>
</tr>
</tbody>
</table>

Conventions

**NOTE**

Notes provide additional useful information.

**CAUTION**

Cautions signify information that could prevent service interruption.

**WARNING**

Warnings provide information that could prevent damage to the equipment or endangerment to human life.
Safety Instructions

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

1. Do not use this product near water, such as a bathtub, wash bowl, kitchen sink, laundry tub, in a wet basement, or near a swimming pool.
2. Avoid using a telephone (other than a cordless-type) during an electrical storm. There is a remote risk of shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.
4. Use only the power cord, power supply, and/or batteries indicated in the manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for special disposal instructions.

Save These Important Safety Instructions
FCC-Required Information

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

1. This equipment complies with Part 68 of the FCC rules and requirements adopted by ACTA. On 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 your 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 compliant with Part 68 and requirements adopted by ACTA.

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

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Registration Number</th>
<th>Service Type</th>
<th>REN/SOC</th>
<th>FIC</th>
<th>USOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1200373L2</td>
<td>HDCUSA35154DEN</td>
<td>1.544 Mbps - SF, 1.544 Mbps - SF and B8ZS</td>
<td>6.0N</td>
<td>04DU9-BN</td>
<td>RJ-48C</td>
</tr>
<tr>
<td>1203378L1</td>
<td></td>
<td>1.544 Mbps - ESF, 1.544 Mbps - ESF and B8ZS</td>
<td></td>
<td>04DU9-1KN</td>
<td></td>
</tr>
<tr>
<td>1175407L2</td>
<td>HDCUSA35118CNN</td>
<td>Analog Loop Start/Ground Start</td>
<td>2.9A</td>
<td>02LS2</td>
<td></td>
</tr>
<tr>
<td>1175408L2</td>
<td>HDCUSA35102CNN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8. The REN is used to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your number is called. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs of all devices should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

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

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

NOTE

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

WARNING

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.
Affidavit Requirements for Connection to Digital Services

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

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

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

- Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirements for subrate services are waived.
AFFIDAVIT FOR CONNECTION OF CUSTOMER PREMISES EQUIPMENT
TO 1.544 MBPS AND/OR SUBRATE DIGITAL SERVICES

For the work to be performed in the certified territory of __________________ (telco name)
State of ________________
County of ________________
I, ________________ (name), ________________________________ (business address),
____________________ (telephone number) being duly sworn, state:
(   ) I have responsibility for the operation and maintenance of the terminal equipment to be connected to 1.544 Mbps
and/or ________ subrate digital services. The terminal equipment to be connected complies with Part 68 of the
FCC rules except for the encoded analog content and billing protection specifications. With respect to encoded
analog content and billing protection:
(   ) I attest that all operations associated with the establishment, maintenance, and adjustment of the digital CPE with
respect to analog content and encoded billing protection information continuously complies with Part 68 of the
FCC Rules and Regulations.
(   ) The digital CPE does not transmit digital signals containing encoded analog content or billing information which
is intended to be decoded within the telecommunications network.
(   ) The encoded analog content and billing protection is factory set and is not under the control of the customer.
I attest that the operator(s)/maintainer(s) of the digital CPE responsible for the establishment, maintenance, and
adjustment of the encoded analog content and billing information has (have) been trained to perform these functions
by successfully having completed one of the following (check appropriate blocks):
(   ) A. A training course provided by the manufacturer/grantee of the equipment used to encode analog signals;
or
(   ) B. A training course provided by the customer or authorized representative, using training materials and
instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or
(   ) C. An independent training course (e.g., trade school or technical institution) recognized by the
manufacturer/grantee of the equipment used to encode analog signals; or
(   ) D. In lieu of the preceding training requirements, the operator(s)/maintainer(s) is (are) under the control of a
supervisor trained in accordance with _________ (circle one) above.

I agree to provide ______________________ (telco’s name) with proper documentation to demonstrate compliance
with the information as provided in the preceding paragraph, if so requested.
_________________________________Signature
_________________________________Title
_________________________________ Date
Transcribed and sworn to before me
This ________ day of ________________, _______

_________________________________ Notary Public
My commission expires:

_________________________________
Industry Canada Compliance Information

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

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

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

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

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

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

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

Canadian Emissions Requirements

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

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Class A prescrites dans la norme sur le materiel brouilleur: “Appareils Numériques,” NMB-003 edictee par le ministre des Communications.
Product Warranty
ADTRAN will repair and return this product within the warranty period if it does not meet its published specifications or fails while in service. Warranty information can be found at www.adtran.com/warranty.

Software Licensing Agreement
Each ADTRAN product contains a single license for ADTRAN supplied software. Pursuant to the Licensing Agreement, you may: (a) use the software on the purchased ADTRAN device only and (b) keep a copy of the software for backup purposes. This Agreement covers all software installed on the system as well as any software available on the ADTRAN website. In addition, certain ADTRAN systems may contain specific conditions for obtaining software upgrades. The full ADTRAN Software Licensing Agreement can be found at www.adtran.com/licensing.

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

Customer Service, Product Support Information, and Training
ADTRAN will replace or repair this product within the warranty period if it does not meet its published specifications or fails while in service. Warranty information can be found at www.adtran.com/warranty.
A return material authorization (RMA) is required prior to returning equipment to ADTRAN. For service, RMA requests, training, or more information, use the contact information given below.

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

CaPS Department (256) 963-8722

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

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

RMA # ______________

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

http://support.adtran.com
When needed, further pre-sales assistance is available by calling our Applications Engineering Department.

Applications Engineering  (800) 615-1176
Post-Sale Support
Your reseller should serve as the first point of contact for support. If additional support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, updated firmware releases, latest product documentation, service request ticket generation and trouble-shooting tools. All of this, and more, is available at:

http://support.adtran.com

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

Technical Support  (888) 4ADTRAN

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

http://www.adtran.com/aces

For questions, call the ACES Help Desk.

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

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

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

Section 1 System Description ......................................................... 15
This section provides an overview of the Total Access 850 system.

Section 2 Engineering Guidelines .................................................... 23
This section provides equipment dimensions, power requirements, front panel design, rear panel design, LEDs, and at-a-glance specifications.

Section 3 Network Turnup Procedure ................................................. 55
This section provides shipment contents list, grounding instructions, mounting options, and specifics of supplying power to the unit.

Section 4 User Interface Guide .......................................................... 65
This section provides detailed descriptions of all menu options and configuration parameters available for the Total Access 850 when used with a Router Control Unit (RCU). This section does not apply to systems that employ a Bank Control Unit (BCU).
This section of ADTRAN's Total Access 850 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 5 Detail Level Procedures ...................................................... 213
DLP-1 Connecting a VT100 Terminal or PC to the CRAFT Port .................. 215
DLP-2 Logging in to the System ......................................................... 217
DLP-3 Setting IP Parameters for the Total Access 850 .............................. 219
DLP-4 Verifying Communications Over an IP LAN ................................. 221
DLP-5 Connecting to the Total Access 850 Using Telnet ........................... 225
DLP-6 Adding/Removing Users and Changing Password Security Levels ............ 229
DLP-7 Updating the Firmware using TFTP ............................................ 233
DLP-8 Updating the Firmware using XMODEM ....................................... 237
DLP-9 Saving the Current Configuration Using TFTP ............................... 239
DLP-10 Loading a Configuration Using TFTP ....................................... 241
DLP-11 Saving and Transferring a Current Configuration Using XMODEM .......... 245
DLP-12 Loading a Configuration Using XMODEM ................................ 247
DLP-13 Saving and Loading Text Configuration using Terminal Command Line .... 249
DLP-14 A.03 to A.04 Firmware Upgrade ............................................. 253
DLP-15 Using the ADTRAN Utility Syslog ......................................... 257
DLP-16 Connecting the Alarm Contacts and the External Input .................... 261
DLP-17 Configuring the Total Access 850 for Dual T1 Maps ....................... 265

Section 6 ADTRAN Utilities ............................................................... 269
This section provides instructions for configuring and using the ADTRAN Utilities software programs including Telnet, VT100, Syslog, and TFTP.

Section 7 MIBs ........................................................................... 279
This section is divided into two parts: (1) SNMP information for TDM units and (2) SNMP information for ATM units. Each section details the Management Information Bases (MIBs) supported, MIB Compilation Order, Traps Supported, and MIB Variables supported.
SYSTEM DESCRIPTION

This section provides an overview of the Total Access 850 system.

CONTENTS

Features and Benefits ................................................................. 19
  Configuration and Management ........................................... 19
  Software Upgradeable ......................................................... 19
  Signaling Support .............................................................. 19
  Integrated Components (with RCU) ............................... 20
  Testing ................................................................. 20
  Performance Monitoring ........................................... 20

Modules ................................................................. 20
  Total Access 850 Bank Controller Unit (BCU) (P/N 1200373L1) ....... 21
  BCU with Fractional T1 (P/N 1200373L2) .......................... 21
  T1 RCU (P/N 4203376L1#TDM, 4203376L1#ATM and 1203376L1) ...... 21
  SDSL RCU (P/N 1200377L1, 1200377L2) ............................ 21
  Power Supply Unit (P/N 1175006L2) ..................................... 22
  Echo Canceller with ADPCM (P/N 1203384L2) ....................... 22
  Nx56/64K (V.35) Module (P/N 1200372L1) ........................... 22
  Quad FXS Access Module (P/N 1175408L2) .......................... 22
  Quad FXO Access Module (P/N 1175407L2) .......................... 22
  OCU DP Access Module (P/N 1180005L1) ........................... 23
  U-BR1TE Access Module (P/N 1180020L1) ........................... 23
  E&M/TO Access Module (P/N 1180402L1) ........................... 23
  Dual V.35 Access Module (P/N 1180025L1) ......................... 23
  DSX-1 Access Module (P/N 1200385L1) ............................ 23
  Single DS0 DP Access Module (P/N 1180003L1) ................. 23
1. SYSTEM OVERVIEW

The Total Access 850 is an integrated access device designed for cost-effective deployment of voice and data services at the customer premises. The Total Access 850 system benefits integrated communications providers, such as CLECs, ILECs, and ISPs, who require a customer premises device that integrates voice and data functions. It provides a viable migration path from TDM to packet-based technology (see Modules on page 18 for details). The Total Access 850 features remote management, an integrated IP router, and special services slots. Preconfigured Total Access 850 packages are available.

The Total Access 850 is a modular device with two common slots, six access slots for FXS, FXO, Dual V.35, and UBRITE modules, and two slots for special access modules. The FXS, FXO, Dual V.35, and UBRITE modules are supported in the Router Control Unit (RCU); however, the Bank Controller Unit (BCU) also supports E&M, OCU DP, Single DS0 DP, and Nx56/64 modules. Using local or remote inband management, carriers can turn features, functions, and access ports on and off. Easy access to modules, common modules, power supplies, and the battery back-up system simplifies maintenance procedures. Hot-swappable modules may be replaced without disrupting other units. The four-circuit-per-module design ensures that only four analog circuits are affected when replacing a module.

The Total Access 850 is a compact, NEBS-compliant cabinet suitable for the customer premises or the central office. The 2U design uses little rack space; or when wallmounted, the 8½-inch by 11-inch chassis occupies a space the size of a piece of notebook paper. Two Total Access 850 systems can be mounted side-by-side in either 19-inch or 23-inch relay racks.

2. FEATURES AND BENEFITS

The following list gives Total Access 850 features and benefits. Some features are module-dependent.

Configuration and Management
- VT100 Emulation
- SNMP Management (with RCU)
- Telnet (with RCU)
- Dial-up remote management via external analog modem
- Six levels of password protection and privileges for Telnet access (with RCU)

Software Upgradeable
- Flash memory
- TFTP download (with RCU)
- XMODEM via control port

Signaling Support
- T1/FT1 integrated access
- TDM to ATM migration (with RCU)
- Upgradeable to DSL using SDSL RCU
- TR-08 signaling support
- Analog FXS and FXO voice expansion (four per module)
Integrated Components (with RCU)

- IP router
- DSX-1 T1/PBX interface
- V.35 Nx56/64 DTE interface

Testing

- Local and remote: payload/line, V.54 (depending on installed modules)
- Patterns: 511, QRSS, all ones, all zeros (depending on installed modules)

Performance Monitoring

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

3. MODULES

The Total Access 850 system offers several different system modules (including the power supply), system resource modules, and access modules.

System Modules

- Bank Controller Unit (BCU) (P/N 1200373L1)
- BCU with Fractional T1 (P/N 1200373L2)
- T1 Router Control Unit (RCU) with TDM software (P/N 4203376L1#TDM)
- T1 Router Control Unit (RCU) with ATM software (P/N 4203376L1#ATM)
- 3rd Generation T1 Router Control Unit (RCU) (P/N 1203376L1)
- SDSL RCU (P/N 1200377L1)
- 2nd Generation SDSL RCU (P/N 1200377L2)
- Power Supply Unit (P/N 1175006L2)

Resource Modules

- Echo Canceller with ADPCM (P/N 1203384L2)
- Nx56/64K Data Service Unit (DSU) (P/N 1200372L1)

Access Modules

- Quad FXS Access Module (P/N 1175408L2)
- Quad FXO Access Module (P/N 1175407L2)
- UBR1TE Access Module (P/N 1180020L1)
- Dual V.35 Access Module (P/N 1180025L1)
- DSX-1 Access Module (P/N 1200385L1)
Access Modules (Requiring a BCU)

- E&M/TO Access Module (P/N 1180402L1)
- OCU DP Access Module (P/N 1180005L1)
- Single DS0 DP Access Module (P/N 1180003L1)
- Nx56/64 (V.35) Access Module (P/N 1200372L1)

Each access module is hot-swappable, with configuration restored upon replacement.

Replacing an access module with a different module type will result in configuration loss.

Total Access 850 Bank Controller Unit (BCU) (P/N 1200373L1)

The BCU is a common module plug-in unit with a built-in CSU. The BCU provides all control functions for the Total Access 850 common units and all individual access modules. A faceplate DB-9 (ADMIN) interface provides access for a VT100 terminal for screen menu provisioning, and bantam test jacks provide transmit and receive monitoring. An additional DB-9 (TEST) interface provides timing for DS0 test equipment. Faceplate LEDs show status information for the network and Fractional T1 (DSX-1 on L2 only). The unit consists of a main circuit board and daughter card and inserts directly in the controller slot on the Total Access 850 shelf. An 8-position DIP-switch is mounted on the daughter card and is used for T1 provisioning and clocking.

BCU with Fractional T1 (P/N 1200373L2)

The BCU with Fractional T1 provides all the functionality of the traditional BCU as well as a DSX-1/Fractional T1 interface for additional T1 service.

T1 RCU (P/N 4203376L1#TDM, 4203376L1#ATM and 1203376L1)

The RCU is a dual board assembly that provides the network interface for the Total Access 850 system. The RCU can provision, test, and provide status for any card in the system. A faceplate DB-9 (CRAFT) interface provides access for a VT100 terminal for screen menu provisioning, and bantam test jacks provide transmit and receive monitoring capabilities. Terminal menu access is also provided through the RJ-45 CRAFT interface located on the rear of the chassis. Faceplate LEDs show status information for the network port and Ethernet port. In addition, the RCU has an integrated router access through the 10BaseT connector on the backplane of the chassis. (3rd Generation RCUs provide a 10/100BaseT interface.) A DSX-1/Fractional T1 interface for additional T1 service is also provided.

SDSL RCU (P/N 1200377L1, 1200377L2)

The SDSL RCU is a dual board assembly that includes an SDSL network interface, Nx56/64 V.35 interface, and built-in IP router. The SDSL RCU can provision, test, and provide status for any card in the system. The faceplate has a DB-9 (CRAFT) port connection, and network, V.35, and Ethernet LEDs. An additional RJ-45 terminal menu interface is located on the rear of the chassis and is labeled CRAFT. The SDSL RCU is only used in ATM applications. It supports vendor-specific SDSL protocols, ATM, and Copper Mountain Frame Relay. Therefore, the SDSL RCU can interoperate with a variety of DSLAMs, including Lucent, Nortel, Copper Mountain, Nokia, and Alcatel. It also supports several voice gateways, including Jetstream and Broadband Loop Emulation Services (BLES) gateways. The SDSL RCU has
built-in Echo Cancellation for up to 24 voice ports. Adaptive Differential Pulse Code Modulation (ADPCM) resources are also built-in for up to 16 ports.

**Power Supply Unit (P/N 1175006L2)**

The Total Access 850 PSU is a common module plug-in unit designed to supply power to the system. The faceplate contains a momentary ACO pushbutton, a ring voltage Enable/Disable pushbutton, a Bank Alarm LED, Ring LED, and a power LED. All power, ground, and timing signals are pre-wired, thus eliminating additional wiring requirements.

**Echo Canceller with ADPCM (P/N 1203384L2)**

An Echo Canceller Module is available for use with the legacy T1 RCU (P/N 1200376L1 - ATM firmware only). Echo cancellation and ADPCM resources are built into the 3rd Generation T1 (P/N 1203376L1) and SDSL (P/N 1200 377Lx) versions of the RCU, so this module is not required when using the SDSL RCU. The Echo Canceller Module provides G.168 echo cancellation for voice over ATM applications and includes Adaptive Differential Pulse Code Modulation (ADPCM). ADPCM is a speech coding method which uses fewer bits than traditional Pulse Code Modulation (PCM), allowing the user to get more analog voice calls on less bandwidth. This is a dual-slot module and must be installed in the system resource slots (A and B).

---

**NOTE**

The Echo Canceller module ADPCM functionality automatically shifts ON/OFF when fax or modem calls are placed. To find out the current status of the Echo Canceller functionality, check the current status of each FXS port. The path of the current status can be found at the following path: **L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > PVC STATUS > PROTOCOL STATUS > POTS STATS > CODING TYPE** (this will display either PCM or ADPCM).

---

**Nx56/64K (V.35) Module (P/N 1200372L1)**

This module is only available in Total Access 850 systems using a BCU. The Nx56/64k (V.35) Module activates the V.35 port on the rear of the chassis. This is a dual-slot module and must be installed in the system resource slots (A and B).

**Quad FXS Access Module (P/N 1175408L2)**

The Quad FXS Module provides analog voice extension for the Total Access 850 platform. Four analog voice ports are used to connect to analog phones. The Quad FXS Module supports Foreign Exchange Subscriber, Dial Pulse Terminate (DPT), and Private Line Automatic Ringdown (PLAR) and provides Ground Start/Loop Start to E&M conversion capability.

**Quad FXO Access Module (P/N 1175407L2)**

The Foreign Exchange Office (FXO) module interfaces to the Central Office switch and to an FXS or RPOTS card over a T1 facility. Four analog voice ports on the FXO access module provide four individual connections to the switch. The FXO supports standard Loop Start and Ground Start options as well as Dial Pulse Terminate (DPT) functionality. Up to six Quad FXO Access Modules may be installed in the Total Access 850.
OCU DP Access Module (P/N 1180005L1)
This module is only available in Total Access 850 systems using a BCU. The OCU DP module is a single port access module used to provide the interface between a DS0 time slot on the T1 and a 4-wire DDS device at the customer premises. The OCU DP supports up to 18 kft of copper for remote DSU connectivity.

U-BR1TE Access Module (P/N 1180020L1)
The U-BR1TE is a module that plugs into a single access slot of the Total Access 850. It provides an ISDN U-interface and allows transport of Basic Rate 2B+D information over T1 carriers and twisted pair wiring.

E&M/TO Access Module (P/N 1180402L1)
This module is only available in Total Access 850 systems using a BCU. The E&M/TO module is a single port Ear and Mouth/Transmit Only access module. The primary application for this module is to provide PBX foreign exchange at the customer premises or tandem central office applications. This module is intended for interface with intra-building wiring. The E&M/TO module supports both 2- and 4- wire operation.

Dual V.35 Access Module (P/N 1180025L1)
The Dual V.35 Access Module is a DSU data port with two circuits that each deliver serial data over a V.35 interface. The module is designed as a dual slot module; it requires two slots in the Total Access 850 chassis. Each circuit of the Dual V.35 Access Module provides up to 24 channels of data in 56 or 64 kbps increments. Design operation is to transmit or receive high rate synchronous data from data terminal equipment (DTE) over a T1 interface. This module is currently only supported by the TDM version of the T1 RCU.

DSX-1 Access Module (P/N 1200385L1)
This module is only available in Total Access 850 systems using a T1 RCU. The DSX-1 Module installs into the Total Access 850 system to provide an additional DSX-1 interface (RJ-45) for support of multiple PBXs or other equipment with a DSX-1/FT1 interface. The module is functional in any of the six Total Access 850 module slots.

Single DS0 DP Access Module (P/N 1180003L1)
This module is only available in Total Access 850 systems using a BCU. The DS0 Dataport is a single port access module that serves as an interface to the basic DDS DS0 (64 kbps) signal to a T-carrier line. This module is used in conjunction with an ADTRAN All-Rate Office Channel Unit (OCU) dataport or Total Reach DDS dataport located at the end office to extend the DDS network to an end office which has exclusively-served voice channels.
This section provides equipment dimensions, power requirements, front panel design, rear panel design, LEDs, and at-a-glance specifications.

**CONTENTS**

**Power Requirements**
- AC System ........................................... 25
- DC System .......................................... 25

**Reviewing the Front Panel Design** .............................................................. 25
- Bank Controller Unit (1200373L1 and 1200373L2). ....................... 26
- T1 Router Controller Unit (4200376L1#TDM and 4200376L1#ATM) .......... 28
- 3rd GEN T1 Router Controller Unit (1203376L1) .................. 30
- DSL Router Controller Unit (1200377L1 and 1200377L2) .......... 32

**Reviewing the Rear Panel Design** .............................................................. 33
- 10/100BaseT Connection (JP1) ........................................ 34
- T1 Connection (JP2) ........................................ 35
- DSX-1 Connection (JP3) ........................................ 35
- Rear CRAFT Port (JP4) ........................................ 36
- Ns56k/64k Port (J1) ........................................ 37
- Alarm Relay Connection (P5) ........................................ 37
- Clock Wire-Wrap Strip (P1) ........................................ 38
- Customer Connection (P2) ........................................ 38
- T1 Wire-Wrap Connection (P3) ........................................ 39
- Power Connections (P6 and P7) ........................................ 39

**Access Module Interfaces** .............................................................. 40
- Power Supply Unit (P/N 1175006L2) ........................................ 40
- Quad FXS Access Module (P/N 1175408L2) ...................................... 41
- Quad FXO Access Module (P/N 1175407L1) ...................................... 43
- UBR1TE Access Module (P/N 1180020L1) ...................................... 45
- OCU DP Access Module (P/N 1180005L1) ...................................... 49
- E&M/TO Access Module (P/N 1180402L1) ...................................... 49
- Dual V.35 Access Module (P/N 1180005L1) ...................................... 50
- DSX-1 Access Module (P/N 1200385L1) ...................................... 52

**FIGURES**
- Figure 1. Total Access 850 Front Panel Layout ........................................ 25
- Figure 2. BCU Bantam Jack Test Diagram ........................................ 28
- Figure 3. BCU DB-9 Test Connector ........................................ 28
- Figure 4. RCU Bantam Jack Test Diagram ........................................ 30
- Figure 5. 3rd GEN RCU Bantam Jack Test Diagram .................................. 31
- Figure 6. Total Access 850 Rear Panel ........................................ 33
- Figure 7. Connector Pinout ........................................ 38
- Figure 8. Alternate Power Connection ........................................ 40
- Figure 9. Quad FXS Connector Pin Assignments .................................. 42
- Figure 10. Quad FXO Connector Pin Assignments .................................. 44

**TABLES**
- Table 1. BCU Faceplate LEDs ........................................ 26
- Table 2. BCU DIP-Switch S1 Options ........................................ 26
- Table 3. T1 RCU CRAFT (DB-9, Female) Pinout .................................. 29
Table 4. T1 RCU Faceplate LEDs ................................................................. 29
Table 5. 3rd GEN T1 RCU CRAFT (DB-9, Female) Pinout ................................. 30
Table 6. 3rd GEN T1 RCU Faceplate LEDs .................................................. 31
Table 7. SDSL RCU CRAFT (DB-9, Female) Pinout ...................................... 32
Table 8. SDSL RCU Faceplate LEDs ............................................................ 32
Table 9. SDSL RCU DIP-Switch S1 Options .................................................. 33
Table 10. Total Access 850 Backplane Connections ....................................... 34
Table 11. Ethernet Pinout ............................................................................. 34
Table 12. Network Connection Pinout ............................................................ 35
Table 13. DSX-1 Network Connection Pinout ................................................ 36
Table 14. Rear CRAFT Pinout ...................................................................... 36
Table 15. V.35 Winchester Pinout ................................................................. 37
Table 16. Alarm Relay Connector Pinout ....................................................... 37
Table 17. Alarm Notification ........................................................................ 38
Table 18. T1 Wire-Wrap Connector Pinout ..................................................... 39
Table 19. PSU Faceplate LEDs ..................................................................... 41
Table 20. Quad FXS Module Faceplate LEDs ................................................ 41
Table 21. Quad FXS Module Specifications .................................................... 42
Table 22. Quad FXS Module Compliance Codes .......................................... 43
Table 23. Quad FXO Module Faceplate LEDs ................................................ 43
Table 24. Quad FXO Module Specifications ................................................... 44
Table 25. Quad FXO Module Compliance Codes .......................................... 45
Table 26. UBR1TE Module Faceplate LEDs .................................................. 45
Table 27. UBR1TE Slot/Amphenol Assignment ............................................. 46
Table 28. BCU DIP-Switch S1 Options ........................................................... 46
Table 29. UBR1TE Module Specifications ....................................................... 48
Table 30. UBR1TE Module Compliance Codes ............................................. 48
Table 31. OCU DP Pinout .............................................................................. 49
Table 32. E&M/TO Pinout ........................................................................... 49
Table 33. Dual V.35 Module Faceplate LEDs ................................................ 50
Table 34. Dual V.35 Interface Pinout (DB-26 to V.35) .................................... 50
Table 35. Dual V.35 Module Specifications .................................................... 51
Table 36. Dual V.35 Module Compliance Codes ............................................ 52
Table 37. DSX-1 Module Faceplate LEDs ...................................................... 53
Table 38. DSX-1 Module Interface Pinout ....................................................... 53
Table 39. DSX-1 Module Specifications ........................................................ 53
1. **EQUIPMENT DIMENSIONS**

The Total Access 850 chassis is 8.5” W, 11” D, and 3.5” H and can be mounted in a 19-inch or 23-inch rack (mounting brackets included in shipment). All other equipment (modules) fit inside the base unit.

2. **POWER REQUIREMENTS**

Regardless of the configuration of access modules installed in the chassis, the following power requirements apply:

**AC System**

90/130 VAC, 60 Hz, 50 Watt Max

**DC System**

40/56 VDC, 50 Watt Max

3. **REVIEWING THE FRONT PANEL DESIGN**

Figure 1 shows the Total Access 850 front panel. Refer to *Access Module Interfaces* on page 40 for a discussion of available modules and the front panel functions of each.

---

**NOTE**

UL 60950/NEBS requires all Total Access 850 empty slots to be covered with blank panels (P/N 1175099L1).
Bank Controller Unit (1200373L1 and 1200373L2)

The following is operational information pertaining to the Bank Controller Unit when used with the Total Access 850 system.

**Faceplate LEDs**

The faceplate Network LEDs labeled **T1 NETWORK** and **T1 FRACTIONAL** provide status information using a color coded message format. Table 1 gives a description of all faceplate LEDs for the BCU when used with the Total Access 850 system.

### Table 1. BCU Faceplate LEDs

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network/Frac T1</td>
<td>OFF</td>
<td>there is no power to the system.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>the unit is in Red Alarm (meaning the T1 is down, not connected, or framing is improperly configured).</td>
</tr>
<tr>
<td></td>
<td>YELLOW</td>
<td>the unit is receiving Yellow Alarm (meaning the far end unit is in Red Alarm).</td>
</tr>
<tr>
<td></td>
<td>Solid GREEN</td>
<td>the unit is functioning normally.</td>
</tr>
<tr>
<td></td>
<td>Blinking GREEN</td>
<td>the network T1 interface is in Test mode.</td>
</tr>
</tbody>
</table>

**DIP-Switch Settings**

The Total Access 850 BCU can be provisioned from DIP-switches (S1) mounted on the PCB, or through screen menus accessed via the faceplate **ADMIN** interface. Basic T1 provisioning, clock source, and CSU loopback options are found on the DIP-switch panel. Table 2 gives DIP-switch provisioning information. DIP-switch S1 must be provisioned without the BCU in the chassis. Once the BCU is installed, any software provisioning made will override the DIP-switch settings. If the BCU is withdrawn and reinserted (power-cycled), the software options remain in effect. If a DIP-switch setting is changed while the BCU is withdrawn, the new DIP-switch setting takes effect. If none of the DIP-switch settings were changed, the unit will be provisioned for the last software settings.

### Table 2. BCU DIP-Switch S1 Options

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1-1</td>
<td>Framing Format</td>
<td>Enables either Extended Superframe Format (ESF) or Superframe Format (SF). This option must be configured identically with all other T1 network equipment on this circuit.</td>
</tr>
<tr>
<td></td>
<td>ON*</td>
<td>SF</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>ESF</td>
</tr>
</tbody>
</table>
Table 2. BCU DIP-Switch S1 Options (Continued)

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1-2</td>
<td>Line Code</td>
<td>Enables Bipolar Eight-Zero Substitution (B8ZS), which allows for Clear Channel operation for the T1 carrier system, or enables Alternate Mark Inversion (AMI). This option must be configured identically with all other T1 network equipment on this circuit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ON</strong>* AMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OFF</strong> B8ZS</td>
</tr>
<tr>
<td>S1-3</td>
<td>TR-08 Signaling</td>
<td>Enables or disables the TR-08 signaling option. When enabled, S1-1 is ignored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ON</strong>* Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OFF</strong> Disabled</td>
</tr>
<tr>
<td>S1-4</td>
<td>CSU Loopback</td>
<td>Enables the CSU loopback function. When this switch is enabled, the Total Access 850 will respond to CSU loopbacks sent from a remote network device or test equipment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ON</strong> Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OFF</strong>* Enabled</td>
</tr>
<tr>
<td>S1-5</td>
<td>Timing Mode A</td>
<td>Determines the clock source options for the Total Access 850 system.</td>
</tr>
<tr>
<td>S1-6</td>
<td>Timing Mode B</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>S1-5/S1-6</strong> Function</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OFF/OFF</strong> Loop timing: Derives timing from the network T1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ON/OFF</strong> External Timing: Derives timing from the external bits clock.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OFF/ON</strong> Local Timing: Clock generated from internal timing source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em><em>ON</em>/ON</em> Loop Timing: Derives timing from the network T1.</td>
</tr>
<tr>
<td>S1-7</td>
<td>Line Build Out A</td>
<td>Sets the attenuation properties to configure the receiver sensitivity in decibels (dB).</td>
</tr>
<tr>
<td>S1-8</td>
<td>Line Build Out B</td>
<td>Additional settings can be provisioned through the terminal menu interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>S1-7/S1-8</strong> Setting</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OFF/OFF</strong> 0 dB/0-133 ft</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ON/OFF</strong> -7.5 dB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OFF/ON</strong> -15 dB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em><em>ON</em>/ON</em> -22 dB</td>
</tr>
</tbody>
</table>

* Denotes factory default settings.
**Faceplate Bantam Jack**

The faceplate bantam jack provides a means to monitor the network T1 connected to the rear of the Total Access 850 chassis. The jacks accept standard 310-type bantam plugs. Figure 2 display the bantam jack monitoring points.

![Figure 2. BCU Bantam Jack Test Diagram](image)

**Faceplate TEST Connector**

The faceplate TEST connector provides the necessary clock output required by standard DS0 Logic Test equipment (such as a TPI 108/109 test set). Specifically, the Test connector outputs 8 kHz and 64 kHz clock reference signal. DS0 test equipment is used to test DS0 access modules such as the OCU DP, DS0 DP, or UBRITE. Once the test equipment is connected to the reference clock source, individual tests can be performed on DS0 access modules using the faceplate bantam jacks on each unit. Figure 3 on page 28 illustrates the DB-9 TEST connector.

![Figure 3. BCU DB-9 Test Connector](image)

**T1 Router Controller Unit (4200376L1#TDM and 4200376L1#ATM)**

The following is operational information pertaining to the T1 Router Controller Unit when used with the Total Access 850 system.
**Faceplate CRAFT Interface**

Use the CRAFT port located on the RCU faceplate to configure the system via an EIA-232 connection. Table 3 displays the CRAFT port pinout.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 4, 6-9</td>
<td>UNUSED</td>
<td><em>—</em></td>
</tr>
<tr>
<td>2</td>
<td>RD</td>
<td>Receive Data (Output)</td>
</tr>
<tr>
<td>3</td>
<td>TD</td>
<td>Transmit Data (Input)</td>
</tr>
<tr>
<td>5</td>
<td>SG</td>
<td>Signal Ground</td>
</tr>
</tbody>
</table>

**Table 3. T1 RCU CRAFT (DB-9, Female) Pinout**

**Faceplate LEDs**

The faceplate LEDs provide status information using a color coded message format. Table 4 gives a description of all faceplate LEDs for the T1 RCU when used with the Total Access 850 system.

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>OFF</td>
<td>there is no power to the system.</td>
</tr>
<tr>
<td></td>
<td>Solid GREEN</td>
<td>the system is connected to an active power source.</td>
</tr>
<tr>
<td>T1 ALARM</td>
<td>OFF</td>
<td>there are no active T1 alarms on the system.</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>there is an active T1 alarm (yellow, red, or blue alarm) on the system.</td>
</tr>
<tr>
<td>T1 TEST</td>
<td>AMBER</td>
<td>the network T1 is in test mode (loopback).</td>
</tr>
<tr>
<td>T1 ERROR</td>
<td>Blinking RED</td>
<td>there are errors on the network T1 (framing errors, bipolar violations, or CRC errors).</td>
</tr>
<tr>
<td>V.35 TD</td>
<td>Blinking GREEN</td>
<td>there is transmit data detected on the V.35 port. This LED blinks with data traffic.</td>
</tr>
<tr>
<td>V.35 RD</td>
<td>Blinking GREEN</td>
<td>there is received data detected on the V.35 port. This LED blinks with data traffic.</td>
</tr>
<tr>
<td>ETH LI</td>
<td>OFF</td>
<td>there is no active Ethernet link.</td>
</tr>
<tr>
<td></td>
<td>Solid GREEN</td>
<td>there is a valid Ethernet link on the 10BaseT interface.</td>
</tr>
<tr>
<td>ETH TX/RX</td>
<td>Blinking GREEN</td>
<td>there is received or transmitted data detected on the Ethernet interface. This LED blinks with data traffic.</td>
</tr>
</tbody>
</table>

**Faceplate Bantam Jack**

The faceplate bantam jack provides a means to monitor the network T1 connected to the rear of the Total Access 850 chassis. The jacks accept standard 310-type bantam plugs. Figure 4 displays the bantam jack monitoring points.
Figure 4. RCU Bantam Jack Test Diagram

3rd GEN T1 Router Controller Unit (1203376L1)
The following is operational information pertaining to the 3rd Generation T1 Router Controller Unit when used with the Total Access 850 system.

Faceplate CRAFT Interface
Use the CRAFT port on the RCU faceplate to configure the system via an EIA-232 connection. Table 5 on page 30 displays the CRAFT port pinout.

Table 5. 3rd GEN T1 RCU CRAFT (DB-9, Female) Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 4, 6-9</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>RD</td>
<td>Receive Data (Output)</td>
</tr>
<tr>
<td>3</td>
<td>TD</td>
<td>Transmit Data (Input)</td>
</tr>
<tr>
<td>5</td>
<td>SG</td>
<td>Signal Ground</td>
</tr>
</tbody>
</table>

Faceplate LEDs
The faceplate LEDs provide status information using a color coded message format. Table 6 gives a description of all faceplate LEDs for the T1 RCU when used with the Total Access 850 system.
The faceplate bantam jack provides a means to monitor the network T1 connected to the rear of the Total Access 850 chassis. The jacks accept standard 310-type bantam plugs. Figure 5 display the bantam jack monitoring points.

### Table 6. 3rd GEN T1 RCU Faceplate LEDs

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>GREEN</td>
<td>the network T1 interface is operational.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>the network T1 is in Red Alarm (meaning the T1 is down, not connected, or framing is improperly configured).</td>
</tr>
<tr>
<td></td>
<td>AMBER</td>
<td>the network T1 is in test mode (loopback).</td>
</tr>
<tr>
<td>ETH</td>
<td>GREEN</td>
<td>there is a valid 10 Mbps Ethernet link.</td>
</tr>
<tr>
<td></td>
<td>AMBER</td>
<td>there is a valid 100 Mbps Ethernet link.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>there is no active Ethernet link.</td>
</tr>
</tbody>
</table>

**Faceplate Bantam Jack**

The faceplate bantam jack provides a means to monitor the network T1 connected to the rear of the Total Access 850 chassis. The jacks accept standard 310-type bantam plugs. Figure 5 display the bantam jack monitoring points.

![Figure 5. 3rd GEN RCU Bantam Jack Test Diagram](image-url)
SDSL Router Controller Unit (1200377L1 and 1200377L2)
The following is operational information pertaining to the SDSL Router Controller Unit when used with the Total Access 850 system.

**Faceplate CRAFT Interface**
Use the CRAFT port on the RCU faceplate to configure the system via an EIA-232 connection. Table 7 displays the CRAFT port pinout.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 4, 6-9</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>RD</td>
<td>Receive Data (Output)</td>
</tr>
<tr>
<td>3</td>
<td>TD</td>
<td>Transmit Data (Input)</td>
</tr>
<tr>
<td>5</td>
<td>SG</td>
<td>Signal Ground</td>
</tr>
</tbody>
</table>

**Faceplate LEDs**
The faceplate LEDs provide status information using a color coded message format. Table 8 gives a description of all faceplate LEDs for the SDSL RCU when used with the Total Access 850 system.

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>OFF</td>
<td>there is no power to the system.</td>
</tr>
<tr>
<td></td>
<td>Solid GREEN</td>
<td>the system is connected to an active power source.</td>
</tr>
<tr>
<td>DATA</td>
<td>Blinking GREEN</td>
<td>there is transmit data detected on the network interface.</td>
</tr>
<tr>
<td>NET ALRM</td>
<td>OFF</td>
<td>there are no active network alarms on the system.</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>there is an active network alarm on the system.</td>
</tr>
<tr>
<td>TEST</td>
<td>AMBER</td>
<td>the network interface is in test mode (loopback).</td>
</tr>
<tr>
<td>V.35 TD</td>
<td>Blinking GREEN</td>
<td>there is transmit data detected on the V.35 port. This LED blinks with data traffic.</td>
</tr>
<tr>
<td>V.35 RD</td>
<td>Blinking GREEN</td>
<td>there is received data detected on the V.35 port. This LED blinks with data traffic.</td>
</tr>
<tr>
<td>ETH LI</td>
<td>OFF</td>
<td>there is no active Ethernet link.</td>
</tr>
<tr>
<td></td>
<td>Solid GREEN</td>
<td>there is a valid Ethernet link on the 10BaseT interface.</td>
</tr>
<tr>
<td>ETH TX/RX</td>
<td>Blinking GREEN</td>
<td>there is received or transmitted data detected on the Ethernet interface. This LED blinks with data traffic.</td>
</tr>
</tbody>
</table>
**DIP-Switch Settings**

The Total Access 850 SDSL RCU uses DIP-switches to determine power-up start mode. Table 9 provides details for the DIP-switches.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1-1</td>
<td>Firmware Mode</td>
<td>ON* (down) The unit powers up in the firmware update mode. This mode is not used for normal operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF Disables the firmware update mode.</td>
</tr>
<tr>
<td>S1-2</td>
<td>Factory Defaults</td>
<td>ON* (down) The unit powers up with the factory defaults loaded.</td>
</tr>
</tbody>
</table>

* Denotes factory default settings.

### 4. REVIEWING THE REAR PANEL DESIGN

All connections are made through terminals, jacks, and wire-wraps on the backplane. A removable rear cover provides access to the backplane, and an access panel that mounts to the rear cover allows access to wire-wrap strips P1, P3, and P5, power terminal strip (P7), and clock termination switch (SW1) without removing the main rear cover. Most CPE applications will not require removal of the rear cover.

Before removing the rear cover, do the following:

* For systems using PSU (P/N 1175006L1) – Remove the 20 Hz fuse before exposing backplane or accessing channel unit.
* For systems using PSU (P/N 1175006L2) – Depress the Ring Enable pushbutton to isolate the ring voltage from the Total Access 850.

Figure 6 shows the Total Access 850 backplane, and Table 10 on page 34 gives the backplane connections.

![Figure 6. Total Access 850 Rear Panel](image-url)
### 10/100BaseT Connection (JP1)

Only the 3rd Generation RCUs provide a 10/100BaseT connection. All other available RCU Ethernet interfaces are 10BaseT.

The 10/100BaseT port (RJ-48C) provides a 10/100BaseT Ethernet LAN connection for IP Routing, TFTP, SNMP, and Telnet connections. Table 11 shows the 10/100BaseT pinout.

The 10/100BaseT Ethernet LAN interface may be used for intra-building networks only. This interface should not be connected to public networks.

#### Table 10. Total Access 850 Backplane Connections

<table>
<thead>
<tr>
<th>Ref Des</th>
<th>Device/Label</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>wire-wrap strip</td>
<td>clock/tests</td>
</tr>
<tr>
<td>P2</td>
<td>50 pin amphenol</td>
<td>FXO, FXS, etc.</td>
</tr>
<tr>
<td>P3</td>
<td>wire-wrap strip</td>
<td>alternate T1 interface</td>
</tr>
<tr>
<td>P5</td>
<td>wire-wrap strip</td>
<td>alarms</td>
</tr>
<tr>
<td>P6</td>
<td>4 pin jack</td>
<td>primary -48 V in</td>
</tr>
<tr>
<td>P7</td>
<td>3-lug terminal</td>
<td>alternate -48 V in</td>
</tr>
<tr>
<td>JP1</td>
<td>RJ-48/E-NET</td>
<td>10BaseT Ethernet</td>
</tr>
<tr>
<td>JP2</td>
<td>RJ-48/T1</td>
<td>primary T1 interface</td>
</tr>
<tr>
<td>JP3</td>
<td>RJ-48/FT1</td>
<td>DSX1 interface</td>
</tr>
<tr>
<td>JP4</td>
<td>RJ-48/MAINT</td>
<td>EIA-232 CRAFT interface</td>
</tr>
<tr>
<td>J1</td>
<td>V.35</td>
<td>Nx56K/64K</td>
</tr>
</tbody>
</table>

#### Table 11. Ethernet Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TX1</td>
<td>Transmit Positive</td>
</tr>
<tr>
<td>2</td>
<td>TX2</td>
<td>Transmit Negative</td>
</tr>
<tr>
<td>3</td>
<td>RX1</td>
<td>Receive Positive</td>
</tr>
<tr>
<td>4, 5</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>RX2</td>
<td>Receive Negative</td>
</tr>
<tr>
<td>7, 8</td>
<td>UNUSED</td>
<td>—</td>
</tr>
</tbody>
</table>
T1 Connection (JP2)

The Total Access 850 provides dual T1 connection points. In all cases, only one of the connection points is used. When wire-wrapping of the T1 is utilized (using P3), a blank plug must be placed in the primary T1 connection (JP2). There is a potential of Class A3 T1 Span Power Voltage coming from the network.

The Total Access 850 system provides a single T1 port (located on the rear panel) and complies with the applicable ANSI and AT&T™ standards. The T1 interface provides the following functions:

- AMI or B8ZS
- Manual line build-out
- D4 or ESF framing
- Network performance monitoring and reporting
- Test loopbacks with QRSS generation checking
- Extensive self-testing

The T1 connection pinout is shown in Table 12.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RXDATA-RING</td>
<td>Receive data from the network</td>
</tr>
<tr>
<td>2</td>
<td>RXDATA-TIP</td>
<td>Receive data from the network</td>
</tr>
<tr>
<td>3</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>TXDATA-RING</td>
<td>Transmit data toward the network</td>
</tr>
<tr>
<td>5</td>
<td>TXDATA-TIP</td>
<td>Transmit data toward the network</td>
</tr>
<tr>
<td>6, 7, 8</td>
<td>UNUSED</td>
<td>—</td>
</tr>
</tbody>
</table>

DSX-1 Connection (JP3)

The Total Access 850 system provides a single DSX-1 port (located in the rear of the unit). The DSX-1 interface provides the following functions:

- AMI or B8ZS
- Manual line build-out
- D4 or ESF framing
The DSX-1 interface pinout is shown in Table 13.

### Table 13. DSX-1 Network Connection Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RXDATA-RING</td>
<td>Transmit data from the network.</td>
</tr>
<tr>
<td>2</td>
<td>RXDATA-TIP</td>
<td>Transmit data from the network.</td>
</tr>
<tr>
<td>3</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>RXDATA-RING</td>
<td>Receive data toward the network.</td>
</tr>
<tr>
<td>5</td>
<td>RXDATA-TIP</td>
<td>Receive data toward the network.</td>
</tr>
<tr>
<td>6, 7, 8</td>
<td>UNUSED</td>
<td>—</td>
</tr>
</tbody>
</table>

**Rear CRAFT Port (JP4)**

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

- Accepts EIA-232 input from a PC or a modem for controlling the Total Access 850.
- Baud rate is user-configurable.
- Acts as input for either VT100 or PC control.
- Acts as an interface for flash memory software downloads using XMODEM.

Table 14 shows the rear CRAFT port pinout.

### Table 14. Rear CRAFT Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GND</td>
<td>Ground - connected to unit chassis</td>
</tr>
<tr>
<td>2</td>
<td>RTS</td>
<td>Request to send - flow control</td>
</tr>
<tr>
<td>3</td>
<td>RXDATA</td>
<td>Data received by the Total Access 850</td>
</tr>
<tr>
<td>4</td>
<td>DTR</td>
<td>Data terminal ready</td>
</tr>
<tr>
<td>5</td>
<td>TXDATA</td>
<td>Data transmitted by the Total Access 850</td>
</tr>
<tr>
<td>6</td>
<td>CD</td>
<td>Carrier detect</td>
</tr>
<tr>
<td>7</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>CTS</td>
<td>Clear to send - flow control</td>
</tr>
</tbody>
</table>
Nx56k/64k Port (J1)

The Total Access 850 system provides a single V.35 Winchester-style connection on the rear of the chassis (as defined in Table 15).

Table 15. V.35 Winchester Pinout

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

Alarm Relay Connection (P5)

This connection alerts the user when a selected alarm condition exists. Alarm relay contacts are open during normal operation. The alarm relay contacts close in the event of a local alarm condition or the receipt of an alarm from the T1 carrier. In a carrier alarm condition such as a Red, Yellow, or Blue (unframed all 1s), various alarm contacts in the PSU close. Carrier alarm conditions cause the Total Access 850 to initiate trunk processing. The following chain of events then occur:

1. MJ will be directly shorted to MJR.
2. MJV will be directly shorted to MJVR.

Contacts MJ and MJR can be overridden manually during an alarm condition by pressing the ACO pushbutton on the PSU faceplate. If the 3-Amp power fuse on the PSU trips, the -48ALM relay will close, providing a -48 VDC signal on that pin. This alarm cannot be overridden by the ACO pushbutton. Refer to Table 17 for alarm notifications.

Table 16 shows the pinout for the Alarm Relay connector.

Table 16. Alarm Relay Connector Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-48 ALM</td>
<td>DC alarm output.</td>
</tr>
<tr>
<td>2</td>
<td>MJVR</td>
<td>Closes when a selected alarm condition is present.</td>
</tr>
<tr>
<td>3</td>
<td>MJV</td>
<td>Common connection between external circuitry and NC or NO terminal.</td>
</tr>
<tr>
<td>4</td>
<td>MJR</td>
<td>Major alarm audible common</td>
</tr>
<tr>
<td>5</td>
<td>MJ</td>
<td>Major alarm audible</td>
</tr>
</tbody>
</table>
### Table 17. Alarm Notification

<table>
<thead>
<tr>
<th>Alarm Condition</th>
<th>Relays Activated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MJR</td>
</tr>
<tr>
<td>Red Alarm</td>
<td>X</td>
</tr>
<tr>
<td>Yellow Alarm</td>
<td>X</td>
</tr>
<tr>
<td>AIS Alarm</td>
<td>X</td>
</tr>
<tr>
<td>PSU Power Fuse Fails</td>
<td>X</td>
</tr>
<tr>
<td>Alarms ACO Deactivates</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note:** ACO will not deactivate MJR after a power fuse failure.

### Clock Wire-Wrap Strip (P1)

A single wire-wrap strip is provided on the Total Access 850 backplane for connection to an external bits clock. The external bits clock may be used to provide master timing for the Total Access 850 system.

### Customer Connection (P2)

One 50-pin female amphenol connector (P2) provides the interconnect wiring for the access modules located in slots 1 through 6 of the chassis. This connector is usually terminated with a punch-down block for premises wiring or connected directly to a cross-connect or main distribution frame. Figure 7 details the connector pinout.

![Figure 7. Connector Pinout](image-url)
T1 Wire-Wrap Connection (P3)

**WARNING**  
Network T1 connections can have up to 140 VDC. Use caution when making T1 connections.

There are two termination points for connecting the network T1 to the chassis: the primary RJ-48 connector (JP2) and the alternate wire-wrap pins on terminal strip P3 (see Figure 6 on page 33). Only one connector type is used (not both). The T1 primary connection is via the RJ-48 connector labeled T1 (JP2). This arrangement provides a convenient T1 connection for those installations where a T1 Smart Jack is used. Table 18 on page 39 shows the pinout for the T1 wire-wrap connector.

**WARNING**  
The Total Access 850 provides dual T1 connection points. In all cases, only one of the connection points is used. When wire-wrapping of the T1 is utilized (using P3), a blank plug must be placed in the primary T1 connection (JP2). There is a potential of Class A3 T1 Span Power Voltage coming from the network.

Table 18. T1 Wire-Wrap Connector Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>R1</td>
<td>DS1 Ring input from network</td>
</tr>
<tr>
<td>2</td>
<td>T1</td>
<td>DS1 Tip input from network</td>
</tr>
<tr>
<td>3</td>
<td>R</td>
<td>DS1 Ring output from network</td>
</tr>
<tr>
<td>4</td>
<td>T</td>
<td>DS1 Tip output from network</td>
</tr>
<tr>
<td>5</td>
<td>Gnd</td>
<td>Ground</td>
</tr>
</tbody>
</table>

Power Connections (P6 and P7)

There are two power connections on the backplane: a modular DC plug (P6), and a three-lug terminal strip (P7) (refer to Figure 8 on page 40). The primary connection is the modular plug, which receives -48 VDC from an approved ADTRAN power supply/battery charging unit (for example, P/N 1175043L2). The alternate connection is screw terminal P7, which can be used if -48 VDC is available as in central office applications. The screw terminal connection is shown in Figure 8 on page 40.

**CAUTION**  
During installation, power should be the last connection made after all other wire-wrap connections are completed.
5. ACCESS MODULE INTERFACES

Power Supply Unit (P/N 1175006L2)

The PSU receives externally supplied -48 VDC from connectors P4 (normal) and P5 (alternate) on the rear of the unit. Connector P4 connects from an approved ADTRAN Power Supply and Battery Charger unit. P5 is a 3-lug terminal strip that receives -48 VDC from the customer-supplied office power. Through switchmode operation, the PSU converts the incoming -48 VDC to regulated +5 VDC, +3.3 VDC, -7.5 VDC, -26 VDC, and -48 VDC for distribution to other modules. Ring voltage circuitry within the PSU generates 105 Vrms, 20 Hz ring voltage for distribution to the system’s FXS cards. Ring voltage is disabled by pushing the RING ENABLE button.

Faceplate LEDs

The faceplate LEDs provide status information using a color coded message format. Table 20 gives a description of all faceplate LEDs for the Quad FXS Module when used with the Total Access 850 system.
Quad FXS Access Module (P/N 1175408L2)
The Quad FXS Access Modules use the 50-pin female amphenol connector on the rear of the Total Access 850 chassis to provide the interconnect wiring for the four analog circuits on each access module.

**Faceplate LEDs**
The faceplate LEDs provide status information using a color coded message format. Table 20 gives a description of all faceplate LEDs for the Quad FXS Module when used with the Total Access 850 system.

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BUSY</strong></td>
<td>OFF</td>
<td>the interface is currently on-hook and not in use.</td>
</tr>
<tr>
<td></td>
<td>Solid GREEN</td>
<td>the interface is currently off-hook (busy).</td>
</tr>
<tr>
<td></td>
<td>Blinking GREEN</td>
<td>the interface is ringing.</td>
</tr>
<tr>
<td></td>
<td>Sequencing 1-4</td>
<td>the assigned network T1 time slot is unavailable for use by the module.</td>
</tr>
</tbody>
</table>

**Table 19. PSU Faceplate LEDs**

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POWER</strong></td>
<td>OFF</td>
<td>the system is disconnected from the power source or powered off.</td>
</tr>
<tr>
<td></td>
<td>GREEN</td>
<td>the system is connected to a power source and is powered on.</td>
</tr>
<tr>
<td><strong>RING</strong></td>
<td>OFF</td>
<td>ring generation is disabled for the system.</td>
</tr>
<tr>
<td></td>
<td>GREEN</td>
<td>ring generation is enabled for the system.</td>
</tr>
<tr>
<td><strong>BANK ALM</strong></td>
<td>OFF</td>
<td>the system is in normal operation.</td>
</tr>
<tr>
<td></td>
<td>Solid RED</td>
<td>there is currently an active alarm condition.</td>
</tr>
<tr>
<td></td>
<td>Blinking RED</td>
<td>there was an alarm condition, but it was acknowledged by pressing the ACO pushbutton (located on the PSU faceplate).</td>
</tr>
</tbody>
</table>
**Interface Pinout**

Figure 9 shows the pinout connection for the amphenol connector. See Figure 7 on page 38 for closer detail.

![Pinout Diagram]

**Specifications**

Table 21 provides the detailed specifications for the Total Access 850 Quad FXS Module.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td>6 W (off-hook)</td>
</tr>
<tr>
<td><strong>Loop Current</strong></td>
<td>23 mA (nominal)</td>
</tr>
<tr>
<td></td>
<td>20 mA (minimum)</td>
</tr>
<tr>
<td><strong>Loop Resistance</strong></td>
<td>1200 Ω (nominal)</td>
</tr>
<tr>
<td></td>
<td>1650 Ω (maximum) – 900 Ω/1350 Ω (line), 300 Ω (phone)</td>
</tr>
<tr>
<td><strong>Terminating Impedance</strong></td>
<td>900 Ω + 2.16 μF</td>
</tr>
<tr>
<td></td>
<td>600 Ω + 2.16 μF</td>
</tr>
<tr>
<td></td>
<td>900 Ω</td>
</tr>
<tr>
<td></td>
<td>600 Ω</td>
</tr>
<tr>
<td><strong>Return Loss</strong></td>
<td>900 Ω + 2.16 μF</td>
</tr>
<tr>
<td></td>
<td>ERL &gt; 28 dB</td>
</tr>
<tr>
<td></td>
<td>SRL &gt; 20 dB</td>
</tr>
<tr>
<td><strong>Trans Hybrid Loss</strong></td>
<td>900 Ω + 2.16 μF</td>
</tr>
<tr>
<td></td>
<td>ERL &gt; 28 dB</td>
</tr>
<tr>
<td></td>
<td>SRL &gt; 20 dB</td>
</tr>
<tr>
<td><strong>Longitudinal Balance</strong></td>
<td>200, 500, and 1000 Hz: &gt; 58 dB min, &gt; 63 dB avg</td>
</tr>
<tr>
<td></td>
<td>3000 Hz: &gt; 53 dB min, &gt; 58 dB avg</td>
</tr>
<tr>
<td><strong>Frequency Response</strong></td>
<td>300 to 3400 Hz: -0.5 dB and 1.0 dB</td>
</tr>
<tr>
<td><strong>Idle Channel Noise</strong></td>
<td>&lt; 20 dBmC</td>
</tr>
</tbody>
</table>
Table 22. Quad FXS Module Compliance Codes

<table>
<thead>
<tr>
<th>CODE</th>
<th>IN</th>
<th>OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Code (PC)</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Telecommunication Code (TC)</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>Installation Code</td>
<td>A</td>
<td>–</td>
</tr>
</tbody>
</table>

Quad FXO Access Module (P/N 1175407L1)

The Quad FXO Access Modules use the 50-pin female amphenol connector on the rear of the Total Access 850 chassis to provide the interconnect wiring for the four analog circuits on each access module.

Faceplate LEDs

The faceplate LEDs provide status information using a color coded message format. Table 23 gives a description of all faceplate LEDs for the Quad FXO Module when used with the Total Access 850 system.

Table 23. Quad FXO Module Faceplate LEDs

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUSY</td>
<td>OFF</td>
<td>the interface is currently on-hook and not in use.</td>
</tr>
<tr>
<td></td>
<td>GREEN</td>
<td>the interface is currently off-hook (busy).</td>
</tr>
<tr>
<td></td>
<td>Blinking GREEN</td>
<td>the interface is ringing.</td>
</tr>
<tr>
<td></td>
<td>Sequencing 1–4</td>
<td>the assigned network T1 time slot is unavailable for use by the module.</td>
</tr>
</tbody>
</table>
**Interface Pinout**

Figure 10 shows the pinout connection for the amphenol connector. See Figure 7 on page 38 for closer detail.

![Quad FXO Connector Pin Assignments](image)

**Specifications**

Table 24 provides the detailed specifications for the Total Access 850 Quad FXO Module.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>2 W (off-hook)</td>
</tr>
<tr>
<td>Terminating Impedance</td>
<td>900 Ω + 2.16 µF</td>
</tr>
<tr>
<td>Return Loss</td>
<td>900 Ω + 2.16 µF</td>
</tr>
<tr>
<td></td>
<td>ERL &gt; 28 dB</td>
</tr>
<tr>
<td></td>
<td>SRL &gt; 20 dB</td>
</tr>
<tr>
<td>Trans Hybrid Loss</td>
<td>900 Ω + 2.16 µF</td>
</tr>
<tr>
<td></td>
<td>ERL &gt; 28 dB</td>
</tr>
<tr>
<td></td>
<td>SRL &gt; 20 dB</td>
</tr>
<tr>
<td>Longitudinal Balance</td>
<td>200, 500, and 1000 Hz: &gt; 58 dB min, &gt; 63 dB avg</td>
</tr>
<tr>
<td></td>
<td>3000 Hz: &gt; 53 dB min, &gt; 58 dB avg</td>
</tr>
<tr>
<td>Frequency Response</td>
<td>300 to 3400 Hz: -0.5 dB and 1.0 dB</td>
</tr>
<tr>
<td>Idle Channel Noise</td>
<td>&lt; 20 dBmC</td>
</tr>
<tr>
<td>Signal to Distortion Ratio</td>
<td>0 to -30 dBm0: &gt; 33 dB</td>
</tr>
<tr>
<td></td>
<td>-30 to -40 dBm0: &gt; 27 dB</td>
</tr>
<tr>
<td></td>
<td>-40 to -45 dBm0: &gt; 22 dB</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>Up to 95% noncondensing</td>
</tr>
<tr>
<td>Temperature</td>
<td>Operate at -40 °C to +65 °C</td>
</tr>
<tr>
<td></td>
<td>Store at -40 °C to +70 °C</td>
</tr>
<tr>
<td>Tests</td>
<td>Self-test, digital loopback, network on-hook/off-hook, customer ring, and 100 Hz tone generation</td>
</tr>
</tbody>
</table>
**Compliance Codes**
Table 25 provides the compliance codes for the Total Access 850 Quad FXO Module.

<table>
<thead>
<tr>
<th>Code</th>
<th>IN</th>
<th>OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Code (PC)</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Telecommunication Code (TC)</td>
<td>–</td>
<td>X</td>
</tr>
</tbody>
</table>

**UBR1TE Access Module (P/N 1180020L1)**
Each port of the UBR1TE Access Module provides an ISDN U-interface and allows the transport of Basic Rate 2B+D information over the T1 carrier and twisted pair wiring.

**Faceplate LEDs**
The faceplate LEDs provide status information using a color coded message format. Table 26 gives a description of all faceplate LEDs for the UBR1TE Module when used with the Total Access 850 system.

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATUS</td>
<td>OFF</td>
<td>both the loop and the carrier synchronization are established.</td>
</tr>
<tr>
<td></td>
<td>Solid RED</td>
<td>neither the loop nor the carrier synchronization is established.</td>
</tr>
<tr>
<td></td>
<td>Blinking RED (every two seconds)</td>
<td>loop synchronization is established, but carrier synchronization is not.</td>
</tr>
<tr>
<td></td>
<td>Blinking RED (twice every second)</td>
<td>carrier synchronization is established, but loop synchronization is not.</td>
</tr>
<tr>
<td>GREEN</td>
<td>Layer 1 is established from the ISDN switch to the customer ISDN terminal equipment.</td>
<td></td>
</tr>
<tr>
<td>Solid AMBER</td>
<td>front panel test in progress or the unit is responding to a 2B + D loopback request.</td>
<td></td>
</tr>
<tr>
<td>Blinking AMBER (every two seconds)</td>
<td>the unit is responding to a B1 loopback request or has been forced into a B1 loopback from the terminal menus.</td>
<td></td>
</tr>
<tr>
<td>Blinking AMBER (twice every second)</td>
<td>the unit is responding to a B2 loopback request or has been forced into a B2 loopback from the terminal menus.</td>
<td></td>
</tr>
<tr>
<td>REM (Remote)</td>
<td>GREEN</td>
<td>the unit has been provisioned by the BCU/RCU.</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>the unit is provisioned by DIP-switches.</td>
</tr>
</tbody>
</table>
Interface Pinout
Table 27 provides the interface pinout for the UBR1TE interface slot/amphenol connector assignment.

<table>
<thead>
<tr>
<th>Total Access 850 Slot</th>
<th>Port 1 T/R</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>26/1</td>
</tr>
<tr>
<td>2</td>
<td>30/5</td>
</tr>
<tr>
<td>3</td>
<td>34/9</td>
</tr>
<tr>
<td>4</td>
<td>38/13</td>
</tr>
<tr>
<td>5</td>
<td>42/17</td>
</tr>
<tr>
<td>6</td>
<td>46/21</td>
</tr>
</tbody>
</table>

DIP-Switch Settings
The Total Access 850 UBR1TE Module can be provisioned from either the DIP-switches (S1) mounted on the PCB, or through screen menus accessed via the faceplate CRAFT interface port. Table 28 provides the DIP-switch setting details.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1-1</td>
<td>MODE</td>
<td>Sets the termination mode as LULT (RT Typical) or LUNT (COT Typical).</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>Unit is installed as Adjacent-to-U-Repeater, Adjacent-to-Customer, or Tandem Office Source configuration.</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>Unit is installed as Adjacent-to-Switch or Tandem Office Sink configuration.</td>
</tr>
</tbody>
</table>
Table 28. BCU DIP-Switch S1 Options  *(Continued)*

<table>
<thead>
<tr>
<th>Switch</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1-2</td>
<td>Tandem Office Installation</td>
<td>Indicates whether the unit is installed in a Tandem Office installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ON</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
</tr>
<tr>
<td>S1-3</td>
<td>Service for: S1-3: B1 S1-4: B2 S1-5: D</td>
<td>Selects the service level to option the U-BR1TE module to deliver full ISDN (2B+D) or any of the following levels:</td>
</tr>
<tr>
<td>S1-4</td>
<td></td>
<td>Service Level</td>
</tr>
<tr>
<td>S1-5</td>
<td></td>
<td>2B+D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B1+D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B2+D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td>S1-6</td>
<td>Zero Byte Substitution</td>
<td>Sets the Zero Byte Substitution parameter. The ZBS option must be set the same for the COT and RT. Check local provisioning guidelines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ON</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF*</td>
</tr>
</tbody>
</table>
Specifications
Table 29 provides the detailed specifications for the Total Access 850 UBR1TE Module.

Table 29. UBR1TE Module Specifications

<table>
<thead>
<tr>
<th>Loop Interface (ANSI T1.601)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line</strong></td>
</tr>
<tr>
<td>2-wire (tip and ring)</td>
</tr>
<tr>
<td><strong>Operating Mode</strong></td>
</tr>
<tr>
<td>full duplex</td>
</tr>
<tr>
<td><strong>Data Rate</strong></td>
</tr>
<tr>
<td>160 kbps total; 144 kbps available to customer</td>
</tr>
<tr>
<td><strong>Signal Format</strong></td>
</tr>
<tr>
<td>2B1Q</td>
</tr>
<tr>
<td><strong>Transmit Power</strong></td>
</tr>
<tr>
<td>13 dBm to 14 dBm nominal</td>
</tr>
</tbody>
</table>

| DS1 Facility Interface      |
| BR1/10 compatible equipment.|

<table>
<thead>
<tr>
<th>Network Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
</tr>
<tr>
<td>ISDN and other digital service, according to TR-NWT-000397</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mechanical</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dimensions</strong></td>
</tr>
<tr>
<td>3.125” H x 0.62” W, 1.01” D</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
</tr>
<tr>
<td>&lt; 1 lb</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Power</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current Draw</strong></td>
</tr>
<tr>
<td>0.023 A maximum (@ -48V)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Environmental</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Temperature</strong></td>
</tr>
<tr>
<td>Operating: -40 °C to +70 °C</td>
</tr>
<tr>
<td><strong>Relative Humidity</strong></td>
</tr>
<tr>
<td>Up to 95% noncondensing</td>
</tr>
<tr>
<td><strong>Heat Dissipation</strong></td>
</tr>
<tr>
<td>1.10 W (maximum)</td>
</tr>
</tbody>
</table>

Compliance Codes
Table 30 provides the compliance codes for the Total Access 850 UBR1TE Module.

Table 30. UBR1TE Module Compliance Codes

<table>
<thead>
<tr>
<th>CODE</th>
<th>IN</th>
<th>OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Code (PC)</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Telecommunication Code (TC)</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>Installation Code</td>
<td>A</td>
<td>–</td>
</tr>
</tbody>
</table>
OCU DP Access Module (P/N 1180005L1)

The OCU DP Access Module may be used for intra-building networks only. This interface should not be connected to public networks.

The OCU DP module is a single port access module used to provide the interface between a DS0 time slot on the T1 and a 4-wire DDS device at the customer premises. The OCU DP supports up to 18 kft of copper for remote DSU connectivity. This module is currently only supported by BCU L1 and L2. Table 31 gives this pinout.

<table>
<thead>
<tr>
<th>Total Access 850 Slot</th>
<th>T/R RX</th>
<th>T1/R1 TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>26/1</td>
<td>27/2</td>
</tr>
<tr>
<td>2</td>
<td>30/5</td>
<td>31/6</td>
</tr>
<tr>
<td>3</td>
<td>34/9</td>
<td>35/10</td>
</tr>
<tr>
<td>4</td>
<td>38/13</td>
<td>39/14</td>
</tr>
<tr>
<td>5</td>
<td>42/17</td>
<td>43/18</td>
</tr>
<tr>
<td>6</td>
<td>46/21</td>
<td>47/22</td>
</tr>
</tbody>
</table>

E&M/TO Access Module (P/N 1180402L1)

The E&M/TO Access Module may be used for intra-building networks only. This interface should not be connected to public networks.

The E&M/TO module is a single port Ear and Mouth/Transmit Only access module. The primary application for this module is to provide PBX foreign exchange at the customer premises or tandem central office applications. The E&M/TO module supports both 2- and 4-wire operation. This module is currently only supported by BCU L1 and L2. Table 32 gives the E&M/TO module pinout.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Slot 1</th>
<th>Slot 2</th>
<th>Slot 3</th>
<th>Slot 4</th>
<th>Slot 5</th>
<th>Slot 6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>17</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
<td>18</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>15</td>
<td>19</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td>24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pin</th>
<th>Slot 1</th>
<th>Slot 2</th>
<th>Slot 3</th>
<th>Slot 4</th>
<th>Slot 5</th>
<th>Slot 6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>26</td>
<td>30</td>
<td>34</td>
<td>38</td>
<td>42</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>31</td>
<td>35</td>
<td>39</td>
<td>43</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>32</td>
<td>36</td>
<td>40</td>
<td>44</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>33</td>
<td>37</td>
<td>41</td>
<td>45</td>
<td>49</td>
</tr>
</tbody>
</table>
Dual V.35 Access Module (P/N 1180025L1)

The Dual V.35 module provides additional V.35 interfaces for customer premises equipment. The module takes up two access slots; therefore three modules (six additional ports) can be added to an empty chassis. The Total Access 850 can support a maximum of seven V.35 interfaces. V.35 ports provided by the Dual V.35 module are accessed on the front of the Total Access 850. This module is currently only supported by the TDM version of the T1 RCU. An ADTRAN 35 ft DB-26/V.35 adapter cable is required (P/N 1200167L1).

**Faceplate LEDs**

The faceplate LEDs provide status information using a color coded message format. Table 33 gives a description of all faceplate LEDs for the Dual V.35 Module when used with the Total Access 850 system.

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>GREEN</td>
<td>the module is operating normally.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>there is a card failure, or the T1 is down, or there is no valid data transfer occurring.</td>
</tr>
<tr>
<td></td>
<td>AMBER</td>
<td>there is a test in progress.</td>
</tr>
<tr>
<td></td>
<td>Blinking AMBER</td>
<td>no DS0s have been assigned to the interface.</td>
</tr>
<tr>
<td><strong>TD</strong></td>
<td>GREEN</td>
<td>the module is transmitting data to the network interface.</td>
</tr>
<tr>
<td><strong>RD</strong></td>
<td>GREEN</td>
<td>the module is receiving data from the network and transmitting it out the V.35 interface (to the DTE equipment).</td>
</tr>
</tbody>
</table>

**Interface Pinouts**

Table 34 provides the interface pinout for the DB-26 and V.35 interfaces.

<table>
<thead>
<tr>
<th>Pin (DB-26)</th>
<th>Pin (V.35)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A</td>
<td>Frame ground</td>
</tr>
<tr>
<td>2,3</td>
<td>–</td>
<td>Unused</td>
</tr>
<tr>
<td>4</td>
<td>C</td>
<td>Request to send (RTS)</td>
</tr>
<tr>
<td>5</td>
<td>D</td>
<td>Clear to send (CTS)</td>
</tr>
<tr>
<td>6</td>
<td>E</td>
<td>Data set ready (DSR)</td>
</tr>
<tr>
<td>7</td>
<td>B</td>
<td>Signal ground</td>
</tr>
<tr>
<td>8</td>
<td>F</td>
<td>Carrier detect (CD)</td>
</tr>
<tr>
<td>9</td>
<td>P</td>
<td>Transmitted data (TD-A) from DTE</td>
</tr>
<tr>
<td>10</td>
<td>S</td>
<td>Transmitted data (TD-B) to DTE</td>
</tr>
<tr>
<td>11</td>
<td>R</td>
<td>Received data (RD-A) to DTE</td>
</tr>
</tbody>
</table>
Table 34. Dual V.35 Interface Pinout (DB-26 to V.35) (Continued)

<table>
<thead>
<tr>
<th>12</th>
<th>T</th>
<th>Received data (RD-B) to DTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>U</td>
<td>External TX clock (ETC-A) from DTE</td>
</tr>
<tr>
<td>14-16</td>
<td>–</td>
<td>Unused</td>
</tr>
<tr>
<td>17</td>
<td>J</td>
<td>Ring indicator (RI)</td>
</tr>
<tr>
<td>18</td>
<td>L</td>
<td>LL</td>
</tr>
<tr>
<td>19</td>
<td>NN</td>
<td>Test mode (TM) to DTE</td>
</tr>
<tr>
<td>20</td>
<td>H</td>
<td>Data terminal ready (DTR) from DTE</td>
</tr>
<tr>
<td>21</td>
<td>–</td>
<td>Unused</td>
</tr>
<tr>
<td>22</td>
<td>Y</td>
<td>TX clock (TC-A) to DTE</td>
</tr>
<tr>
<td>23</td>
<td>AA</td>
<td>TX clock (TC-B) to DTE</td>
</tr>
<tr>
<td>24</td>
<td>V</td>
<td>RX clock (RC-A) to DTE</td>
</tr>
<tr>
<td>25</td>
<td>X</td>
<td>RX clock (RC-B) to DTE</td>
</tr>
<tr>
<td>26</td>
<td>W</td>
<td>External TX clock (ETC-B) from DTE</td>
</tr>
</tbody>
</table>

Specifications

Table 35 provides the detailed specifications for the Total Access 850 Dual V.35 Module.

Table 35. Dual V.35 Module Specifications

<table>
<thead>
<tr>
<th>Data Rates</th>
<th>56 kbps to 1.536 Mbps (per interface)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative Humidity</td>
<td>Up to 95% noncondensing</td>
</tr>
<tr>
<td>Cable Assembly</td>
<td>DB-26 to V.35 P/N 1200167L1</td>
</tr>
</tbody>
</table>
| Temperature | Operate at -40 °C to +65 °C  
Store at -40 °C to +85 °C |
| Tests | Self-test, DTE loopback, Network Loopback, 511 Pattern generation |
| Electrical | Voltage | Current |
| | -42 to -56 VDC | 0 mA |
| | +3.3 VDC ± 10% | 20 mA |
| | +5.0 VDC ± 5% | 160 mA |
| | -7.5 VDC ± 10% | 50 mA |
| | -24 to -30 VDC | 0 mA |
| Dimensions | 3 3/16” W x 1 5/16” H x 10 1/8” D |
| Weight | 4.8 ounces |
**Compliance Codes**

Table 36 provides the compliance codes for the Total Access 850 Dual V.35 Module.

<table>
<thead>
<tr>
<th>CODE</th>
<th>IN</th>
<th>OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Code (PC)</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Telecommunication Code (TC)</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Installation Code</td>
<td>A</td>
<td>–</td>
</tr>
</tbody>
</table>

**DSX-1 Access Module (P/N 1200385L1)**

> The DSX-1 interface provided on the DSX-1 Access Module may be used for intra-building networks only. This interface should not be connected to public networks.

The DSX-1 Module is a single port (RJ-45) access module that provides a DSX-1 connection for customer premises equipment. This module supports PBXs or other equipment with a DSX-1/FT1 interface. This module is currently supported by the T1 RCU only.

> Robbed-Bit Signaling is only passed to the DSX-1 Module from the 3rd Generation RCUs. Older RCUs do not have this capability.

**Faceplate LEDs**

The faceplate LEDs provide status information using a color coded message format. Table 37 on page 53 gives a description of all faceplate LEDs for the DSX-1 Module when used with the Total Access 850 system.
Table 37. DSX-1 Module Faceplate LEDs

<table>
<thead>
<tr>
<th>For these LEDs...</th>
<th>This color light...</th>
<th>Indicates that...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>OFF</td>
<td>there is no power to the system.</td>
</tr>
<tr>
<td></td>
<td>GREEN</td>
<td>the DSX-1 signal is present and synchronized; the channel is configured for use.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>there is a present channel alarm on the T1 interface.</td>
</tr>
<tr>
<td></td>
<td>Solid AMBER</td>
<td>there is a channel test in progress.</td>
</tr>
<tr>
<td></td>
<td>Blinking AMBER</td>
<td>the card is initializing (during startup).</td>
</tr>
</tbody>
</table>

**Interface Pinout**

Table 38 provides the interface pinout for the provided RJ-45 DSX-1 interface.

Table 38. DSX-1 Module Interface Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>R1</td>
<td>RXDATA-RING</td>
</tr>
<tr>
<td>2</td>
<td>T1</td>
<td>RXDATA-TIP</td>
</tr>
<tr>
<td>3</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>R</td>
<td>TXDATA-RING</td>
</tr>
<tr>
<td>5</td>
<td>T</td>
<td>TXDATA-TIP</td>
</tr>
<tr>
<td>6,7,8</td>
<td>UNUSED</td>
<td>—</td>
</tr>
</tbody>
</table>

**Specifications**

Table 39 provides the detailed specifications for the Total Access 850 DSX-1 Module.

Table 39. DSX-1 Module Specifications

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity</td>
<td>T1: 1 to 24 DS0s</td>
</tr>
<tr>
<td>Framing</td>
<td>ESF and SF(D4)</td>
</tr>
<tr>
<td>Line Build Out</td>
<td>DSX-1: 0 to 655 feet in 133-foot increments</td>
</tr>
<tr>
<td>Line Coding</td>
<td>AMI (alternate mark inversion) or B8ZS (bipolar 8 zero substitution)</td>
</tr>
<tr>
<td>Line Rate</td>
<td>1.544 Mbps, ± 75 bps</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>Up to 95% noncondensing</td>
</tr>
<tr>
<td>Terminating Impedance</td>
<td>100 ohms ± 5%</td>
</tr>
<tr>
<td>Temperature</td>
<td>Operate at -0 °C to +50 °C Store at -40 °C to +70 °C</td>
</tr>
<tr>
<td>Tests</td>
<td>Self-test, local line, local payload, remote line, and remote payload</td>
</tr>
</tbody>
</table>
NETWORK TURNUP PROCEDURE

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

CONTENTS

Tools Required ................................................................. 56
Unpack and Inspect the SYSTEM ........................................... 56
  Contents of ADTRAN Shipments ........................................ 57
Telecommunications Codes .................................................. 57
Grounding Instructions ....................................................... 57
Supplying Power to the Unit ............................................... 58
  AC Powered Systems ..................................................... 58
  DC Powered Systems ..................................................... 59
  Making Alternate Power Connections .................................. 59
Mounting Options ............................................................. 60
  Required Clearances ..................................................... 60
  Wallmounting the Chassis ................................................ 60
Installing Modules ............................................................ 61
  Instructions for Installing the Power Supply Unit (P/N 1175006L2) .......................................................... 61
  Instructions for Installing the Total Access 850 Controller and Access Modules ............................................ 62
Module Shipping Contents .................................................... 62
  Quad FXO Access Module (P/N 1175407L2) .............................. 62
  Quad FXS Access Module (P/N 1175408L2) .............................. 62
  UBR1TE Access Module (P/N 1180020L1) ............................... 62
  OCU DP Access Module (P/N 1180005L1) ............................... 63
  E&M/TO Access Module (P/N 1180402L1) ............................... 63
  Dual V.35 Access Module (P/N 1180025L1) ............................... 63
  DSX-1 Module (P/N 1200385L1) ......................................... 63

FIGURES

Total Access 850 Slot Designation (Front View) .......................... 61

TABLES

Table 1. Total Access 850 System Codes .................................... 57
Table 2. Power Supply Unit Codes .......................................... 57
1. INTRODUCTION

This section discusses Total Access 850 installation.

2. TOOLS REQUIRED

The tools required for wallmount installation of the Total Access 850 shelf are:

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

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

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

CAUTION
Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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 Total Access 850 is shipped in its own cardboard shipping carton. Open each carton carefully and avoid deep penetration into the carton with sharp objects.

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

Your ADTRAN shipment of the Total Access 850 chassis includes the following items:

- The Total Access 850 Base Unit
- The Total Access 850 Series System CD
- Wallmount brackets and screws
- RJ-45 to RJ-45 8-pin cable (15 ft) - ADTRAN P/N 3125M008
- UL 1950 Notice Card - ADTRAN P/N 61200375L1-17

Customer must supply Ethernet cable and the DB-9 serial cable for configuration via the VT100 CRAFT interfaces.

4. TELECOMMUNICATIONS CODES

The installation configurations codes are given below.

<table>
<thead>
<tr>
<th>Table 1. Total Access 850 System Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CODE</td>
</tr>
<tr>
<td>PC</td>
</tr>
<tr>
<td>IC</td>
</tr>
<tr>
<td>TC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2. Power Supply Unit Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CODE</td>
</tr>
<tr>
<td>PC</td>
</tr>
<tr>
<td>IC</td>
</tr>
<tr>
<td>TC</td>
</tr>
</tbody>
</table>

5. GROUNDING INSTRUCTIONS

To following paragraphs provide grounding instruction information from the Underwriters’ Laboratory UL1950 Standard for Safety of Information Technology Equipment Including Electrical Business Equipment, of July 28, 1995.

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

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

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

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

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

6. SUPPLYING POWER TO THE UNIT

The Total Access 850 has two power connection points. In all cases, only one of the
connection points is used. Adhere to the alternate connection instructions to ensure correct
installation.

On the Total Access 850 chassis, the incoming power termination point is on either of two backplane
connections, P6 or P7 (see Power Connections (P6 and P7) on page 39). Both sources connect directly to
the PSU. Connector P6 is used when the chassis is powered by an approved ADTRAN AC/DC Power
Supply and Battery Charger (for example, P/N 1175043Lx) which mounts directly to the chassis.
Connector P7 is used when -48 VDC is available on site and screw-type terminal connections are required.

AC Powered Systems

As shipped, the Total Access 850 is set to factory default conditions. After installing the chassis and any
access modules, the Total Access 850 is ready for power-up. To power-up the unit, ensure that the unit is
properly connected to an appropriate power source.
DC Powered Systems

The DC powered Total Access 850 comes equipped with a DC Power supply to furnish the voltages necessary for proper backplane operation. As shipped, the Total Access 850 is set to factory default conditions. After installing the chassis and any access modules, the Total Access 850 is ready for power-up.

Making Alternate Power Connections

For wire-wrap or screw terminal connections, the rear cover does not need to be removed; only the terminal access cover needs to be removed. Make wire-wrap or screw terminal connections as follows:

1. Unscrew the access cover hold-down screw.
2. Slide the access cover down slightly to disengage the lock-tabs from their slots.
3. Identify the wire-wrap pins designated for use, and make the connections starting with the pins closest to the exit port to avoid wiring interference as work progresses.
4. If alternate power connection to P7 is to be used, make those terminal connections last.
5. Carefully route wiring through the exit port.
6. Position and align the access cover tabs to the slots; insert the tabs and slide the cover up slightly until the screw holes are aligned. Ensure that exit wiring is not pinched or damaged.
7. Reinsert the hold-down screw.

- 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).
- To comply with GR-1089-CORE, Issue 3, this equipment MUST only be installed in a DC-C bonding and grounding environment. It may not be utilized in a DC-I (isolated) bonding and grounding environment.
- Power to the Total Access 850 DC system must be from a reliably grounded -48 VDC source which is electrically isolated from the AC source.
- The branch circuit overcurrent protection shall be a fuse or circuit breaker rated minimum 48 VDC, maximum 20A.
- A readily accessible disconnect device, suitably approved and rated, shall be incorporated in the input source wiring.
- Maximum recommended ambient operating temperature is 45 °C.

Use wire gauge suitable for the application.
7. MOUNTING OPTIONS

The Total Access 850 chassis may be wallmounted or installed in a 19-inch or 23-inch rack. Wallmount brackets are included with the chassis. For a rackmount installation, the Total Access 850 Base Unit allows flush-face mount, face-forward mount, center mount, and rear mount.

The Total Access 850 chassis includes wallmount brackets. If rack mount brackets are needed, use part number 1175045L1 or 1175046L1 for 19 inch or 23 inch, respectively.

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

Required Clearances

A minimum 10-inch clearance is required on the front end for access module insertion and withdrawal. On the backplane end, a five-inch clearance is required for wiring access to the V.35 connector. For those units installed in a communications bay, standard bay clearances are satisfactory.

Wallmounting the Chassis

Tools Needed

The Total Access 850 chassis mounts and connects with standard fasteners and hand tools:

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

Installing the Chassis

1. Position the chassis at the desired location; observe required clearances and ensure cable plugs reach their designated sockets.
2. Ensure the chassis is plumb; then mark through the flange mounting holes to identify where the pilot holes will be drilled.
3. Using a 1/16-inch drill bit, drill pilot holes at the marked locations.
4. Mount the chassis using the four #8 x 3/4-inch pan-head wood screws.
8. INSTALLING MODULES

Figure 1 shows the slot numbering designation as viewed from the front of the Total Access 850 chassis. The functionally identical option slots only accept Total Access 850 access modules, and the controller slots only accept Total Access 850 controller modules.

Figure 1. Total Access 850 Slot Designation (Front View)

WARNING
Access modules are intended to be serviced by qualified service personnel only.

Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.

Instructions for Installing the Power Supply Unit (P/N 1175006L2)

Follow the steps below to install the Power Supply Unit.

1. The Power Supply Unit inserts directly into the common card area in the position labeled PSU. The unit is mechanically keyed to prevent insertion in any other slot.

   NOTE
   Prior to circuit card installation, remove the chassis card-lock safety bar by disengaging the captured screw and lifting the safety bar away from the chassis.

2. To install the PSU, grasp the unit by the faceplate while supporting the bottom side.
3. Align the card edges to the guide grooves and insert the unit until the edge connector seats firmly into the backplane.

4. Lock the card in place by pushing in on the lock lever.

5. Reinstall the card-lock safety bar.

**Instructions for Installing the Total Access 850 Controller and Access Modules**

Individual access modules insert from the front. A locking bar holds the modules in place for added security. Disengaging the captured screw allows removal of the locking bar. To install Controller Resource and Access Modules for the Total Access 850, follow the steps outlined below.

1. Hold the access module by the faceplate while supporting the bottom side.

2. Align the module edges to the guide grooves for the designated slot.

3. Insert the module until the edge connector seats firmly into the backplane.

4. Lock the module in place by pushing in on the locking lever.

5. Connect the cables to the associated device(s). All wiring connections terminate on the backplane of the chassis.

**9. MODULE SHIPPING CONTENTS**

**Quad FXO Access Module (P/N 1175407L2)**

**Shipping Contents**

The ADTRAN shipment of the Quad FXO Access Module includes the following:

- Quad FXO Access Module

**Quad FXS Access Module (P/N 1175408L2)**

**Shipping Contents**

The ADTRAN shipment of the Quad FXS Access Module includes the following:

- Quad FXS Access Module

**UBR1TE Access Module (P/N 1180020L1)**

**Shipping Contents**

The ADTRAN shipment of the UBR1TE Access Module includes the following items:

- UBR1TE Access Module
- UBR1TE Access Module Job Aid
OCU DP Access Module (P/N 118005L1)

Shipping Contents

The ADTRAN shipment of the OCU DP Access Module includes the following items:
- OCU DP Access Module
- OCU DP Access Module Job Aid

E&M/TO Access Module (P/N 1180402L1)

Shipping Contents

The ADTRAN shipment of the E&M/TO Access Module includes the following items:
- E&M/TO Access Module
- E&M/TO Access Module Job Aid

Dual V.35 Access Module (P/N 118025L1)

Shipping Contents

The ADTRAN shipment of the Dual V.35 Access Module includes the following items:
- Dual V.35 Access Module
- Dual V.35 Access Module Job Aid

DSX-1 Module (P/N 1200385L1)

The ADTRAN shipment of the DSX-1 Module includes the following:
- DSX-1 Module
This section provides detailed descriptions of all menu options and configuration parameters available for the Total Access 850 when used with a Router Control Unit (RCU). This section does not apply to systems that employ a Bank Control Unit (BCU).

This section of ADTRAN’s Total Access 850 System Manual is designed for use by network administrators and others who will configure and provision the system. It contains information about navigating the VT100 user interface, configuration information, and menu descriptions.

**CONTENTS**

**Navigating the Terminal Menu** ................................................................. 69  
   Terminal Menu Window ................................................................................ 69  
   Navigating using the Keyboard Keys ........................................................... 71

**MAIN Menu and System Control** .............................................................. 73  
   Selecting the Appropriate Menu ............................................................... 73  
   Security Levels .......................................................................................... 74

**Menu Descriptions** .................................................................................. 74  
   System Info ................................................................................................. 75  
   System Config. ........................................................................................... 77  
   System Utility ............................................................................................. 90  
   Interfaces .................................................................................................... 96  
   Interfaces (Network T1) ............................................................................. 96  
   Interfaces (DSX) .......................................................................................... 100
   Interfaces (ETH) .......................................................................................... 103
   Interfaces (V35) ........................................................................................... 104
   Interfaces (FXS) .......................................................................................... 105
   Interfaces (FXO) .......................................................................................... 109
   Interfaces (DSX-1 Module) ......................................................................... 111
   Interfaces (UBR1TE Module) ....................................................................... 113
   L2 Protocol (T1 TDM Firmware) ................................................................. 118
   L2 Protocol (T1 TDM Firmware) – T1 Interface ........................................ 119
   L2 Protocol (T1 TDM Firmware) – T1 Interface > PPP ............................... 120
   L2 Protocol (T1 TDM Firmware) – T1 Interface > FRE Protocol ................. 123
   L2 Protocol (T1 TDM Firmware) – T1 Interface > HDLC Protocol ............ 127
   L2 Protocol (T1 TDM Firmware) – T1 Interface > Auto Protocol ............... 128
   L2 Protocol (T1 ATM Firmware) ................................................................. 130
   L2 Protocol (T1 ATM Firmware) – T1 Interface ........................................ 131
   L2 Protocol (T1 ATM Firmware) – T1 Interface > ATM ............................. 131
   L2 Protocol (T1 ATM Firmware) – T1 Interface > CuMTN ........................... 141
   L2 Protocol (T1 ATM Firmware) – V.35 Interface ....................................... 143
   L2 Protocol (T1 ATM Firmware) – DSX Interface ....................................... 145
   L2 Protocol (All Firmware) – ETH Interface > 802.3 Protocol .................. 146
   Bridge .......................................................................................................... 147
   Router ......................................................................................................... 150
   Security ...................................................................................................... 172
   DS0 Maps .................................................................................................... 181

**Appendices (T1 TDM Applications)** ......................................................... 184

**Appendices (T1 ATM Applications)** ......................................................... 201
FIGURES

Figure 1. Top-Level Terminal Menu Window ......................................................... 69
Figure 2. Alternate Menu View ............................................................................. 70
Figure 3. System Info Menu .................................................................................. 75
Figure 4. System Config Menu ............................................................................ 77
Figure 5. System Utility Menu ............................................................................. 90
Figure 6. Interfaces Menus .................................................................................... 96
Figure 7. UBR1TE Network Configurations .......................................................... 114
Figure 8. L2 Protocol (T1 TDM) Menu. ................................................................. 118
Figure 9. L2 Protocol (T1 TDM) Menu. ................................................................. 130
Figure 10. Bridge Menu ....................................................................................... 147
Figure 11. Router Menu ....................................................................................... 150
Figure 12. Security Menu ..................................................................................... 173
Figure 13. DS0 Maps Menu .................................................................................. 181
Figure 7. Application Diagram ............................................................................ 201
Figure 10. Application Diagram ........................................................................... 206

TABLES

Table 1. Password Security Level ......................................................................... 74
Table 2. Instructions for Changing Passwords ...................................................... 78
Table 3. Telnet Security Levels ............................................................................. 80
1. **NAVIGATING THE TERMINAL MENU**

To access the terminal menus and management features of the Total Access 850, connect the unit to a VT100 terminal (or VT100 terminal emulator) via the CRAFT interface on the front of the unit or the rear CRAFT interface on the backplane. Configure the terminal settings for 9600 data rate, no parity, 8 data bits, 1 stop bit, and no flow control.

After connecting to the unit and beginning a terminal session, a login screen appears. There is no default password for the Total Access 850; press <ENTER> to access the terminal menus. (Refer to DLP-2, *Logging in to the System* for detailed instructions.)

**Terminal Menu Window**

After logging in, all menu items and data fields are displayed in the terminal menu window (see Figure 1), through which you have complete control of the Total Access 850.

---

**Menu Path**

The first line of the terminal menu window (the menu path) shows the session’s current position (path) in the menu structure. For example, Figure 1 shows the top-level menu with the cursor on the SYSTEM CONFIG submenu; therefore, the menu path reads **TOTAL ACCESS 850/SYSTEM CONFIG**.

**Window Panes**

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

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

![Figure 2. Alternate Menu View](image_url)

**Window Pane Navigation**

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

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Press this key...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move from left pane to right pane</td>
<td>Tab, Enter, Right arrow</td>
</tr>
<tr>
<td>Move from right pane to left pane</td>
<td>Tab, Escape, Left arrow, Backspace</td>
</tr>
<tr>
<td>Move within each pane</td>
<td>Up arrow, Down arrow, Left arrow, Right arrow</td>
</tr>
</tbody>
</table>
Right Window Pane Notation
The right window pane shows the contents of the currently selected menu. These contents include both submenu items and data fields. Some submenus contain additional submenus and some data fields contain additional data fields. The following chart explains the notation used to identify these additional items.

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

Additional Terminal Menu Window Features
- **DS0 Status** – displays the current mapping of DS0s in the Total Access 850 system. DS0s mapped to the router display r, unmapped DS0s display –, and all other DS0s display *.
- **Tool Tip** – provides a brief description of the currently selected mode.
- **Slot Status** – displays type of module installed in each slot. No entry will appear for slots not containing a module.
- **Telnet Info** – displays information pertaining to the active Telnet session. This information is not displayed when connecting to the system via the CRAFT interface.
- **Ethernet Link Status** – displays the current status of the integrated Ethernet interface (located on the rear of the chassis). This information is only available when using a 3rd Generation RCU.
- **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 the current time.
- **Network Status** – displays network status information as UP or DOWN.

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

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Press this key...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return to the home screen</td>
<td>H</td>
</tr>
<tr>
<td>Jump between two menu items</td>
<td>J</td>
</tr>
<tr>
<td>Press &lt;J&gt; while the cursor is located on a menu item, and you jump back to the main screen.</td>
<td></td>
</tr>
<tr>
<td>Go to another menu item, press &lt;J&gt;, and you jump back to the screen that was displayed the first time you pressed &lt;J&gt;.</td>
<td></td>
</tr>
<tr>
<td>Press &lt;J&gt; anytime you want to jump between these items.</td>
<td></td>
</tr>
</tbody>
</table>
### Session Management Keystrokes

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Press this key...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select items</td>
<td>Arrows</td>
</tr>
<tr>
<td>Edit a selected menu item</td>
<td>Enter</td>
</tr>
<tr>
<td>Cancel an edit</td>
<td>Escape</td>
</tr>
<tr>
<td>Close pop-up help screen</td>
<td>Escape</td>
</tr>
<tr>
<td>Move between the left and right panes</td>
<td>Tab Arrows</td>
</tr>
<tr>
<td>Move to the top of a screen</td>
<td>A</td>
</tr>
<tr>
<td>Move to the bottom of a screen</td>
<td>Z</td>
</tr>
<tr>
<td>Ascend one menu level</td>
<td>Backspace</td>
</tr>
<tr>
<td>Jump to terminal mode</td>
<td>CTRL+T</td>
</tr>
<tr>
<td>Jump to NAT menu</td>
<td>CTRL+N</td>
</tr>
</tbody>
</table>

### Configuration Keystrokes

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Press this key...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log out of a session</td>
<td>CTRL+L</td>
</tr>
<tr>
<td>Refresh the screen</td>
<td>CTRL+R</td>
</tr>
<tr>
<td>To do this... Refresh the screen</td>
<td></td>
</tr>
<tr>
<td>To save time, only the portion of the screen that has changed is refreshed. This option should only be necessary if the display picks up incorrect characters caused by disconnecting and reconnecting the terminal session.</td>
<td></td>
</tr>
<tr>
<td>Restore factory default settings</td>
<td>F</td>
</tr>
<tr>
<td>Copy selected items to the clipboard</td>
<td>C</td>
</tr>
<tr>
<td>The amount of information you can copy depends on the cursor location when you press &lt;C&gt;:</td>
<td></td>
</tr>
<tr>
<td>If the cursor is over an editable field, only that item is copied.</td>
<td></td>
</tr>
<tr>
<td>If the cursor is over the index number of a list, then all of the items in the row of the list are copied. For example, if the cursor is over the selection # field in the INTERFACES screen, all of the information associated with the interface is copied.</td>
<td></td>
</tr>
<tr>
<td>Paste the item stored in the clipboard, if the information is compatible</td>
<td>P</td>
</tr>
<tr>
<td>You must confirm all pastes — except those to a single editable field.</td>
<td></td>
</tr>
</tbody>
</table>
Getting Help
The bottom line of the terminal menu window contains context-sensitive help information. When the cursor is positioned over a set of configuration items, a help message displays (when available) providing a description of the item. When more detailed help is available for a particular item, ^A displays at the bottom of the window. At this point, pressing <CTRL+A> displays a pop-up help screen with information about the item.

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

2. MAIN MENU AND SYSTEM CONTROL

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

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Press this key...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increment the value of certain types of fields by one when you paste information into those fields</td>
<td>&gt;</td>
</tr>
<tr>
<td>Decrement the value of certain types of fields by one when you paste information into those fields</td>
<td>&lt;</td>
</tr>
<tr>
<td>Save the current configuration immediately to RAM</td>
<td>CTRL+W</td>
</tr>
<tr>
<td>Insert a new list item</td>
<td>I</td>
</tr>
<tr>
<td>For example, add a new item to the TELNET USER connection list by pressing &lt;I&gt; while the cursor is over the index number.</td>
<td></td>
</tr>
<tr>
<td>Delete a list item</td>
<td>D</td>
</tr>
<tr>
<td>For example, delete an item from the TELNET USER connection list by pressing &lt;D&gt; while the index number is active.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Go to this menu...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review and monitor general system information for the Total Access 850</td>
<td>SYSTEM INFO</td>
</tr>
<tr>
<td>Set up the operational configuration for the Total Access 850</td>
<td>SYSTEM CONFIG</td>
</tr>
<tr>
<td>Upgrade firmware, perform config transfers, ping, and access terminal mode</td>
<td>SYSTEM UTILITY</td>
</tr>
<tr>
<td>Review and configure settings for all interfaces (including installed modules)</td>
<td>INTERFACES</td>
</tr>
<tr>
<td>Configures the Layer 2 protocol for the various interfaces (T1, Ethernet, etc.) and provides all applicable L2 status information</td>
<td>L2 PROTOCOL</td>
</tr>
<tr>
<td>Configure the bridging parameters and view applicable bridging statistics</td>
<td>BRIDGE</td>
</tr>
</tbody>
</table>
Security Levels

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

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

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

## 3. MENU DESCRIPTIONS

The remainder of this section describes Total Access 850 menu and submenu options.

*To help you follow the terminal menu hierarchy, the following notations are used:*

**MENUS > SUBMENUS > SUB-SUBMENUS**
SYSTEM INFO

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

![Figure 3. System Info Menu](image)

**SYSTEM INFO > SYSTEM NAME**

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

**SYSTEM INFO > SYSTEM LOCATION**

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

**SYSTEM INFO > SYSTEM CONTACT**

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or E-mail address of a person responsible for the unit. You can enter up to 127 alpha-numeric characters in this field, including spaces and special characters (such as an underscore).
**SYSTEM INFO > UNIT NAME**
(Read only) Displays a product-specific name for the unit (such as TA 850 RCU).

**SYSTEM INFO > CLEI CODE**
(Read only) Displays the registered CLEI code for the unit.

**SYSTEM INFO > PART NUMBER**
(Read only) Displays the ADTRAN-specific part number for the unit.

**SYSTEM INFO > SERIAL NUMBER**
(Read only) Displays the serial number for the unit. The serial number of the Total Access 850 will automatically display in this field. This serial number matches the serial number located on the bottom of the unit’s chassis.

**SYSTEM INFO > FIRMWARE REVISION**
(Read only) Displays the current firmware revision level of the unit.

**SYSTEM INFO > BOOTCODE REVISION**
(Read only) Displays the current bootcode revision.

**SYSTEM INFO > SYSTEM UPTIME**
Displays the length of time the Total Access 850 system has been running. Each time you reset the system, this value resets to 0 days, 0 hours, 0 min and 0 secs.

**SYSTEM INFO > DATE/TIME**
Displays the current date and time, including seconds. To edit this field, place the cursor on the field and press `<ENTER>`. Then, enter the time in a 24-hour format (such as 23:00:00 for 11:00 pm), and the date in mm-dd-yyyy format (for example, 10-30-1998). Press `<ENTER>` when you are finished to accept the change.

---

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

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

**SYSTEM CONFIG > MANAGEMENT**

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

**SYSTEM CONFIG > MANAGEMENT > CRAFT PORT**

Set up the **CRAFT PORT** parameters from this menu. The unit’s VT100 **CRAFT** port can be accessed via an RJ-48 connector located on the rear of the unit, or via the DB-9 connector on the front of the unit.

**SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PASSWORD PROTECT**

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

**SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > PASSWORD**

Enter the user-defined password (up to 30 alphanumeric characters including spaces and special characters) to protect the **CRAFT** port. By default, no password is entered. Table 2 on page 76 provides instructions for changing the password.

**NOTE**

Connecting directly to the **CRAFT** port provides full access to all menus. Enable the password on the **CRAFT** port to protect against unauthorized access.
Table 2. Instructions for Changing Passwords

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select the PASSWORD field—a new PASSWORD field displays.</td>
</tr>
<tr>
<td>2</td>
<td>Type the new password in the ENTER field.</td>
</tr>
<tr>
<td>3</td>
<td>Type the new password again in the CONFIRM field.</td>
</tr>
</tbody>
</table>

**SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > IDLE TIME**

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

**SYSTEM CONFIG > MANAGEMENT > CRAFT PORT > BAUD RATE**

This is the asynchronous rate that the CRAFT port will run. The possible values are 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200. The default value is 9600.

**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. The Total Access 850 supports up to five simultaneous Telnet sessions.

> The Total Access 850 ships with default Telnet Access parameters of: guest (user), password (password). Change this password during the initial configuration to protect your unit.

**SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > ACCESS**

Sets ACCESS to ON or OFF. The factory default value for this parameter is ON.
**SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > AUTHEN METHOD**
Set up the Telnet authentication method from this menu. The choices are **LOCAL PASSWORD**, **RADIUS**, **LOCAL/RADIUS**, and **RADIUS/LOCAL**. **LOCAL/RADIUS** indicates that the unit will try Local Password Authentication first, and if that fails, it will try Radius Authentication. **RADIUS/LOCAL** indicates that the unit will try Radius authentication first, and if that fails, it will try Local Password authentication. The default is **LOCAL PASSWORD**.

**SYSTEM CONFIG > MANAGEMENT > TELNET PORT**
Defines the TCP port number used when establishing a Telnet session. Normal Telnet port is 23. Enter a customized port number if desired.

**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 TO 255 MINUTES**.

```
LEVEL
```
This is the security level granted to the user. Table 3 on page 78 gives a brief description of each level. The factory default is **FULL**.
### Table 3. Telnet Security Levels

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>The user has all access to view and configure all menus (same as logging in to the CRAFT port)</td>
</tr>
<tr>
<td>Support</td>
<td>The user has read only access to view the SYSTEM_INFO menu. The user has privileges to view and change everything under the SYSTEM_CONFIG menu except for the CRAFT port settings, Telnet access lists, and the SNMP management communities. The user has full access to the SYSTEM UTILITY menu, including the ability to upgrade firmware and reset the unit. The user has full access to the INTERFACES, L2 PROTOCOL, BRIDGE, ROUTER, and DS0 menus. The user does not have the ability to set RADIUS_SERVER settings under the SECURITY menu.</td>
</tr>
<tr>
<td>Config</td>
<td>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.</td>
</tr>
<tr>
<td>Router</td>
<td>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.</td>
</tr>
<tr>
<td>Voice</td>
<td>The user has read only privileges for the SYSTEM_INFO menu. The user has access to the PING and TRACEROUTE utilities from the SYSTEM UTILITIES menu. The user has full access to the FXS module from the INTERFACES menu.</td>
</tr>
<tr>
<td>Status</td>
<td>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.</td>
</tr>
</tbody>
</table>

**SYSTEM_CONFIG > MANAGEMENT > TELNET_ACCESS > ACTIVE_SESSIONS**

Provides a list of all Telnet sessions currently active on the Total Access 850 system.

- **#**
  Displays the index number of the Telnet user.

- **NAME**
  Displays the text string entered in the Telnet configuration for this user.

- **PORT**
  Displays the TCP port used for this Telnet session.

- **TIME TO LIVE**
  Displays the amount of time (in minutes) before this Telnet session is terminated by the Total Access 850.
**SYSTEM CONFIG > MANAGEMENT > TELNET ACCESS > IP ACCESS LIST**

Set up the list of allowed Telnet managers.

**NETWORK ADDRESS**

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

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

**MASK**

Enter a subnet mask corresponding to the entered network address. 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 blocks all host Telnet access.

The factory default is **0.0.0.0** for both parameters, which allows all users Telnet IP access.

**SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT**

Active 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 > TRAP DELAY**

When enabled, the Total Access 850 inserts a delay before transmitting a created trap for the SNMP session.

**SYSTEM CONFIG > MANAGEMENT > SNMP MANAGEMENT > COMMUNITIES**

Set up the SNMP communities parameters from this menu.

**#**

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

**NAME**

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

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

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

**MANAGER IP**

This may be used in conjunction with the Netmask field to define a range of manager IPs. A netmask of 255.255.255.255 defines a single IP as the manager host IP. 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 255.255.255.254 netmask is used, which determines the far-side address as well (since there can be only two addresses on a subnet with that netmask). When set to **Off**, the user must input the IP address assigned to the FDL interface. Default is **On**.

**SYSTEM CONFIG > MANAGEMENT > FDL MANAGEMENT > ACCEPT ALL SNMP**
When set to **On**, SNMP gets/sets received over the FDL link are always accepted regardless of the community table. When set to **Off**, the community table is searched for valid manager IP addresses and the SNMP traffic is rejected if a match is not found. Default is **On**.

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

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

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

**SYSTEM CONFIG > SYSLOG > SYSLOG IP**
IP address of the syslog daemon to which log message should be sent. The values must be dotted decimal notation.
SYSTEM CONFIG > SYSLOG > SYSLOG FORMAT

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

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.

This does not have to correspond to the facility level shown in the terminal mode option. See SYSLOG using Terminal Mode on page 83.

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.

ADTRAN recommends using DEBUG for only short periods of time, and for debug purposes only.
SYSLOG using Terminal Mode
Another option for configuring syslog is using the terminal mode command `log dump <logname>`. The logname must be all CAPS and be one of the following names:

- FATAL
- ALERT
- CRITICAL
- ERROR
- WARNING
- NOTICE
- INFO
- FILTER
- 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**
Minimum required level for sending log messages about communication with the Nokia DSLAM. Messages are only generated for products with an SDSL WAN interface.

**SYSTEM CONFIG > SYSLOG > AUTOBAUD LEVEL**
Minimum required level for sending log messages about communication with the Lucent Stinger DSLAM. Messages are only generated for products with an SDSL WAN interface.

**SYSTEM CONFIG > SYSLOG > TOLLBRG LEVEL**
Minimum required level for sending log messages about communication with the Tollbridge Voice Gateway. Messages are only generated for ATM products.
SYSTEM CONFIG > SYSLOG > CMCP LEVEL
Minimum required level for sending log messages about communication with the CopperMountain DSLAM. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > SDSL LEVEL
This parameter is for ADTRAN internal use only.

SYSTEM CONFIG > SYSLOG > L1 LEVEL
Minimum required level for sending log messages about WAN physical or Layer 1 connection.

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

SYSTEM CONFIG > SYSLOG > JETSTREAM LEVEL
Minimum required level for sending log messages about communication with the JetStream Voice Gateway. Messages are only generated for ATM products.

SYSTEM CONFIG > SYSLOG > POTS LEVEL
Minimum required level for sending log messages about POTS line cards and services.

SYSTEM CONFIG > SYSLOG > LESCAS LEVEL
Minimum required level for sending messages about communication with LESCAS compatible Voice Gateways. Messages are only generated for ATM products.
**SYSTEM CONFIG > SYSLOG > ATM LEVEL**
Minimum required level for sending ATM log messages. Messages are only generated for ATM products.

**SYSTEM CONFIG > SYSLOG > COPPERCOM LEVEL**
Minimum required level for sending log messages about communication with the CopperCom Voice Gateway. Messages are only generated for ATM products.

**SYSTEM CONFIG > SYSLOG > VOFR LEVEL**
Minimum required level for sending voice-over-frame-relay log messages about communication with the CopperMountain DSLAM. Messages are only generated for ATM products.

**SYSTEM CONFIG > SYSLOG > XMODEM LEVEL**
Minimum required level for sending XMODEM log messages for firmware and configuration transfers.

**SYSTEM CONFIG > SYSLOG > EMWEB LEVEL**
This parameter is for ADTRAN internal use only.

**SYSTEM CONFIG > SYSLOG > FRELAY LEVEL**
Minimum required level for sending frame relay log messages.

**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**
Minimum required level for sending Voice-over-ATM log messages.

**SYSTEM CONFIG > SYSLOG > PPPOA LEVEL**
Minimum required level for sending PPP-over-ATM log messages.

**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.

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.

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.

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.

> If you execute this command, the unit retrieves the configuration file, reboots, then restarts 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.

> 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 > CPU UTILIZATION**
Provides maximum CPU utilization percentages for the following intervals:

<table>
<thead>
<tr>
<th>Interval</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FROM POWER-UP</strong></td>
<td>Max CPU utilization since the last Total Access 850 restart.</td>
</tr>
<tr>
<td><strong>LAST SECOND</strong></td>
<td>Max CPU utilization in the last second. This is the most current CPU utilization information.</td>
</tr>
<tr>
<td><strong>FROM LAST CLEAR</strong></td>
<td>Max CPU utilization since the last manual clear of the performance statistics using the <strong>CLEAR STATS</strong> command.</td>
</tr>
</tbody>
</table>

**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.

- **SYSTEM UTILITY > PING > HOST ADDRESS**
  IP address or domain name (if DNS is configured) of device to receive the ping. The factory default is no entry in the host address field.

- **SYSTEM UTILITY > PING > SIZE (40-1500)**
  Total size of the ping to send. Range is 40 to 1500 bytes. The default is 64.

- **SYSTEM UTILITY > PING > # OF PACKETS**
  Total packets to send 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 milliseconds) given to a host (along a path to the final destination) to respond to the probe datagram sent before considering the packet a failure.

SYSTEM UTILITY > TRACEROUTE > RETRIES
Specifies the number of times the probe datagram is sent to each host (along the path to the final destination).

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

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

- Use the save command to write the entire configuration to flash.
- Display the unit’s MAC address with the command mac.
- Perform a ping or extended ping. Syntax is:
  
  ping hostname/address [repeat xx] [size xx] [timeout xx] [source xx] [noNat]

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

Options may be entered in any order and may be truncated.
Valid interface names are eth0, fd10, ppp0, fr0, fr1, etc.

Example usage: **ping 10.0.0.5 r si 1500 so eth0 n**
This will ping with a repeat count of 10. The datagram size is 1500 bytes, and the source address used in the ping packet will be the Ethernet IP address. The “noNat” option has been specified, so if NAT is enabled, this packet will NOT be translated.

- Perform a traceroute or extended traceroute. Syntax is:

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

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

  Options may be entered in any order and may be truncated.
  Valid interface names are eth0, fd10, ppp0, fr0, fr1, etc.

  Example usage: **trace 10.0.0.5 h 20 t 1 r 1 so eth0**
  This will perform a trace to 10.0.0.5 with a max hop count of 20. The timeout for each hop is 1 second, and the retry count per hop is 1. The Ethernet IP will be used as the source address, and the packet WILL go through NAT if NAT is enabled, meaning that the packet will be translated and the source address will be replaced by the NAPT address.

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

  **Telnet hostname/address [port xx]**
  Default port is 23 (TELNET).

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

**NOTE**

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

Use the INTERFACES menu to view and configure parameters for the T1, ETHERNET, V.35, FXS, FXO, DSX-1 MODULE, and UBR1TE interfaces as shown in Figure 6.

**INTERFACES (NETWORK T1)**

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

**INTERFACES (T1) > CONFIG**

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

**INTERFACES (T1) > 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) > CONFIG > FORMAT**

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

**INTERFACES (T1) > CONFIG > LINE CODE**

This sets the line code for the T1 interface. The setting must match the line code of the circuit to which the interface is connected. Choices are B8ZS (bipolar with 8-zero substitution) and AMI (alternate mark inversion). Default is B8ZS.
**INTERFACES (T1) > CONFIG > EQUALIZATION**
Select the line build out for the T1 interface. These are attenuation settings. 0 dB is the strongest signal, and the other settings make the T1 transmit signal weaker. The setting of this field depends on whether the circuit is provisioned for DS1 by the telephone company. The choices are 0 dB, -7.5 dB, -15 dB, -22 dB. Default is 0 dB.

**INTERFACES (T1) > CONFIG > CSU LPBK**
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) > CONFIG > RX SENSITIVITY**
Configures the sensitivity of the T1 receiver for this interface to provide increased sensitivity for long-run T1 applications. Choices are AUTO, -36 dB, and -10 dB.

**INTERFACES (T1) > STATUS**
Displays the T1 status including performance data and alarm histories.

**INTERFACES (T1) > STATUS > PERFORMANCE**
Displays the T1 performance data.

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

**INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > INTERVAL**
Identifies the interval (CURRENT or TOTAL) for the listed performance statistics.

**INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > ES**
ES (Errored Second) - For ESF mode, an errored second is defined as a second with one or more Path Code Violations (PCVs), or one or more Out of Frame (OOF) defects, or one or more Controlled Slip events, or a detected AIS (blue alarm) defect. For D4 (SF) mode, the presence of Bipolar Violations (BPVs) also triggers an errored second.

**INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SES**
SES (Severely Errored Second) - For ESF mode, an SES is a second with 320 or more PCVs, or one or more OOF defects, or a detected AIS defect. For D4 (SF) mode, an SES is a second with one or more Framing Error events, or an OOF defect, or at least 1544 Line Code Violations or more.

**INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SEF**
SEF (Severely Errored Frame) - An SEF condition occurs when 2 out of 6 consecutive frame bits are in error.
INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > FS
FS (Frame Slip) - A frame slip is defined as one or more frame bit errors in a one-second interval.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > LCV
LCV (Line Code Violation) - A Line Code Violation is defined as a Bipolar Violation (BPV), not including the B8ZS code word if B8ZS is employed. The number displayed is LCV events, which is defined as one or more BPVs in a one-second interval.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > SLP
SLP (Slip Error Event) - This occurs when a received frame is either repeated or deleted. A SLP error indicates a timing problem.

INTERFACES (T1) > STATUS > PERFORMANCE > CURRENT AND TOTALS > UAS
UAS (Unavailable Seconds) - When 10 consecutive 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-SES seconds have occurred.

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

INTERFACES (T1) > STATUS > PERFORMANCE > CLEAR CURRENT DATA
Clears all statistics collected in the CURRENT AND TOTALS statistics table.

INTERFACES (T1) > STATUS > PERFORMANCE > CLEAR ALL DATA
Clears all statistics collected in the CURRENT AND TOTALS and the EXTENDED 24 hour statistics tables.

INTERFACES (T1) > STATUS > ALARMS
Displays current alarms and alarm history for T1 interface.

INTERFACES (T1) > STATUS > ALARMS > CURRENT ALARMS
Displays the current alarms on the T1 interface. An asterisk in a field indicates that an alarm is active.

- LOS: Loss of Signal. No signal detected on port interface.
- RED: Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF).
- YELLOW: Remote alarm indicator (RAI) being received on port.
- BLUE: Receiving unframed all ones from the port alarm indicator signal (AIS).
**Interfaces (T1) > Status > Alarms > Alarm History**
Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history. Refer to *Interfaces (T1) > Status > Alarms > Current Alarms* on page 96 for more details on listed alarm conditions.

**Interfaces (T1) > Status > Alarms > Clear History**
Selecting this activator will clear the Alarm History for the T1 interface.

**Interfaces (T1) > Status > Rx Level**
Displays the level (in dB) of the received T1 signal on the interface.

**Interfaces (T1) > Test**
These options are used to initiate local and remote loopback tests and display the test status.

**Interfaces (T1) > Test > Loc LB**
Loopback of the local unit. Choices are **NONE**, **LINE**, and **PAYLOAD**. **LINE** loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **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) > 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) > Test > Test Status**
Indicates whether a test is in progress.
**INTERFACES (DSX)**

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

**INTERFACES (DSX) > Config**

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

**INTERFACES (DSX) > Config > Format**

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

**INTERFACES (DSX) > Config > Line Code**

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

**INTERFACES (DSX) > Config > Equalization**

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

**INTERFACES (DSX) > Config > CSU LPBK**

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 (DSX) > Config > RX Sensitivity**

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

**INTERFACES (DSX) > Status**

Displays the T1 status including performance data and alarm histories.

**INTERFACES (DSX) > Status > Performance**

Displays the T1 performance data.

**INTERFACES (DSX) > Status > Performance > Current and Totals**

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

**INTERFACES (DSX) > Status > Performance > Current and Totals > Interval**

Identifies the interval (**Current** or **Total**) for the listed performance statistics.
**INTERFACES (DSX) > STATUS > PERFORMANCE > CURRENT AND TOTALS > ES**

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

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

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

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

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

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

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

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

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

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

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

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

**UAS** (Unavailable Seconds) - When 10 consecutive 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-SES seconds have occurred.

**INTERFACES (DSX) > STATUS > PERFORMANCE > EXTENDED**

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

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

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

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

Clears all statistics collected in the CURRENT AND TOTALS and the EXTENDED 24 hour statistics tables.
**INTERFACES (DSX) > STATUS > ALARMS**
Displays current alarms and alarm history for the integrated DSX interface.

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

**INTERFACES (DSX) > STATUS > ALARMS > CLEAR HISTORY**
Selecting this activator will clear the Alarm History for the integrated DSX interface.

**INTERFACES (DSX) > STATUS > RX LEVEL**
Displays the level (in dB) of the received T1 signal on the interface.

**INTERFACES (DSX) > TEST**
These options are used to initiate local and remote loopback tests and display the test status.

**INTERFACES (DSX) > TEST > LOC LB**
Loopback of the local unit. Choices are **NONE, LINE, AND PAYLOAD**. **LINE** loopback loops all of the received data back toward the network. The transmitted data is the identical line code that was received, including any bipolar violations. **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 (DSX) > 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 (DSX) > TEST > TEST STATUS**
Indicates whether a test is in progress.
INTERFACES (ETH)

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

INTERFACES (ETH) > CONFIG

Configure the various Ethernet parameters from this menu.

INTERFACES (ETH) > CONFIG > AUTO NEGOTIATION

The Total Access 850 has the capability of auto negotiating the rate and duplex of the connected Ethernet link. Additionally, when this parameter is set to OFF, the rate and duplex are set manually. Auto Negotiation is only available when using a 3rd Generation RCU with the Total Access 850 system.

INTERFACES (ETH) > CONFIG > DATE RATE

Defines the Ethernet interface as 100BASET or 10BASET. Data Rate configuration is only available when using a 3rd Generation RCU with the Total Access 850 system.

INTERFACES (ETH) > CONFIG > DUPLEX TYPE

Defines operation on the Ethernet interface as FULL DUPLEX or HALF DUPLEX. Duplex Type configuration is only available when using a 3rd Generation RCU with the Total Access 850 system.

INTERFACES (ETH) > STATUS

Displays the Ethernet status information.

INTERFACES (ETH) > STATUS > MAC ADDRESS

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

INTERFACES (ETH) > STATUS > DATA LINK

Displays the current status of the Ethernet link as either UP or DOWN. If there is an active Ethernet link, the status displays UP. Data Link status information is only available when using a 3rd Generation RCU with the Total Access 850 system.

INTERFACES (ETH) > STATUS > DATA RATE

Displays the Ethernet interface current rate of operation (as defined by the DATA RATE configuration parameter).

INTERFACES (ETH) > STATUS > DUPLEX TYPE

Displays the Ethernet interface current mode of operation (as defined by the DUPLEX TYPE configuration parameter). Duplex Type status information is only available when using a 3rd Generation RCU with the Total Access 850 system.
**INTERFACES (V35)**

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

**INTERFACES (V35) > Config**

Configure the DTE leads from this menu.

**INTERFACES (V35) > Config > CTS**

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

**INTERFACES (V35) > Config > DCD**

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

**INTERFACES (V35) > Config > DSR**

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

**INTERFACES (V35) > Status**

View the status of the DTE leads from this menu.

**INTERFACES (V35) > Status > RTS**

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

**INTERFACES (V35) > Status > DTR**

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

**INTERFACES (V35) > Test**

These options are used to loopback tests.

**INTERFACES (V35) > Test > Loopback**

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

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

INTERFACES (FXS) > CONFIG

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

INTERFACES (FXS) > CONFIG > SLOT

Displays the slot number associated with the installed FXS Module.

INTERFACES (FXS) > CONFIG > PORT

Indicates the port on which the FXS is installed.

INTERFACES (FXS) > CONFIG > MODE

Choices are given below. Default is LOOP START.

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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOOP START</td>
<td>Sets the port to use FXS loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.</td>
</tr>
<tr>
<td>GROUND START</td>
<td>Sets the port to use FXS ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.</td>
</tr>
<tr>
<td>PLAR</td>
<td>Sets the port to use Private Line, Automatic Ringdown signaling on the analog 2-wire interface. When one end of a PLAR circuit goes off-hook, the other end automatically rings. PLAR circuits are point to point between two interfaces.</td>
</tr>
<tr>
<td>TR08 SINGLE</td>
<td>Sets the port to use Single Party Channel Unit signaling on the T-span (as defined by TR-TSY-000008) and loop start supervision on the analog 2-wire interface.</td>
</tr>
<tr>
<td>TR08 UVG</td>
<td>Sets the port to use Universal Voice Grade signaling on the T-span (as defined by TR-TSY-000008) and either loop start or ground start supervision on the analog 2-wire interface.</td>
</tr>
<tr>
<td>DPO</td>
<td>Sets the port to use Dial Pulse signaling to originate dialed numbers.</td>
</tr>
<tr>
<td>TANDEM (E&amp;M)</td>
<td>Sets the port to use E&amp;M signaling on the T-span and either loop start or ground start supervision on the analog 2-wire interface. See the TANDEM submenus for more information.</td>
</tr>
</tbody>
</table>
**INTERFACES (FXS) > Config > Tx (dB)**

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

**INTERFACES (FXS) > Config > Rx (dB)**

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

**INTERFACES (FXS) > Config > Svc Mode**

Indicates whether the module is *In Service* or *Out of Svc*. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 Maps** menu. Default is *In Service*.

**INTERFACES (FXS) > Config > Line Z**

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

**INTERFACES (FXS) > Config > Msg Ind**

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

**INTERFACES (FXS) > Config > Tandem**

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

**INTERFACES (FXS) > Config > Tandem > Conversion Mode**

Sets the port to either **Loop Start** or **Ground Start** mode. Default is **Loop Start**.

**INTERFACES (FXS) > Config > Tandem > Supervision**

Sets the supervision method used to either **Immediate** or **Wink**. Default is **Immediate**.

**INTERFACES (FXS) > Config > Tandem > Dial Tone**

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

**INTERFACES (FXS) > Config > Tandem > Ring Back**

Used to enable or disable the option of generating ring back tone towards the T-span. Default is **Disable**.
INTERFACES (FXS) > CONFIG > TANDEM ANSWER SUPERVISION
Causes the polarity of tip and ring to be reversed when the far-end answers. Can be enabled or disabled. Default is DISABLE.

INTERFACES (FXS) > CONFIG > TANDEM > DNIS OPTIONS
This parameter is used in conjunction with DNIS DELAY. Choices are DISABLE, ENABLE, and ENABLE w/ NO ANSWER WINK. Default is DISABLE.

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

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

INTERFACES (FXS) > CONFIG > TANDEM > FWD DISC BATTERY
In Tandem mode, selects whether battery is to be removed or reversed during forward disconnect. Choices are REMOVE and REVERSE. Default is REMOVE.

INTERFACES (FXS) > STATUS
Displays the status of the FXS signal bits.

INTERFACES (FXS) > STATUS > SLOT
Displays the slot number associated with the installed FXS Module.

INTERFACES (FXS) > STATUS > PORT
Displays the port number.

INTERFACES (FXS) > STATUS > TA SIG
This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXS) > STATUS > TB SIG
This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXS) > STATUS > RA SIG
This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

INTERFACES (FXS) > STATUS > RB SIG
This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.
**INTERFACES (FXS) > TEST**
Activate tests and monitor test status on a per port basis from this menu.

**INTERFACES (FXS) > TEST > SLOT**
Displays the slot number for the installed FXS Module.

**INTERFACES (FXS) > TEST > PORT**
Displays the port number.

**INTERFACES (FXS) > TEST > TEST**
Choices are given below. Default is **NONE**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NONE</strong></td>
<td>Indicates that no test is currently active.</td>
</tr>
<tr>
<td><strong>DIGITAL NETWORK</strong></td>
<td>Used to loop back DS0 data coming from the network for each channel. Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit’s transmit time slot.</td>
</tr>
<tr>
<td><strong>LPBK</strong></td>
<td></td>
</tr>
<tr>
<td><strong>NETWORK ON HOOK TEST</strong></td>
<td>Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.</td>
</tr>
<tr>
<td><strong>NETWORK OFF HOOK TEST</strong></td>
<td>Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced off-hook while this test is active.</td>
</tr>
<tr>
<td><strong>1 KHZ TONE-NEAR END</strong></td>
<td>For Near End, the 2-wire side sends out a 1 kHz tone to verify talk path.</td>
</tr>
<tr>
<td><strong>1 KHZ TONE-FAR END</strong></td>
<td>For Far End, the tone side is sent out across the Network and can be heard if monitoring on the T1 as well as off of the Far End 2-wire side. This verifies talk path.</td>
</tr>
<tr>
<td><strong>CUSTOMER RING TEST</strong></td>
<td>The customer ring test will activate the unit’s ring relay in a 2-on /4-off cadence, providing ringing to the customer loop.</td>
</tr>
</tbody>
</table>

**INTERFACES (FXS) > TEST > TEST STATUS**
This option indicates whether a test is in progress.
**INTERFACES (FXO)**

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

**INTERFACES (FXO) > CONFIG**

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

**INTERFACES (FXO) > CONFIG > SLOT**

Displays the slot number of the installed FXO Module.

**INTERFACES (FXO) > CONFIG > PORT**

Indicates the port on which the FXO is installed.

**INTERFACES (FXO) > CONFIG > MODE**

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

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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LOOP START</strong></td>
<td>Sets the port to use FXO loop start signaling on the T-span and loop start supervision on the analog 2-wire interface.</td>
</tr>
<tr>
<td><strong>GROUND START</strong></td>
<td>Sets the port to use FXO ground start signaling on the T-span and ground start supervision on the analog 2-wire interface.</td>
</tr>
<tr>
<td><strong>DPO</strong></td>
<td>Sets the port to use Dial Pulse signaling to originate dialed numbers.</td>
</tr>
<tr>
<td><strong>MODIFIED DPT</strong></td>
<td>Sets the port to use DPT signaling on the interface. In DPT mode, digits are transmitted out the FXO interface to the user equipment. DPT mode is one-way operation only (outbound calls only).</td>
</tr>
</tbody>
</table>

**INTERFACES (FXO) > CONFIG > Tx (dB)**

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

**INTERFACES (FXO) > CONFIG > Rx (dB)**

Sets the RX direction level points. This signal will change the volume of the voice. A higher number indicates more attenuation which equals lower volume. The value entered must be less than 10 dB. Default is **0.0 dB**.
**INTERFACES (FXO) > Config > Svc Mode**
Indicates whether the module is **in Service** or **Out of Svc**. This does not indicate whether the port has been mapped. For proper operation, the port must be mapped using the **DS0 Maps** menu. Default is **In Service**.

**INTERFACES (FXO) > Status**
Displays the status of the FXO signal bits.

**INTERFACES (FXO) > Status > Slot**
Displays the slot number for the installed FXO Module.

**INTERFACES (FXO) > Status > Port**
Displays the port number.

**INTERFACES (FXO) > Status > TA Sig**
This parameter displays the status of the Transmit A signal bit. The high/low status is indicated by a 0 or 1.

**INTERFACES (FXO) > Status > TB Sig**
This parameter displays the status of the Transmit B signal bit. The high/low status is indicated by a 0 or 1.

**INTERFACES (FXO) > Status > RA Sig**
This parameter displays the status of the Receive A signal bit. The high/low status is indicated by a 0 or 1.

**INTERFACES (FXO) > Status > RB Sig**
This parameter displays the status of the Receive B signal bit. The high/low status is indicated by a 0 or 1.

**INTERFACES (FXO) > Test**
Activate tests and monitor test status on a per port basis from this menu.

**INTERFACES (FXO) > Test > Slot**
Displays the slot number for the installed FXO Module.

**INTERFACES (FXO) > Test > Port**
Displays the port number.
**INTERFACES (FXO) > TEST > TEST**
Choices are given below. Default is **NONE**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NONE</strong></td>
<td>Indicates that no test is currently active.</td>
<td></td>
</tr>
<tr>
<td><strong>DIGITAL NETWORK</strong></td>
<td>Used to loop back DS0 data coming from the network for each channel.</td>
<td></td>
</tr>
<tr>
<td><strong>LPBK</strong></td>
<td>Received data is latched in on the appropriate receive time slot on the receive bus. This data is then placed on the transmit bus in the unit’s transmit time slot.</td>
<td></td>
</tr>
<tr>
<td><strong>NETWORK ON HOOK</strong></td>
<td>Used to test signaling sent to the network by the unit. On-hook signaling is sent to the network. The customer loop is forced on-hook while this test is active.</td>
<td></td>
</tr>
<tr>
<td><strong>TEST</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NETWORK OFF HOOK</strong></td>
<td>Used to test signaling sent to the network by the unit. Off-hook signaling is sent to the network. The customer loop is forced off-hook while this test is active.</td>
<td></td>
</tr>
<tr>
<td><strong>1004 Hz - 0DCBM0 TONE GEN</strong></td>
<td>Used to verify talk path by sending out 1004 Hz tone to test across the network. Monitoring of the T1 as well as the Far-End 2-wire side verifies the talk path if the tone is heard.</td>
<td></td>
</tr>
</tbody>
</table>

**INTERFACES (FXO) > TEST > TEST STATUS**
This option indicates whether a test is in progress.

**INTERFACES (DSX-1 MODULE)**
View the DSX-1 Module interface status and configure the DSX-1 Module parameters from this menu.

**INTERFACES (DSX-1) > Config**
Configures the DSX-1 interface format and code from this menu.

**INTERFACE (DSX-1) > Config > Slot**
Indicates the slot in which the DSX-1 Module is installed.

**INTERFACE (DSX-1) > Config > Port**
Indicates the port on which the DXS is installed.

**INTERFACE (DSX-1) > Config > Format**
This setting must match the frame format of the circuit to which the interface is connected. Choices are **ESF** and **SF** (D4). Extended Superframe (ESF) provides a non-disruptive means of full-time monitoring on the facility data link (FDL). The default is **ESF**.
**INTERFACE (DSX-1) > CONFIG > LINE CODE**
This 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). The default is **B8ZS**.

**INTERFACES (DSX-1) > STATUS**
Displays the DSX-1 interface status including performance data and alarm histories.

**INTERFACES (DSX-1) > STATUS > ALARMS**
Displays current alarms and alarm history for the DSX-1 interface.

**INTERFACES (DSX-1) > STATUS > ALARMS > CURRENT ALARMS**
Displays the current alarms on the DSX-1 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 (DSX-1) > STATUS > ALARMS > ALARM HISTORY**
Displays the alarm history for the T1 interface. An asterisk in a field indicates that an alarm has occurred on the T1 interface since the last clear history. Refer to **Interfaces (DSX-1) > Status > Alarms > Current Alarms** for more details on listed alarm conditions.

**INTERFACES (DSX-1) > STATUS > ALARMS > CLEAR HISTORY**
Selecting this activator will clear the Alarm History for the T1 interface.

**INTERFACES (DSX-1) > TEST**
These options are used to initiate local and remote loopback tests and display the test status.

**INTERFACES (DSX-1) > TEST > SLOT**
Displays the slot number of the installed DSX-1 Module.

**INTERFACES (DSX-1) > 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 (DSX CARD) > TEST > TEST STATUS**
Indicates whether a test is in progress.
INTERFACES (UBR1TE MODULE)

View the UBR1TE Module interface status and configure the UBR1TE Module parameters from this menu.

INTERFACES (UBR1TE) > Config
Configures the UBR1TE interface format and code from this menu.

INTERFACE (UBR1TE) > Config > Slot
Indicates the slot in which the UBR1TE Module is installed.

INTERFACE (UBR1TE) > Config > Mode
Choices are LUNT, LUNT w/WakeUp, and LULT. The U-BR1TE port should be configured to operate in the LULT mode if being operated in the Adjacent to Customer or Tandem Office Source positions (see Figure 7). The MODE should be set to LUNT if the port is operated in the Adjacent to Switch or Tandem Office
Sink positions. Default is **LULT**.

**Figure 7. UBR1TE Network Configurations**

**INTERFACE (UBR1TE) > CONFIG > SERVICE**

Allows the user to select the ISDN channels transmitted over the T1 facility. Each channel requires one DS0 of the T1 in which to transmit and receive data. All switched applications will require the D channel. Choices are **2B+D**, **B1+D**, **B2+D**, **B1+B2**, **B1**, **B2**, and **D**. Default is **2B+D**.

> The user must provision the proper number of consecutive DS0s of the T1 facility for proper operation.

**INTERFACE (UBR1TE) > CONFIG > ZERO BYTE SUB**

For proper operation, the ZBS (zero byte substitution) for two U-BR1TE ports connected by a T1 facility must be the same value. The **ENABLE** parameter for ZBS must be selected if the T1 is using AMI line coding. If the T1 facility is using B8ZS line coding, the **DISABLE** parameter may be chosen. Default is **ENABLED**.
**INTERFACE (UBR1TE) > CONFIG > SEALING CURRENT**
DC sealing current is only applicable if the mode is **LULT**. Sealing current should be present for Adjacent-to-Customer applications. Default is **ENABLED**.

**INTERFACE (UBR1TE) > STATUS**
View the interface status information for the UBR1TE Module.

**INTERFACE (UBR1TE) > STATUS > SLOT**
Displays the slot number for the installed UBR1TE Module.

**INTERFACE (UBR1TE) > STATUS > ACT BIT**
This status field indicates whether an NT1 is communicating with the ISDN switch.

**INTERFACE (UBR1TE) > STATUS > LOOP**
Displays synchronization between the UBR1TE card and the NT1 on the loop side of the card. Sync displays **YES** or **NO**.

**INTERFACE (UBR1TE) > STATUS > CARRIER**
Displays synchronization between the ISDN switch and the UBR1TE card on the T1 network side. Sync displays **YES** or **NO**.

**INTERFACE (UBR1TE) > STATUS > RX LOOP CRC ERROR**
Indicates a CRC error has been received on the loop side of the card (indicating it came from the NT1).

**INTERFACE (UBR1TE) > STATUS > RX CARRIER CRC ERROR**
Indicates a CRC error has been received on the carrier side of the card (indicating it came from the ISDN switch).

**INTERFACE (UBR1TE) > STATUS > TEST STATUS**
Indicates whether a test is in progress.

**INTERFACE (UBR1TE) > TEST**
These options are used to initiate tests.

**INTERFACE (UBR1TE) > TEST > SLOT**
Displays the slot number for the installed UBR1TE Module.

**INTERFACE (UBR1TE) > TEST > B1 TEST**
Initiates a test on the first B channel (B1) of the ISDN circuit. The following tests are available:

| None       | No active test. |
LEASED MODE TESTING (INITIATED BY THE NETWORK; NOT A MENU OPTION)

For leased mode applications, the D channel is typically disabled on the UBR1TE. Without the D channel, standard ISDN loopbacks by way of the EOC are not available across the T1 carrier system. For this situation, the UBR1TE responds to independent network-issued OCU and CSU latching loopback sequences for B1 and B2, when configured as Adjacent-to-Customer. Upon receipt of an OCU latching loopback sequence, the UBR1TE initiates a bilateral loopback for the B channel under test. Upon receipt of a CSU latching loopback sequence, and provided the U-interface is terminated by an NT1/TA, the UBR1TE issues an EOC NT1 loopback for the appropriate B channel. In both tests of the OCU and the CSU loopbacks, the other B channel is not affected. The UBR1TE supports simultaneously testing both B channels. The OCU and CSU latching loopbacks are enabled by the following:

<table>
<thead>
<tr>
<th>ADDR1 (LOCAL LPBK)</th>
<th>Loopbacks in the Network-to-Customer direction initiate from either the ISDN switch or the test menus. If a DS0 digital test set is connected to the bantam connector on the front of the module, data from the test set provides the 64 kbps test pattern used in testing B1 or B2. If no test set is connected, an internally generated 2074 test pattern is used. When initiating loopbacks from the UBR1TE Module, the downstream direction is automatically selected based on the card position in the network. These tests are only valid for the Adjacent-to-Customer circuit position. Use ADDR2 to test an ADTRAN U-Repeater deployed from the UBR1TE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDR2</td>
<td>TX INTO CARRIER</td>
</tr>
<tr>
<td>ADDR3</td>
<td>TX INTO LOOP</td>
</tr>
<tr>
<td>ADDR4</td>
<td>BILATERAL LPBK</td>
</tr>
<tr>
<td>NT1</td>
<td>TX INTO CARRIER</td>
</tr>
<tr>
<td></td>
<td>TX INTO LOOP</td>
</tr>
</tbody>
</table>

TX INTO CARRIER A point-to-point (straight-away) test initiated toward the T1 carrier interface. The internal 2047 test pattern generator is used to verify the performance of the bearer channel. This test is valid for all network configurations.

TX INTO LOOP A point-to-point (straight-away) test initiated toward the U-interface. The internal 2047 test pattern generator is used to verify the performance of the bearer channel. This test is valid for all network configurations.

BILATERAL LPBK Loops toward both the U-interface and the T1 carrier network.
Upon receipt of an OCU latching loopback, the UBR1TE provides a bilateral loopback on the bearer channel that received the loopback sequence. The other bearer channel is not affected during this loopback.

Upon receipt of a CSU latching loopback sequence in either B1 or B2 channels and the U-interface is in sync, the UBR1TE issues an EOC loopback request to the NT1 for the appropriate channel. If the U-interface is not in sync, the UBR1TE sends abnormal station (*0011110) in both B1 and B2 channels.

For a UBR1TE in a CSU latching loopback, receipt of the 35 TIPs will release the test in progress, following the release code to a UBR1TE in a CSU test, the UBR1TE issues a Return-To-Normal EOC message to the NT1/TA.

**INTERFACE (UBR1TE) > TEST > B2 TEST**

Initiates a test on the first B channel (B1) of the ISDN circuit. Refer to *Interface (UBR1TE) > Test > B1 Test* on page 113 for more details on available tests.
L2 PROTOCOL (T1 TDM Firmware)

Use the L2 protocol menu to select the L2 protocol, configure the protocol specific parameters and view the status as shown in Figure 8. The following menus are for Total Access 850 systems using T1 TDM firmware.

![Figure 8. L2 Protocol (T1 TDM) Menu](image)

For convenience, the following heading notations identify the type of firmware and L2 protocol configured in the Total Access 850 system:

- **L2 Protocol (T1 TDM – T1 – PPP)**
  - Firmware and RCU type. (For example, T1 TDM, T1 ATM, SDSL.)
  - Interface type. (For example, T1, Ethernet, etc.)
  - Configured Layer 2 protocol. (For example, PPP, FRE, Auto, etc.)
L2 PROTOCOL (T1 TDM Firmware) – T1 Interface

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

**L2 Protocol (T1 TDM – T1) > Protocol**

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

**L2 Protocol (T1 TDM – T1) > Protocol > PPP**

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

**L2 Protocol (T1 TDM – T1) > Protocol > FRE**

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

**L2 Protocol (T1 TDM – T1) > Protocol > HDLC**

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

**L2 Protocol (T1 TDM – T1) > Protocol > Auto**

Setting the **L2 Protocol** to **Auto** allows the unit to automatically detect the **L2 Protocol** from the network.

---

*Note: The L2 Protocol must be set to Auto in order to use the Auto-config feature.*
L2 PROTOCOL (T1 TDM Firmware) – T1 Interface > PPP

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

L2 Protocol (T1 TDM–T1–PPP) > Config

Configure the L2 Protocol parameters for the T1 interface using PPP protocol.

L2 Protocol (T1 TDM–T1–PPP) > Config > Mode

Select the L2 Protocol mode. Choices are Route IP, Bridge All, and Route IP/Bridge Other. The default is Route IP.

L2 Protocol (T1 TDM–T1–PPP) > Config > Authentication

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

L2 Protocol (T1 TDM–T1–PPP) > Config > Authentication > Tx Method

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

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

L2 Protocol (T1 TDM–T1–PPP) > Config > PPP

Configure the PPP specific parameters such as Max Config, Max Timer, Max Failure, and Force Peer IP Address from this menu.

L2 Protocol (T1 TDM–T1–PPP) > Config > PPP > Max Config

This value is the number of unanswered configuration-requests that should be transmitted before resetting PPP negotiations. The possible values are 5, 10, 15 and 20 (def).
L2 Protocol (T1 TDM–T1–PPP) > Config > PPP > Max Timer (Sec)
This value is the numbers of seconds to wait between unanswered configuration-requests. The possible values are 1 Sec, 2 Secs, 3 Secs (def), 5 Secs, and 10 Secs.

L2 Protocol (T1 TDM–T1–PPP) > Config > PPP > Max Failure
Due to the nature of PPP, configuration options may not be agreed upon between two PPP peers. This value is the number of configuration-naks that should occur before an option is configuration-rejected. The possible values are 5 (def), 10, 15, and 20.

L2 Protocol (T1 TDM–T1–PPP) > Config > PPP > Keepalive Period
This option allow the user to generate PPP keepalive packets that can be sent one every 1 minute, 2 minutes or every 5 minutes. A value of 0 (def) disables the PPP keepalive packet generating feature.

L2 Protocol (T1 TDM–T1–PPP) > Config > PPP > Force Peer IP Address
This option forces the PPP to negotiate the IP address entered instead of allowing the IP address to be assigned by the remote end.

L2 Protocol (T1 TDM–T1–PPP) > Config > PPP > Send Identification
When enabled, this option enables the Total Access 850 to send the system identification code in response to a configure acknowledgement from the peer equipment. For most peer routers this option should be configured as Yes. If set to No, the Total Access 850 will accommodate peer routers that do not correctly respond to the identification code.

L2 Protocol (T1 TDM–T1–PPP) > Status
View the L2 Protocol status for the T1 interface using the PPP protocol.

L2 Protocol (T1 TDM–T1–PPP) > Status > LCP
Link Control Protocol. Reflects the LCP layer active.

L2 Protocol (T1 TDM–T1–PPP) > Status > BCP
Shows UP if PPP Bridge Control Protocol has negotiated successfully.

L2 Protocol (T1 TDM–T1–PPP) > Status > IPCP
Shows UP if PPP IP Control Protocol has negotiated successfully.

L2 Protocol (T1 TDM–T1–PPP) > Status > Up Time
Displays how long the PPP session has been connected.

L2 Protocol (T1 TDM–T1–PPP) > Status > Tx Pkts
Number of packets transmitted on the T1 interface.
L2 Protocol (T1 TDM–T1–PPP) > Status > Rx Pkts
Number of packets received on the T1 interface.

L2 Protocol (T1 TDM–T1–PPP) > Status > Tx Bytes
Number of bytes transmitted on the T1 interface.

L2 Protocol (T1 TDM–T1–PPP) > Status > Rx Bytes
Number of bytes received on the T1 interface.

L2 Protocol (T1 TDM–T1–PPP) > Status > Current Util (b/s)
Current utilization of the T1 interface bandwidth presented in bits per second.

L2 Protocol (T1 TDM–T1–PPP) > Status > Current Util (%)
Current utilization of the T1 interface bandwidth presented in percentage format.

L2 Protocol (T1 TDM–T1–PPP) > Status > Average Util (b/s)
Average utilization of the T1 interface bandwidth (since the last stats reset) presented in bits per second.

L2 Protocol (T1 TDM–T1–PPP) > Status > Average Util (%)
Average utilization of the T1 interface bandwidth (since the last stats reset) presented in percentage format.

L2 Protocol (T1 TDM–T1–PPP) > Status > Tx Pkts
Number of packets transmitted on the T1 interface

L2 Protocol (T1 TDM–T1–PPP) > Status > Clear Stats
Clears the PPP stats (returning the counters to 0) for the T1 interface.
L2 PROTOCOL (T1 TDM Firmware) – T1 Interface > FRE Protocol

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

L2 Protocol (T1 TDM–T1–FRE) > Config

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

L2 Protocol (T1 TDM–T1–FRE) > Config > Maintenance Protocol

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

- **Annex D (ANSI)**
  This ANSI standard ANSI T1.617-D and is the most commonly used in the United States.

- **Annex A (Q933A)**
  This is the CCITT European standard, ITU-T Q.933-A.

- **LMI**
  This was developed by a vendor consortium and is also known as the “Consortium” management interface specification. It is still used by some carriers in the United States.

- **Static (No Sig)**
  This should be selected when there is no Frame Relay switch in the circuit. The DLCIs are assigned in the DLCI Mapping and must be the same for the device it will communicate with.

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

L2 Protocol (T1 TDM–T1–FRE) > Config > Polling Frequency (5-30)

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

L2 Protocol (T1 TDM–T1–FRE) > Config > DLCI Mapping

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

When empty and a maintenance protocol other than the static is used, the unit will poll the switch to determine which DLCIs are active. 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 TDM–T1–FRE) > CONFIG > DLCI MAPPING > NUM**
Displays the index number in the DLCI mapping table.

**L2 PROTOCOL (T1 TDM–T1–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 TDM–T1–FRE) > CONFIG > DLCI MAPPING INTERFACE**
Shows the user the physical and logical port associated with each DLCI. This is a read-only field.

**L2 PROTOCOL (T1 TDM–T1–FRE) > CONFIG > DLCI MAPPING > DLCI**
This DLCI (Data Link Connection Identifier) number identifies the virtual circuit being configured.

**L2 PROTOCOL (T1 TDM–T1–FRE) > CONFIG > DLCI MAPPING > MODE**
The mode identifies how the data will be forwarded. The choices are:

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

**L2 PROTOCOL (T1 TDM–T1–FRE) > CONFIG > DLCI MAPPING > BECN TIMEOUT (MSEC)**
This value is expressed in milliseconds and represents the amount of time the unit will stop transmitting over a PVC which received a packet with the BECN bit set. Range is **50-5000** msec; the default is **50 MILLISECONDS**.

**L2 PROTOCOL (T1 TDM–T1–FRE) > STATUS**
View the L2 protocol status for the T1 interface using the Frame Relay protocol.
L2 Protocol (T1 TDM-T1-FRE) > Status > Port
View the Frame Relay statistics on the WAN port.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Port Index
Integer used for identifying DLCIs on an interface. A single DLCI will always be port index 0. Subsequent DLCIs will have incrementing port indices.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Signal State
Displays “up” when the unit is communicating with the Frame Relay switch; otherwise displays “down”.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Tx Frames
Total frames transmitted out the WAN port.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Rx Frames
Total frames received from the WAN port.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Tx Bytes
Total bytes transmitted out the WAN port.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Rx Bytes
Total bytes received on the WAN port.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Current Util (b/s)
Current utilization of the T1 interface bandwidth presented in bits per second.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Current Util (%)
Current utilization of the T1 interface bandwidth presented in percentage format.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Average Util (b/s)
Average utilization of the T1 interface bandwidth (since the last stats reset) presented in bits per second.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Average Util (%)
Average utilization of the T1 interface bandwidth (since the last stats reset) presented in percentage format.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Full Status Tx Frames
Number of full status frames transmitted out the WAN port.

L2 Protocol (T1 TDM-T1-FRE) > Status > Port > Full Status Rx Frames
Number of full status frames received on the WAN port.
L2 Protocol (T1 TDM–T1–FRE) > Status > Port > Link Integrity Status Tx Frames
Number of Link-Integrity (LI) only frames transmitted out the WAN port.

L2 Protocol (T1 TDM–T1–FRE) > Status > Port > Link Integrity Status Rx Frames
Number of LI only frames received on the WAN port.

L2 Protocol (T1 TDM–T1–FRE) > Status > Port > Drop Unknown DLCI
Number of frames received that were not associated with any known PVC.

L2 Protocol (T1 TDM–T1–FRE) > Status > Port > Drop Invalid DLCI
Number of frames received that had illegal DLCIs.

L2 Protocol (T1 TDM–T1–FRE) > Status > Port > Clear Stats
Selecting this activator will clear the port Frame Relay Statistics.

L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s)
View the Frame Relay status on a per PVC basis.

L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > DLCI
The DLCI number identifies the virtual circuit being monitored.

L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > State
The state of the virtual circuit:

- **Inactive**: The circuit exists but has been deactivated by the Frame Relay switch.
- **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 TDM–T1–FRE) > Status > PVC(s) > Tx Frames
Number of Frame Relay packets that have been transmitted via this DLCI.

L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > Rx Frames
Number of Frame Relay packets that have been received via this DLCI.

L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > Tx Bytes
Number of Frame Relay bytes that have been transmitted via this DLCI.
**L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > Rx Bytes**
Number of Frame Relay bytes that have been received via this DLCI.

**L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > DE Count**
Number of packets received on this DLCI with the Discharge Eligible (DE) bit set.

**L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > CR Count**
Number of packets received on this DLCI with the Command Response (CR) bit set.

**L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > BECN Count**
Number of packets received on this DLCI with the Backward Explicit Congestion Notification (BECN) bit set.

**L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > FECN Count**
Number of packets received on this DLCI with the Forward Explicit Congestion Notification (FECN) bit set.

**L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > Unknown Frame Rx**
Number of frames that have been received that the unit does not know where to route.

**L2 Protocol (T1 TDM–T1–FRE) > Status > PVC(s) > Clear Stats**
Clears all gathered statistics for this interface and returns counters to 0.

---

**L2 Protocol (T1 TDM Firmware) – T1 Interface > HDLC Protocol**

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

**L2 Protocol (T1 TDM–T1–HDLC) > Status**
View the status of traffic flow and utilization for the T1 interface with an L2 Protocol set to HDLC.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > Tx Pkts**
Number of packets transmitted on the T1 interface.
**L2 Protocol (T1 TDM–T1–HDLC) > Status > RxPkts**
Number of packets received on the T1 interface.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > TxBytes**
Number of bytes transmitted on the T1 interface.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > RxBytes**
Number of bytes received on the T1 interface.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > Current Util (b/s)**
Current utilization of the T1 interface bandwidth presented in bits per second.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > Current Util (%)**
Current utilization of the T1 interface bandwidth presented in percentage format.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > Average Util (b/s)**
Average utilization of the T1 interface bandwidth (since the last stats reset) presented in bits per second.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > Average Util (%)**
Average utilization of the T1 interface bandwidth (since the last stats reset) presented in percentage format.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > TxPkts**
Number of packets transmitted on the T1 interface.

**L2 Protocol (T1 TDM–T1–HDLC) > Status > Clear Stats**
Clears all the gathered statistics for this interface and returns the counters to 0.

**L2 Protocol (T1 TDM Firmware) – T1 Interface > Auto Protocol**

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

**L2 Protocol (T1 TDM–T1–Auto) > Status**

View the status of the auto detect function and traffic flow for the T1 interface with an L2 Protocol set to Auto.
L2 PROTOCOL (T1 TDM–T1–AUTO) > Status > State

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

- **Off**: The T1 interface is down, so the auto-detect/configuration process is currently idle.
- **Detecting L2 Protocol**: The T1 interface is up and waiting for the first control/signaling packet.
- **Confirment 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.
- **Confirment 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 TDM–T1–AUTO) > Status > Tx Pkts

Number of packets transmitted out of the WAN port.

L2 PROTOCOL (T1 TDM–T1–AUTO) > Status > Rx Pkts

Number of packets received on WAN port.

L2 PROTOCOL (T1 TDM–T1–AUTO) > Status > Tx Bytes

Number of bytes transmitted out of the WAN port.

L2 PROTOCOL (T1 TDM–T1–AUTO) > Status > Rx Bytes

Number of bytes received out of the WAN port.

L2 PROTOCOL (T1 TDM–T1–AUTO) > Status > Clear Stats

Clears all the gathered statistics for this interface and returns the counters to 0.
L2 PROTOCOL (T1 ATM FIRMWARE)

Use the L2 PROTOCOL menu to select the L2 PROTOCOL, configure the protocol specific parameters, and view the status as shown in Figure 8. The following menus are for Total Access 850 systems using T1 ATM firmware.

![Figure 9. L2 Protocol (T1 TDM) Menu](image_url)

For convenience, the following heading notations identify the type of firmware and L2 protocol configured in the Total Access 850 system:

**L2 Protocol (T1 ATM – T1 – ATM)**

- Firmware and RCU type. (For example, T1 TDM, T1 ATM, SDSL.)
- Interface type. (For example, T1, Ethernet, etc.)
- Configured Layer 2 protocol. (For example, ATM or CuMTN.)
L2 PROTOCOL (T1 ATM FW) – T1 INTERFACE

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

L2 PROTOCOL (T1 ATM – T1) > PROTOCOL


L2 PROTOCOL (T1 ATM – T1) > PROTOCOL > ATM

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

L2 PROTOCOL (T1 ATM – T1) > PROTOCOL > CuMTN

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

L2 PROTOCOL (T1 ATM FW) – T1 INTERFACE > ATM

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

L2 PROTOCOL (T1 ATM–T1–ATM) > Config

Configure the L2 Protocol parameters for the T1 interface using ATM protocol.

L2 PROTOCOL (T1 ATM–T1–ATM) > Config > ATM Config

Use the ATM Config menu to set the parameters listed below.

L2 PROTOCOL (T1 ATM–T1–ATM) > Config > ATM Config > Idle Cells

The Idle Cells format must be configured for either ATM Forum (Unassigned) or ITU (Idle). Configuring this setting incorrectly for a particular circuit will cause poor performance at the ATM Layer. The default is ATM Forum (Unassigned).
**L2 Protocol (T1 ATM–T1–ATM) > Config > ATM Config > Data Scrambling**

Data Scrambling can be Enabled or Disabled for cell traffic. Configuring this setting incorrectly for a particular circuit will cause poor performance at the ATM Layer.

*NOTE*

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

**L2 Protocol (T1 ATM–T1–ATM) > Config > ATM Config > HEC Coset**

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

**L2 Protocol (T1 ATM–T1–ATM) > Config > PVC Config**

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

*NOTE*

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

*NOTE*

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

**L2 Protocol (T1 ATM–T1–ATM) > Config > PVC Config > Num**

Displays the index number for the PVC entry.

**L2 Protocol (T1 ATM–T1–ATM) > Config > PVC Config > Active**

Activates the ATM PVC. The choices are Yes or No. Default is No.

**L2 Protocol (T1 ATM–T1–ATM) > Config > PVC Config > Sub-Interface**

The T1 Sub-Interface is ATM [0.0] that represents the T1 physical and logical ports respectively. This is a read-only field.

**L2 Protocol (T1 ATM–T1–ATM) > Config > PVC Config > VPI**

ATM Virtual Path Identifier located in the ATM cell header identifies the virtual path over which this port is running. The range is 0-256. The default is 0.
L2 PROTOCOL (T1 ATM–T1–ATM) > CONFI G > PVC CONFI G > VCI
This is the ATM Virtual Channel Identifier that serves as an address for the virtual channel cell transmissions between two devices. The range is 0-65355. The default setting is 38.

L2 PROTOCOL (T1 ATM–T1–ATM) > CONFI G > PVC CONFI G > CONNECTION
Select the physical and logical method of data transfer over the virtual path. There are three valid connection entries: ROUTER, V35, and VOICE. Select ROUTER to connect traffic from this PVC to the Total Access 850 integral IP router. Select V35 to connect traffic from this PVC to a V.35 interface on the system. Select VOICE to connect traffic from this PVC to a voice connection (on a DSX-1 or FXS interface).

L2 PROTOCOL (T1 ATM–T1–ATM) > CONFI G > PVC CONFI G > SETUP (ROUTER)
Use these menus to configure the router parameters for this logical connection from the router to the T1 interface. These menus are only applicable when the CONNECTION parameter is set to ROUTER.

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

CONNECTION (ROUTER) > SETUP > MODE
Identifies how the data will be transferred through the Total Access 850 system. The following choices are available:
- ROUTE IP (def) – All IP data for this PVC is routed through the Total Access 850 integral router.
- BRIDGE ALL – All data for this PVC is bridged through the Total Access 850 system.
- ROUTE IP/BRIDGE OTHER – All IP data for this PVC is routed through the Total Access 850 integral router and all other data is bridged through the system.

CONNECTION (ROUTER) > SETUP > PPP SETUP
Provides PPP configuration parameters for the PVC. These menus are only visible when the MODE is set to PPP.

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

Specifies the method the Total Access 850 uses to obtain PPP authentication from the peer. There are four possible selections:

- **NONE**  
  The connection will not allow the PPP peer to authenticate it.

- **PAP, CHAP, OR EAP**  
  The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** or **PAP**.

- **CHAP OR EAP**  
  The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** but not **PAP**.

- **EAP ONLY**  
  The unit will only allow **EAP** to be negotiated. If the PPP peer is not capable of doing **EAP**, then the connection will not succeed.

- **PAP ONLY**  
  The unit will only allow **PAP** to be negotiated. If the PPP peer is not capable of doing **PAP**, then the connection will not succeed.

**RX METHOD**

Specifies the method the Total Access 850 uses to authenticate the PPP peer. There are four possible selections:

- **NONE**  
  The connection will not allow the PPP peer to authenticate it.

- **PAP, CHAP, OR EAP**  
  The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** or **PAP**.

- **CHAP OR EAP**  
  The unit will ask for **EAP** during the first PPP LCP negotiation and allow the PPP peer to negotiate down to **CHAP** but not **PAP**.

- **EAP ONLY**  
  The unit will only allow **EAP** to be negotiated. If the PPP peer is not capable of doing **EAP**, then the connection will not succeed.

- **PAP ONLY**  
  The unit will only allow **PAP** to be negotiated. If the PPP peer is not capable of doing **PAP**, then the connection will not succeed.

**PPP**

Configure the PPP specific parameters such as **MAX CONFIG**, **MAX TIMER**, **MAX FAILURE**, and **FORCE PEER IP ADDRESS** from this menu.
**MAX CONFIG**
This value is the number of unanswered configuration-requests that should be transmitted before resetting PPP negotiations. The possible values are 5, 10, 15, and 20 (def).

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

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

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

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

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

**L2 PROTOCOL (T1 ATM–T1–ATM) > CONFIG > PVC CONFIG > SETUP (V35)**
Use these menus to configure the V35 parameters for this logical connection from the T1 interface to the V.35 port. These menus are only applicable when the CONNECTION parameter is set to V35.

**CONNECTION (V35) > SETUP > SETUP**
Use these menus to configure the Protocol mapping, DE map, and FECN map for the V.35 PVC connections.
Connection (V35) > Setup > Setup > Protocol Mapping

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

Connection (V35) > Setup > Setup > DE Map

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

Connection (V35) > Setup > Setup > FECN Map

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

Connection (V35) > Setup > DLCI Mapping

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

Connection (V35) > Setup > DLCI Mapping > Map

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

Connection (V35) > Setup > DLCI Mapping > Active

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

Connection (V35) > Setup > Setup > Interface

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

L2 Protocol (T1 ATM–T1–ATM) > Config > PVC Config > Setup (Voice)

Use these menus to configure the voice parameters for this logical connection from the T1 interface to the DSX-1 of FXS port being used as a voice interface. These menus are only applicable when the Connection parameter is set to Voice.
**Connection (Voice) > Setup > Call Control**

The Call Control setting is used to configure the correct Voice Gateway protocol for voice signaling control between the Total Access 850 and the configured Gateway. The **Call Control** setting must be configured correctly before the voice circuits will work correctly. The Total Access 850 supports Jetstream, Coppercom, Tollbridge, and LES-CAS. The default is LES-CAS.

**Connection (Voice) > Setup > LES Profile**

This options applies when **Call Control** is set to **LES-CAS**. The choices are **ITU Profile 1**, **ATM Forum Profile 9**, and **ATM Forum Profile 10**. The default is **ATM Forum Profile 10**.

**ATM Forum Profile 9** provides ability to support 64 kbps PCM calls. **ATM Forum Profile 10** enables support of 64 Kbps PCM calls as well as 32 kbps ADPCM calls.

**Connection (Voice) > Setup > LES-CAS GW Sim**

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

**L2 Protocol (T1 ATM–T1–ATM) > Config > PVC Config > QOS**

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

**QOS > Quality of Service**

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

**QOS > Peak Cell Rate**

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

\[
\text{Peak Cell Rate} = \frac{\text{Bit Rate}}{424}
\]

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

**L2 Protocol (T1 ATM–T1–ATM) > Status**

Displays all available ATM statistics (both overall and PVC-specific).
L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > ATM STATUS
Displays overall ATM link performance statistics. The following statistics are available:

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

L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > ATM STATUS > CLEAR STATS
Clears all ATM statistics contained in the ATM status field and returns all counters to 0.

L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > PVC STATUS
View the ATM PVC statistics from this menu.

L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > PVC STATUS > NUM
Displays the index number in the PVC Status menu.
L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > PVC STATUS > SUB-INTERFACE

The T1 SUB-INTERFACE is ATM[0.0], representing the T1 physical and logical ports, respectively. This is a read-only field.

L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > PVC STATUS > AAL STATS

Shows the statistics of ATM Adaptation Layer frames.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAX PDU SIZE</strong></td>
<td>Maximum Protocol Data Unit size for the ATM AAL5 frame. All data information larger than the PDU must be transmitted in multiple frames.</td>
</tr>
<tr>
<td><strong>TX DATA BYTES</strong></td>
<td>Number of AAL5 data bytes transmitted.</td>
</tr>
<tr>
<td><strong>TX FRAMES</strong></td>
<td>Number of AAL5 frames transmitted.</td>
</tr>
<tr>
<td><strong>TX CELLS (ALL TYPES)</strong></td>
<td>Total number of AAL5 cells transmitted (all types).</td>
</tr>
<tr>
<td><strong>TX OAM CELLS</strong></td>
<td>Number of AAL5 Operations, Administration, and Maintenance cells transmitted.</td>
</tr>
<tr>
<td><strong>TX RM CELLS</strong></td>
<td>Number of AAL5 Resource Management cells transmitted.</td>
</tr>
<tr>
<td><strong>TX EFCI=1 CELLS</strong></td>
<td>Number of AAL5 EFCI=1 cells transmitted.</td>
</tr>
<tr>
<td><strong>TX CLPI=1 CELLS</strong></td>
<td>Number of AAL5 CLPI=1 transmitted.</td>
</tr>
<tr>
<td><strong>RX DATA BYTES</strong></td>
<td>Number of AAL5 data bytes received.</td>
</tr>
<tr>
<td><strong>RX FRAMES</strong></td>
<td>Number of AAL5 frames received.</td>
</tr>
<tr>
<td><strong>RX USER CELLS</strong></td>
<td>Number of AAL5 user cells received.</td>
</tr>
<tr>
<td><strong>RX OAM CELLS</strong></td>
<td>Number of AAL5 OAM cells received.</td>
</tr>
<tr>
<td><strong>RX BAD OAM CELLS</strong></td>
<td>Number of AAL5 Bad OAM cells received.</td>
</tr>
<tr>
<td><strong>RX RM CELLS</strong></td>
<td>Number of AAL5 RM cells received.</td>
</tr>
<tr>
<td><strong>RX BAD RM CELLS</strong></td>
<td>Number of AAL5 Bad RM cells received.</td>
</tr>
<tr>
<td><strong>RX EFCI=1 CELLS</strong></td>
<td>Number of AAL5 EFCI=1 cells received.</td>
</tr>
<tr>
<td><strong>RX CLPI=1 CELLS</strong></td>
<td>Number of AAL5 CLPI=1 cells received.</td>
</tr>
<tr>
<td><strong>DISCARD RX CELLS</strong></td>
<td>Number of AAL5 RX cells which were discarded.</td>
</tr>
<tr>
<td><strong>DISCARD RX FRAMES</strong></td>
<td>Number of AAL5 RX frames which were discarded.</td>
</tr>
<tr>
<td><strong>DISCARD TX FRAMES</strong></td>
<td>Number of AAL5 TX frames which were discarded.</td>
</tr>
<tr>
<td><strong>TX QUEUE OVERFLOW</strong></td>
<td>Number of cells discarded due to queue overflow.</td>
</tr>
<tr>
<td><strong>TX OUT OF CELLS</strong></td>
<td>Number of AAL5 TX Out of Cells.</td>
</tr>
<tr>
<td><strong>TX INACTIVE</strong></td>
<td>Number of TX frames discarded while PVC is inactive.</td>
</tr>
<tr>
<td><strong>RX INACTIVE</strong></td>
<td>Number of RX frames discarded while PVC is inactive.</td>
</tr>
<tr>
<td><strong>CRC ERRORS</strong></td>
<td>Number of AAL5 CRC Errors.</td>
</tr>
<tr>
<td><strong>REASSEMBLY TIMEOUTS</strong></td>
<td>Number of AAL5 Reassembly Timeouts.</td>
</tr>
<tr>
<td><strong>TOO LONG FRAMES</strong></td>
<td>Number of AAL5 Too Long Frames.</td>
</tr>
<tr>
<td><strong>CLEAR COUNTS</strong></td>
<td>Clears all recorded statistics and returns all counters to 0.</td>
</tr>
</tbody>
</table>
L2 PROTOCOL (T1 ATM–T1–ATM) > STATUS > PVC STATUS > PROTOCOL STATUS

Use these menus to view the AAL2 STATS, POTS STATS, and to CLEAR STATS for the PVC Protocol.

**AAL2 Stats**

ATM Adaptation Layer 2 statistics is used to provide error information on voice traffic. This menu displays **RX AAL2 HEC ERRORS**, **RX AAL2 SEQK ERRORS**, **RX VOICE SEQ ERRORS**, **RX VOICE BAD CID**, **RX VOICE BAD UUI**, **RX VOICE EOC CELLS**, and **Peak Cell Rate**.

**RX AAL2 HEC ERRORS**

A CRC code (used for data integrity checks) is contained in the last byte of an AAL2 header. A received HEC error could result in dropped packets and poor voice quality.

**RX AAL2 SEQK ERRORS**

A single bit of the AAL2 header is used as a sequence bit and toggles from 1 to 0 with each successive transmitted cell. If two cells are received back to back with the same sequence bit, a sequence error is denoted.

**RX VOICE SEQ ERRORS**

Indicates that the Total Access 850 received voice packets that were out of sequence according to the voice sequencing bits. The Total Access 850 does not drop these packets, but the error is logged because invalid sequence numbers were received.

**RX VOICE BAD CID**

Indicates that the channel identifier (used for identifying voice calls in the ATM cell) was not valid.

**RX VOICE BAD UUI**

The User Indication designates the signaling bit pattern for PCM/ADPCM and identifies the packet as Type 1 (voice) or Type 3 (signaling). This error indicates the Total Access 850 received an incorrectly formatted UUI.

**RX VOICE EOC CELLS**

Indicates an EOC cell was received with a voice designation.

**Peak Cell Rate**

Indicates the number of times (since the last statistics reset) that the PVC has reached the peak cell rate.
**POTS Stats**

Selecting this menu options will show real-time indication status of each voice port on the Total Access 850. On a per port basis, the user can determine which ports are active/inactive as well as view other statistics like **TxQ**, **Inserts** and **Drops indicators**.

---

**NOTE**

*The Echo Canceller module ADPCM functionality automatically shifts ON/OFF when fax or modem calls are placed. To find out the current status of the Echo Canceller functionality, check the current status of each FXS port. The path of the current status can be found at the following path: L2 Protocol > Status > PVC Status > Protocol Status > POTS Stats > Coding Type (this will display either PCM or ADPCM).*

---

**TxQ**

Displays the numbers of cells waiting in the buffer to transmit out the POTS port. Buffering voice cells is used to minimize jitter.

---

**Inserts**

Displays the number of cells the Total Access 850 inserted on the analog interface to keep the current voice call connected when the network is idle.

---

**Drops**

Displays the number of voice cells the Total Access 850 dropped due to a full buffer. This indicates that the network is sending traffic faster than the Total Access 850 is anticipating receiving cells; thus overrunning the jitter buffer. Excess drops could result in a timing mismatch.

---

**Clear Stats**

Clears all recorded statistics and returns all counters to 0.

---

**L2 Protocol (T1 ATM Firmware) – T1 Interface > CuMTN**

Configure the **L2 Protocol** parameters and view the status of the T1 interface using Copper Mountain Frame Relay protocol from this menu.
L2 PROTOCOL (T1 ATM–T1–CuMTN) > CONFIG

Configure the L2 Protocol parameters for the T1 interface using Copper Mountain Frame Relay protocol.

**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 ATM–T1–CuMTN) > CONFIG > NUM

Displays the index number in the DLCI config table. The number range is 0-9.

---

L2 PROTOCOL (T1 ATM–T1–CuMTN) > CONFIG > ACTIVE

When this parameter is set to YES (def), the mapping is used to determine the protocols used. If set to NO, the unit will ignore the virtual circuit with this DLCI.

---

L2 PROTOCOL (T1 ATM–T1–CuMTN) > CONFIG > INTERFACE

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

---

L2 PROTOCOL (T1 ATM–T1–CuMTN) > CONFIG > DLCI

The DLCI (Data Link Connection Identifier) number identifies the virtual circuit being configured. The DLCI range is 16-1023. The default is 16-25 corresponding to the index numbers 0-9 respectfully.

---

L2 PROTOCOL (T1 ATM–T1–CuMTN) > CONFIG > CONNECTION

Select the physical and logical method of data transfer over the virtual path. There are two valid connection entries: ROUTER and VOICE. Select ROUTER to connect traffic from this PVC to the Total Access 850 integral IP router. Select VOICE to connect traffic from this PVC to a voice connection (normally an FXS interface).

---

L2 PROTOCOL (T1 ATM–T1–CuMTN) > CONFIG > SETUP

This submenu only appears for VOICE connections. Configure the CALL CONTROL for voice gateway using this menu.

---

L2 PROTOCOL (T1 ATM–T1–CuMTN) > CONFIG > SETUP > CALL CONTROL

The CALL CONTROL setting is used to configure the correct Voice Gateway protocol for voice signaling control between the Total Access 850 and the configured Gateway. The Call Control setting must be configured correctly before the voice circuits will work correctly. The Total Access 850 supports JETSTREAM, COPPERCOM, TOLLBRIDGE and LES-CAS (def).
**L2 Protocol (T1 ATM–T1–CuMTN) > Status**
View the status of the Copper Mountain DLCI connections.

**L2 Protocol (T1 ATM–T1–CuMTN) > Status > Num**
Displays the index number for the Status menu entries.

**L2 Protocol (T1 ATM–T1–CuMTN) > Status > Sub-Interface**
The T1 Sub-Interface is CuMtn[0.0] when the L2 Protocol is set for CuMtn FRE. The [0.0] represents the T1 physical and logical ports respectively. This is a read-only field.

**L2 Protocol (T1 ATM–T1–CuMTN) > Status > DLCI State**
This is a read-only field that displays the live DLCI state.

**L2 Protocol (T1 ATM–T1–CuMTN) > Status > Protocol Status**
This is a read-only field that displays the live protocol status. Menu visible for physical and logical Voice ports only.

**L2 Protocol (T1 ATM–T1–CuMTN) > Status > Protocol Status > Pots Stats**
View the voice port activity and coding type.

**L2 Protocol (T1 ATM–T1–CuMTN) > Status > Protocol Status > Clear Stats**
Clears all recorded statistics for the interface and returns all counters to 0.

---

**L2 Protocol (T1 ATM Firmware) – V.35 Interface**
Configure the L2 Protocol parameters and view the status of the V.35 interface using items from this menu. The V.35 interface is only available when the configured T1 network protocol is ATM. Refer to L2 Protocol (T1 ATM Firmware) – T1 Interface > ATM on page 129.

**L2 Protocol (T1 ATM – V35) > Protocol**
Configure the L2 Protocol mode. Choices are FRF5 (def) and FRF8. Selecting FRF5 configures the interface for network interworking and should be used for Frame Relay over ATM applications. Selecting FRF8 configures the interface for service interworking allowing the Total Access 850 to make the translation between Frame Relay signaling on the V35 interface and ATM protocols on the network interface.

**L2 Protocol (T1 ATM – V35) > Config**
Configures the L2 Protocol parameters for either FRF5 or FRF8 signaling.
L2 PROTOCOL (T1 ATM – V35) > CONFIG > UNI MAINT PROTOCOL
Specifies the maintenance protocol or signaling protocol between the local V.35 port and the attached DTE port. The choices are ANNEX D (def), ANNEX A, LMI, and STATIC.

L2 PROTOCOL (T1 ATM – V35) > CONFIG > UNI POLL TIMEOUT T392 (5-30)
T392 for signaling protocol. This parameter has no meaning if the UNI MAINT PROTOCOL is set to STATIC (no signaling). The default setting is 10.

L2 PROTOCOL (T1 ATM – V35) > STATUS
Displays the L2 statistics for FRF5 or FRF8 operation.

L2 PROTOCOL (T1 ATM – V35) > STATUS > PORT
Displays statistics for all the PVCs configured on this port. The following statistics are available:

| PORT INDEX | Port number |
| SIGNAL State | Frame relay state |
| TX FRAMES | Number of frames transmitted |
| RX FRAMES | Number of frames received |
| TX BYTES | Number of bytes transmitted |
| RX BYTES | Number of bytes received |
| FULL STATUS TX FRAMES | Number of Frame Relay signaling packets transmitted out the port |
| FULL STATUS RX FRAMES | Number of Frame Relay signaling packets received by the port |
| LINK INTEGRITY STATUS TX FRAMES | Number of Link Integrity signaling packets transmitted out the port |
| LINK INTEGRITY STATUS RX FRAMES | Number of Link Integrity signaling received by the port |
| DROP UNKNOWN DLCI | Number of frames received that were not associated with any known PVC |
| DROP INVALID DLCI | Number of frames received that had illegal DLCIs |
| CLEAR STATS | When activated, this field will clear all frame relay port stats |

L2 PROTOCOL (V35[2]-ATM) > STATUS > PVC(s)
Displays statistics for all the PVCs configured on this port on a PVC basis. The following statistics are available:

| DLCI | DLCI number |
| STATE | Frame relay state |
| TX FRAMES | Number of frames transmitted |
| RX FRAMES | Number of frames received |
| RX BYTES | Number of bytes received |
| DE COUNT | Number of packets received on an individual DLCI with the DE bit set |
L2 PROTOCOL (T1 ATM Firmware) – DSX Interface

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

L2 Protocol (T1 ATM – DSX) > Config

Configures the voice parameters for the interface.

Interfaces (T1 ATM – DSX) > Config > Signaling

Configures the voice signaling implemented on the interface. The signaling must match the network application. The choices are:

- E&M (TANDEM) Sets the DSX interface to use E&M signaling.
- LOOP START Sets the DSX interface to use loop start signaling.
- GROUND START Sets the DSX interface to use ground start signaling.
- ISDN PRI Sets the DSX interface to use common channel signaling for ISDN.

Interfaces (T1 ATM – DSX) > Config > Tx OAM

Configures the Total Access 850 to transmit an Operation, Administration, and Maintenance (OAM) cell to the network (voice gateway) when the DSX interface is down.

Interfaces (T1 ATM – DSX) > Config > Rx OAM

Configures the Total Access 850 to transmit an alarm condition to the DSX interface when the network (voice gateway) is down.

Interfaces (T1 ATM – DSX) > Config > Legacy Config

Digital trunk channel ID's are bits used to identify voice calls being carried within ATM cells. Some gateways do not support higher channel IDs, therefore the Total Access 850 supports CID's from 16 or 65. The default is DSX CID FROM 65.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR Count</td>
<td>Number of packets received on an individual DLCI with the CR bit set</td>
</tr>
<tr>
<td>BECN Count</td>
<td>Number of packets received on an individual DLCI with the BECN bit set</td>
</tr>
<tr>
<td>FECN Count</td>
<td>Number of packets received on an individual DLCI with the FECN bit set</td>
</tr>
<tr>
<td>Unknown Frame</td>
<td>RX Frames received that were not associated with any PVC entries</td>
</tr>
</tbody>
</table>
L2 Protocol (All Firmware) – ETH Interface > 802.3 Protocol

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

L2 Protocol (ALL–ETH–802.3) > Protocol
Displays the L2 Protocol for the 10/100BaseT Ethernet port. Currently only 802.3 is supported.

L2 Protocol (ALL–ETH–802.3) > Config
Configure the mode for this 10/100BaseT Ethernet port from this menu.

L2 Protocol (ALL–ETH–802.3) > Config > Mode
The mode identifies how the data will be forwarded. The choices are:

- **Route IP (def)**: All IP data will be routed
- **Bridge All**: All data will be bridged
- **Route IP/Bridge other**: All IP data will be routed. All other data will be bridged.

L2 Protocol (ALL–ETH–802.3) > Status
View the L2 Protocol statistics for the 10/100BaseT Ethernet port from this menu.

L2 Protocol (ALL–ETH–802.3) > Status > Tx Packets
Total number of packets transmitted out the Ethernet port.

L2 Protocol (ALL–ETH–802.3) > Status > Rx Packets
Total number of packets received from the Ethernet port.

L2 Protocol (ALL–ETH–802.3) > Status > Tx Errors
Total number of transmit errors encountered on Ethernet port.

L2 Protocol (ALL–ETH–802.3) > Status > Single Collisions
Total number of single collisions before successful transmission.

L2 Protocol (ALL–ETH–802.3) > Status > Multiple Collisions
Total number of multiple collisions before successful transmission.

L2 Protocol (ALL–ETH–802.3) > Status > Excessive Collisions
Total number of collisions that resulted in packet being dropped.

L2 Protocol (ALL–ETH–802.3) > Status > Deferred Transmissions
Total number of packets deferred due to collisions.

L2 Protocol (ALL–ETH–802.3) > Status > Carrier Sense Errors
Total number of carrier sense errors encountered (no link integrity).
L2 PROTOCOL (ALL–ETH–802.3) > Status > Rx Errors
Number of packets received in error and dropped.

L2 PROTOCOL (ALL–ETH–802.3) > Status > CRCs
Number of packets detected with CRC errors.

L2 PROTOCOL (ALL–ETH–802.3) > Status > Rx Collisions
Number of collisions which occurred during reception.

L2 PROTOCOL (ALL–ETH–802.3) > Status > Non-Aligned
The Non-Aligned parameter is set when the number of bits received is not divisible by 8.

L2 PROTOCOL (ALL–ETH–802.3) > Status > Clear Counts
Selecting this activator clears all the Ethernet stats.

BRIDGE

Configure the bridge parameters and view bridging statistics from this menu as shown in Figure 7.

Figure 10. Bridge Menu

BRIDGE > Config
Configure the interfaces and bridge table parameters from this menu.
BRIDGE > CONFIG > INTERFACES (T1)
Configure the T1 interface bridging parameters from this menu.

BRIDGE > CONFIG > INTERFACES (T1) > 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 0-6 corresponding to the interface number under L2 PROTOCOL > CONFIG > DLCI MAPPING. This is a read-only field.

BRIDGE > CONFIG > INTERFACES (ETH)
Configure the Ethernet Bridging parameters from this menu.

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

BRIDGE > CONFIG > INTERFACES (ETH) > SUB-INTERFACE
The Ethernet sub-interface is 802.3[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 8.

![Router Menu](image)

**Figure 11. 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)**

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

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

**ROUTER > CONFIG > INTERFACES (ETH) > SUB-INTERFACE**

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) > SETUP

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

**PRIMARY IP**
This is used to setup the IP addresses for the LAN on the unit.

**IP ADDRESS**
The IP address assigned to the unit's Ethernet port is set here. This address must be unique within the network. Default is **10.0.0.1**.

**SUBNET MASK**
This is the IP network mask that is to be applied to the unit's Ethernet port. Default is **255.255.255.0**.

**RIP**
Use this menu to enable RIP on the LAN interface.

**VERSION**
Enables or disables RIP and specifies the RIP protocol. Choices are: **OFF** (which disables RIP), **V1** (RIP Version 1) or **V2** (RIP Version 2). The default is **OFF**.

**METHOD**
Specifies the way the RIP protocol sends out its advertisements. The following options are available:

- **SPLIT HORIZON (DEF)**
  Only routes not learned from this circuit are advertised.

- **POISON REVERSE**
  All routes are advertised, but the routes learned from this port are “poisoned” with an infinite metric. The default is Split Horizon.

**DIRECTION**
Allows the direction at which RIP advertisements are sent and received to be specified.

- **TX AND RX (DEF)**
  RIP advertisements are periodically transmitted and are listened to on this port.

- **TX ONLY**
  RIP advertisements are periodically transmitted but are not listened to on this port.

- **RX ONLY**
  RIP advertisements are listened to on this port, but are not transmitted on this port.
V2 SECRET
Enter the secret used by RIP version 2 here.

PROXY ARP
This feature allows the network portion of a group of addresses to be shared among several physical network segments. The ARP protocol provides a way for devices to create a mapping between physical addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a "proxy" for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to YES, when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, the unit will answer the request with its own hardware address. Default is NO.

SECONDARY IPs
This allows the unit to specify additional IP addresses and networks on its Ethernet. The maximum number of entries is 5.

NUM
Displays the index number in the secondary IP list.

IP ADDRESS
This is the second IP address the unit will respond to on the Ethernet. Default is 0.0.0.0.

SUBNET MASK
This is the mask for the network. Default is 255.255.255.255.

NAT MODE
This mode specifies whether Network Address Translation (NAT) should be used on this interface. When this mode is set to PRIVATE (def) NAT is automatically specified on this interface. The other choice is PUBLIC which specifies not going through NAT.

ROUTER > CONFIG > INTERFACES (NET)
Configure the layer 3 options for the network interface from this menu.

The network interface will display in the ROUTER > CONFIG > INTERFACES table showing the name of the network technology (i.e. T1 or SDSL), but only once a PVC to the router (ATM) or DS0s to the router (TDM) have been configured.
ROUTER > CONFIG > INTERFACES (NET) > SUB-INTERFACE
This is a read-only field which displays the physical and logical port of the interface using the following nomenclature: [A,B], where A represents the physical port (network interface is 0, Ethernet is 1) and B represents the logical port for the Layer 2 protocol (i.e. PVC for Frame Relay, PPP link, etc.) Each configured logical port is assigned a number corresponding to the order in which they are listed in the L2 Protocol configuration fields.

ROUTER > CONFIG > INTERFACES (NET) > SETUP
Configure the IP parameters for this interface and sub-interface from this menu.

ACTIVE
This Selection enables IP on this PVC.

VPI
ATM virtual port identifier assigned to this sub-interface in the L2 PROTOCOL menus. This field is only applicable when L2 protocol for this sub-interface is ATM.

VCI
ATM virtual channel identifier assigned to this sub-interface in the L2 PROTOCOL menus. This field is only applicable when L2 protocol for this sub-interface is ATM.

DLCI
Data Link Connection Identifier assigned to this PVC in the L2 PROTOCOL menus. This field is only applicable when L2 protocol for this sub-interface is FRE.

ADDRESS MODE
Specifies the method the unit uses to determine the local and far-end IP addresses. The choices are USER SPECIFIED (default), DHCP CLIENT, or IARP. USER SPECIFIED allows the user configuration for Local IP and Far-End IP addresses, DHCP CLIENT is used for the Total Access 850 to learn his IP address from a DHCP server. IARP allows the unit to determine the far-end IP address using inverse ARP.

LOCAL IP ADDRESS
This is the IP address for this PVC. This field is not visible when ADDRESS MODE is set to DHCP CLIENT.

IP NETMASK
This is the network mask used for this interface. This field is not visible when ADDRESS MODE is set to DHCP CLIENT.
**FAR-END IP ADDRESS**
This is the address of the NEXT hop router on this interface. This field is only visible when **ADDRESS MODE** is set to **USER SPECIFIED**.

**MTU**
Specifies the maximum size for a packet transmitted on this PVC. Default is **1500**. This field is only valid when L2 protocol for this sub-interface is **FRE**.

**NAT**
Use this menu to set up and use Network Address Translation on this interface.

**PORT TRANSLATION**
By enabling port translation, IP packets are modified as they pass through this interface. During transmission, private addresses are translated into a single public (NAPT) IP address. Incoming packets are translated from the public to private address based on the protocol port numbers. Once enabled, additional menus appear and can be used to further customize the NAT configuration. The default is **DISABLED**.

**PUBLIC IP ADDRESS MODE**
Sets the public NAPT address used for translating. Choices are **INTERFACE** (default) and **SPECIFIED**. Selecting **INTERFACE** configures NAT to use the IP address already specified on the interface; the NAPT address and the interface address are the same. Using **SPECIFIED** defines a particular IP address used as the NAPT address.

**PUBLIC IP ADDRESS**
This menu only appears when the **PUBLIC IP ADDRESS MODE** is set to **SPECIFIED**, and allows the user to enter a specific NAPT address.

**TRANSLATE BODY OF UNMAPPED PARTS**
Enabling this function forces NAPT to translate the body of any unmapped solicited traffic originating from the LAN. Default is **DISABLED**.

**TRANSLATION TABLE**
Table used for defining addresses and port translations. This is an indexed list of all translations defined for the router. It specifies the translations for specified public addresses/ports to private addresses/ports. To insert a new translation entry, highlight the index number of the first translation and press the `<I>` key. To delete a particular entry, highlight the index number of the entry and press the `<D>` key. The **TRANSLATION TABLE** parameter descriptions follow.
PUBLIC ADDRESS MODE

Choose NAPT ADDR (default) or SPECIFIED to choose which address to use for this translation. Choosing SPECIFIED allows the user to define a different public IP address to use for this translation.

PUBLIC ADDRESS

This menu appears when the PUBLIC ADDRESS MODE is set to SPECIFIED, and allows the user to enter a specific IP address as the NAPT address for this translation.

PROTOCOL MODE

Defines the protocol of the data for this translation. Choices are TCP, UDP, ICMP, TCP OR UDP, ICMP, ALL, SPECIFIED, or NONE (default). Use this option to specify whether you want to translate a specific protocol, group of protocols, or all protocols.

PROTOCOL

This menu appears when the PROTOCOL MODE is set to SPECIFIED. Use this option to specify a protocol number that does not appear in the list of choices under the Protocol Mode menu. The most common protocols are:

<table>
<thead>
<tr>
<th>Protocol Number</th>
<th>Keyword</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ICMP</td>
<td>Internet Control Message</td>
</tr>
<tr>
<td>6</td>
<td>TCP</td>
<td>Transmission Control</td>
</tr>
<tr>
<td>8</td>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>17</td>
<td>UDP</td>
<td>User Datagram</td>
</tr>
<tr>
<td>47</td>
<td>GRE</td>
<td>General Routing Encapsulation</td>
</tr>
<tr>
<td>50</td>
<td>ESP</td>
<td>IPSEC Encap Security Payload</td>
</tr>
<tr>
<td>51</td>
<td>AH</td>
<td>IPSEC Authentication Header</td>
</tr>
</tbody>
</table>

PROTOCOL TYPE

(Read only) This menu appears when the PROTOCOL MODE is set to SPECIFIED and displays the name of the specified protocol number (if the name is known by the Total Access 850). For example, entering a value of 47 in the PROTOCOL field will cause the PROTOCOL TYPE field to display GRE.
PUBLIC PORT MODE
This option appears when the PROTOCOL MODE is configured with a single protocol (such as TCP, UDP, or ICMP). Choices are ANY PORT (default) and SPECIFIED. The public destination port associated with this entry can be specified to add more control over certain types of traffic. Leave this configured as ANY PORT to cover all port types.

PUBLIC PORT
This menu appears when the PUBLIC PORT MODE is set to SPECIFIED. Use this option to specify the public port number to translate. Some well known TCP/UDP port numbers are shown below:

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Keyword</th>
<th>Port Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>FTP (data)</td>
<td>File Transfer Protocol Data</td>
</tr>
<tr>
<td>21</td>
<td>FTP (control)</td>
<td>File Transfer Protocol Control</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
<td>TCP/IP terminal emulation utility</td>
</tr>
<tr>
<td>666</td>
<td>DOOM</td>
<td>DOOM</td>
</tr>
<tr>
<td>53</td>
<td>DNS</td>
<td>Domain Name Server</td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>110</td>
<td>POP3</td>
<td>Post Office Protocol ver. 3</td>
</tr>
</tbody>
</table>

PRIVATE ADDRESS MODE
Choose ANY INTERNAL (default) or SPECIFIED to choose which address to use for the private address. The private IP address can be specified to filter certain protocols and ports to specific servers in the private network. Likewise, internal hosts can be steered to certain servers on the public network. A new request from the public network that matches this entry’s public parameters is dropped if the PRIVATE ADDRESS MODE is set to ANY INTERNAL (with the exception of protocols that the internal router is expected to respond to, such as ICMP or SNMP).

PRIVATE ADDRESS
This menu appears when the PRIVATE ADDRESS MODE is set to SPECIFIED, and allows the user to enter a specific private IP address for this translation. Packets destined for the public IP address (of this translation) are redirected to the private IP address specified here.
PRIVATE PORT MODE
Select ANY PORT (default) or a SPECIFIED port number for this translation. The private destination port associated with this entry can be specified to provide more control over certain types of traffic. Leave configured as ANY PORT to cover all port types.

PRIVATE PORT MODE
This menu appears when the PRIVATE PORT MODE is set to SPECIFIED, and allows the user to enter the port number that replaces the public port number during the translation of incoming packets. Outgoing packets from the private address space that match this protocol are sent to the specified public address and port, if any.

TRANSLATE BODY
If set to YES, the application payload in the packet is scanned for occurrences of the private/public IP address in binary or ASCII form. Set this to NO for applications where scanning payload data is undesirable.

NAT VIEW
Provides the user a dynamic view of current active router translations. Once the router has translated an inbound or outbound packet, the translation appears in this table. The main view is a listing of all the translations performed thus far. In order to see the detailed view of one of the entries, select the entry index number and press <ENTER>. The NAT View parameters are as follows:

PRIVATE ADDRESS
Private IP address of the active translation.

PUBLIC ADDRESS
Public IP address of the active translation.

SERVER ADDRESS
Server IP address of the public device.

PROTOCOL
Type of protocol active on the translation.

PRIVATE PORT
Private port number used for the translation.
**SPOOFED PORT**

Spoofed port number for the translation. The Total Access 850 often needs to use the spoofed ports to determine which private device to translate the packet to. This would be necessary if multiple applications using the same private port were occurring simultaneously.

**SERVER PORT**

Port number used by the server (public device).

**TOTAL TIME UNUSED**

Time the translation has been unused, in seconds.

**IN COUNT**

Number of inbound packets using this translation.

**OUT COUNT**

Number of outbound packets using this translation.

**NAPT ADDRESS**

(Read only) Displays the NAPT address for the router. This will either be the interface address or the user-specified NAPT address.

**ENTRY COUNT**

The number of translation entries that are currently available in the **NAT VIEW** table. The Total Access 850 supports up to 2000 active translations at any one time.

**ENTRY OVERFLOW COUNT**

The number of overflow **NAT VIEW** entries. After the maximum number of translations is reached, the Total Access 850 will not add new translations, but continues to keep a count of any new translation requests it cannot accommodate.

**RIP**

Use this menu to enable RIP on this interface.

**VERSION**

Enables or disables RIP and specifies the RIP protocol. Choices are: **OFF** (which disables RIP), **V1** (RIP Version 1) or **V2** (RIP Version 2). The default is **OFF**
**ROUTER > CONFIG > ROUTES**

Configures the default gateway and static routes from this menu.

**ROUTER > CONFIG > ROUTES > DEFAULT GATEWAY**

The default gateway is used by the unit to send IP packets whose destination addresses are not found in the route table (otherwise known as the gateway of last resort). 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.

**METHOD**

Specifies the way the RIP protocol sends out its advertisements. The following options are available:

**SPLIT HORIZON**

(Defaults) Only routes not learned from this circuit are advertised.

**POISON REVERSE**

All routes are advertised, but the routes learned from this point are “poisoned” with an infinite metric.

**DIRECTION**

Allows the direction at which RIP advertisements are sent and received to be specified.

**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**.
**ROUTER > CONFIG > DHCP SERVER**

Use this menu to set up the DHCP server.

**ROUTER > CONFIG > DHCP SERVER > DHCP SERVER**

Use this menu to enable the DHCP server (On or Off).

**ROUTER > CONFIG > DHCP SERVER > DHCP ADDRESS POOLS**

Configures the parameters for the various defined DHCP address pools. Multiple DHCP address pools may be defined using these menus.

**NUM**

Displays the index number of the defined DHCP address pools. Multiple address pools are valid, and all will be listed in sequential order. This number is for reference only.

**NAME**

Enter a user-defined alphanumeric text string for the defined DHCP address pool. This text string is for easy identification and reference only.

**TYPE**

Configures the DHCP address pool as either a Network or Host pool.

**LEASE CONFIG**

Configures the lease duration for an IP address from this pool assigned by the DHCP server to a host on the network.

**LEASE DAYS, HOURS, MINUTES**

Defines the lease duration (in days, hours, and minutes) for an IP address from this pool assigned by the DHCP server to a host on the network.

**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.
**NETWORK ADDRESS**
Defines the network address for the configured address pool (for example, 172.24.0.0). The **NETWORK ADDRESS** and **NETWORK MASK** determine the number of addresses available on the network for the configured pool.

**NETWORK MASK**
Defines the network mask associated with the network address for the configured address pool (for example, 255.255.0.0). The **NETWORK ADDRESS** and **NETWORK MASK** determine the number of addresses available on the network for the configured pool.

**POOL INFO**
Configures various network parameters assigned to all hosts given an IP address from the configured address pool.

**NETWORK MASK**
Defines the network mask associated with the network address for the configured address pool (for example, 255.255.0.0). The **NETWORK ADDRESS** and **NETWORK MASK** determine the number of addresses available on the network for the configured pool.

**DEFAULT ROUTER (PRI)**
Defines the primary default router IP address (in dotted decimal notation) for all hosts given an IP address from the configured pool. When specifying a router to use as the primary/secondary preferred router, verify that the listed router is on the same subnet as the DHCP client.

**DEFAULT ROUTER (SEC)**
Defines the secondary default router IP address (in dotted decimal notation) for all hosts given an IP address from the configured pool. When specifying a router to use as the primary/secondary preferred router, verify that the listed router is on the same subnet as the DHCP client.

**DNS SERVER (PRI)**
Defines the primary Domain Name Server IP address (in dotted decimal notation) for all hosts given an IP address from the configured pool.

**DNS SERVER (SEC)**
Defines the secondary Domain Name Server IP address (in dotted decimal notation) for all hosts given an IP address from the configured pool.
**NBNS Server (Pri)**
Defines the primary NetBIOS Windows Internet Naming Service (WINS) name server IP address (in dotted decimal notation) available for use by the Dynamic Host Configuration Protocol (DHCP) clients.

**NBNS Server (Sec)**
Defines the secondary NetBIOS Windows Internet Naming Service (WINS) name server IP address (in dotted decimal notation) available for use by the Dynamic Host Configuration Protocol (DHCP) clients.

**NBNS Node Type**
Defines the type of NetBIOS node used with Dynamic Host Configuration Protocol (DHCP) clients. The following node types are available:
- b-node (1) - Broadcast node
- p-node (2) - Peer-to-Peer node
- m-node (4) - Mixed node
- h-node (8) - Hybrid node (Recommended)

**Router > Config > DHCP Server > Exclusion Ranges**
Defines any IP address (or range of addresses) that should not be used the Total Access 850 DHCP server when making IP assignments to hosts on the network.

**Num**
Displays the index number of the listed IP address exclusion ranges. Multiple address exclusions are valid, and all will be listed in sequential order. This number is for reference only.

**Start**
Configures the start IP address (in dotted decimal notation) for the range of IP addresses to exclude from the DHCP address pool. Use in conjunction with the **End** field to establish a range of IP addresses. To exclude a single IP address, enter the same address in both the **Start** and **End** fields.

**End**
Configures the ending IP address (in dotted decimal notation) for the range of IP addresses to exclude from the DHCP address pool. Use in conjunction with the **Start** field to establish a range of IP addresses. To exclude a single IP address, enter the same address in both the **Start** and **End** fields.

**Router > Config > DHCP Server > Global Server Options**
Configures various network parameters that apply to all hosts given an IP address from the configured address pools (regardless of the pool). Use these commands to configure parameters for all address pools when customizing between the address pools is not necessary. Refer to Pool Info on page 159 for more details on the available parameters.
**ROUTER > Config > UDP Relay**
This menu configures the unit to act as a UDP relay agent for applications requiring a response from UDP hosts that are not on the same network segment as their clients.

**ROUTER > Config > UDP Relay > Mode**
When this option is set to **On**, the unit will act as a relay agent. Default is **Off**.

**ROUTER > Config > UDP Relay > UDP Relay List**
Up to four relay destination servers can be specified in this list.

- **#**
  Indicates the entry number in the UDP Relay List table.

- **Relay Address**
  This is the IP address of the server that will receive the relay packet. Default is **0.0.0.0**.

- **UDP Port Type**
The choices are **Standard** (def) and **Specified**. The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123), NBNS (NetBIOS Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and BootP. When **Specified** is set, the UDP port (1 to 65535) can be specified in the UDP Port columns (up to three per server).

- **UDP Port 1, 2, 3**
  Used for specifying UDP ports to be relayed. These fields only apply when **UDP Port Type** is set to **Specified**. Default is **0**.

**ROUTER > Status**
View the **IP Routes**, **IP Stats**, **ARP Cache**, **DHCP Server**, and **DHCP Client** statistics from this menu.

**ROUTER > Status > IP Routes**
This lists the contents of the unit’s IP route table.

**ROUTER > Status > IP Routes > IP Address**
Network or host destination address.

**ROUTER > Status > IP Routes > Netmask**
Network mask applied to the destination address.

**ROUTER > Status > IP Routes > Gateway**
Host or router to receive this packet.
ROUTER > STATUS > IP ROUTES > PORT
Port gateway is located on:

- **LOCAL**
  - Sent directly to the unit’s router
- **ETH0**
  - The unit’s Ethernet port
- **WAN0**
  - The unit’s first PPP bundle
- **FR 0 . . . FR 9**
  - The unit is connected up to 10 DLCIs

ROUTER > STATUS > IP ROUTES > USE
Number of times the unit has referenced the route.

ROUTER > STATUS > IP ROUTES > FLAGS
Important tags associated with this route entry

- **H**
  - route is a host route
- **G**
  - route is a gateway route
- **S**
  - static route, or learned via IPCP, IARP, DHCP
- **R1**
  - learned from RIP Version 1
- **R2**
  - learned from RIP Version 2
- **I**
  - route learned from an ICMP redirect
- **C**
  - directly connected interface
- **P**
  - route is private and is not advertised with RIP
- **T**
  - route is to a triggered port (updates only when table changes)
- **U**
  - learned by unknown method

ROUTER > STATUS > IP ROUTES > HOPS
Number of routers that must go through to get to destination. Ranges from **0-15** or **16** for infinite (can’t get there from here).

ROUTER > STATUS > IP ROUTES > TTL
Seconds until address is removed from table. Value of 999 means route is static.

ROUTER > STATUS > IP STATS
This section describes the following **STATISTICS** submenus (and see the tables on the pages following):
• IP
• ICMP
• TCP
• UDP

All of these statistics are taken from the MIB-II variables in RFC 1156. To clear the accumulated statistics, press the <ENTER> key on CLEAR COUNTS.

**ROUTER > STATUS > IP STATS > IP**

View the IP statistics from this menu.

**DEFAULT TTL**

The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this unit, whenever a TTL value is not supplied by the transport layer protocol.

**IP DATAGRAMS RECEIVED**

The total number of input datagrams received from interfaces, including those received in error.

**BAD HEADER PACKETS**

The number of input datagrams discarded due to errors in their IP headers, including bad check sums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

**BAD IP ADDRESSES**

The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this unit. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

**TOTALForwarded DATAGRAMS**

The number of input datagrams for which this unit was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this unit, and the Source-Route option processing was successful.

**BAD PROTOCOL DISCARDS**

The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
**DATAGRAMS DISCARDED**
The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

**SENT DATAGRAMS TO UPPER LAYERS**
The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

**IP DATAGRAMS SENT**
IP packets from the unit's IP stack.

**ERRORFREE DISCARDS**
The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in **TOTAL FORWARDED DATAGRAMS** if any such packets met this (discretionary) discard criterion.

**ROUTELESS DISCARDS**
The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in **TOTAL FORWARDED DATAGRAMS** which meet this “no-route” criterion. Note also that this includes any datagrams which a host cannot route because all of its default gateways are down.

**IP REASSEMBLY TIMEOUT**
The maximum number of seconds received fragments are held while awaiting reassembly at this unit.

**DISASSEMBLED FRAGMENTS**
The number of IP fragments received which needed to be reassembled at this unit.

**IP DATAGRAMS REASSEMBLED**
The number of IP datagrams successfully reassembled.

**IP REASSEMBLY FAILURES**
The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably RFC 815s) can lose track of the number of fragments by combining them as they are received.
SUCCESSFUL FRAGMENTS
The number of IP datagrams that have been successfully fragmented at this unit.

FAILED FRAGMENTS
The number of IP datagrams that have been discarded because they needed to be fragmented at this unit but could not be e.g., because their “Don't Fragment” flag was set.

TOTAL IP FRAGMENTS
The number of IP datagram fragments that have been generated as a result of fragmentation at this unit.

DISCARDED ROUTING ENTRIES
A packet the unit couldn't route.

CLEAR COUNTS
Setting this activator clears the IP Statistics.

ROUTER > STATUS > IP STATS > ICMP

ICMP MESSAGES RECEIVED
The total number of ICMP messages the unit received. Note that this counter includes all those counted by ICMP SPECIFIC ERRORS.

ICMP SPECIFIC ERRORS
The number of ICMP messages the unit received but determined as having errors (bad ICMP checksums, bad length, etc.)

ICMP DEST. UNREACHABLE MSGS RCVD
The number of ICMP Destination Unreachable messages received.

ICMP TIMEOUTS RECEIVED
The number of ICMP Time Exceeded messages received.

ICMP PARAMETER PROBLEM MSGS RCVD
The number of ICMP Parameter Problem messages received.

ICMP SOURCE QUENCH MSGS RCVD
The number of ICMP Source Quench messages received.
**ICMP Redirected Messages Rcvd**
The number of ICMP Redirect messages received.

**ICMP Echo Request Msgs Rcvd**
The number of ICMP Echo (request) messages received.

**ICMP Echo Reply Msgs Rcvd**
The number of ICMP Echo Reply messages received.

**ICMP Timestamp Request Msgs Rcvd**
The number of ICMP Timestamp (request) messages received.

**ICMP Timestamp Reply Msgs Rcvd**
The number of ICMP Timestamp Reply messages received.

**ICMP Address Mask Request Msgs Rcvd**
The number of ICMP Address Mask Request messages received.

**ICMP Address Mask Reply Msgs Rcvd**
The number of ICMP Address Mask Reply messages received.

**ICMP Messages Sent**
The total number of ICMP messages this unit attempted to send. Note that this counter includes all those counted by **ICMP Packet Errors**.

**ICMP Packet Errors**
The number of packets the unit did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.

**ICMP Dest. Unreachable Msgs Sent**
The number of ICMP Destination Unreachable messages sent.

**ICMP Time Exceeded Msgs Sent**
The number of ICMP Time Exceeded messages sent.
ICMP Parameter Problem Msgs Sent
The number of ICMP Parameter Problem messages sent.

ICMP Source Quench Msgs Sent
The number of ICMP Source Quench messages sent.

ICMP Redirect Msgs Sent
The number of ICMP Redirect messages sent.

ICMP Echo Request Msgs Sent
The number of ICMP Echo (request) messages sent.

ICMP Echo Reply Msgs Sent
The number of ICMP Echo Reply messages sent.

ICMP Timestamp Request Msgs Sent
The number of ICMP Timestamp (request) messages sent.

ICMP Timestamp Reply Msgs Sent
The number of ICMP Timestamp Reply messages sent.

ICMP Addr Mask Request Msgs Sent
The number of ICMP Address Mask Request messages sent.

ICMP Addr Mask Reply Msgs Sent
The number of ICMP Address Mask Reply messages sent.

Clear Counts
Selecting this activator will clear the ICMP statistics.

Router > Status > IP Stats > UDP
View the UDP statistics from this menu.

UDP Datagrams Received
The total number of UDP datagrams delivered to UDP users.
**NO APPLICATION AT DEST. PORT**

The total number of received UDP datagrams for which there was no application at the destination port.

**UDP BAD PACKETS**

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

**UDP DATAGRAMS SENT**

The total number of UDP datagrams sent from this unit.

**CLEAR COUNTS**

Selecting this activator clears the UDP statistics.

**ROUTER > STATUS > IP STATS > UDP TABLE**

View the UDP table statistics from this menu.

**LOCAL IP ADDRESS**

The destination IP address of the packet

**PORT**

The destination UDP port of the packet.

**ROUTER > STATUS > IP STATS > TCP**

View the TCP statistics from this menu.

**RETRANSMISSION TIMEOUT ALGORITHM**

The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.

**MIN RETRANSMISSION TIMEOUT (MS)**

The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the **LBOUND** quantity described in RFC 793.

**MAX RETRANSMISSION TIMEOUT (MS)**

The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the **UNBOUND** quantity described in RFC 793.
**MAX TCP CONNECTIONS**
The limit on the total number of TCP connections the unit can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

**ACTIVE TCP CONNECTIONS**
The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

**TCP PASSIVE CONNECTIONS**
The number of times TCP connections have made a direct transition to the SYN-Rcvd state from the LISTEN state.

**TCP FAILED ATTEMPTS**
The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-Rcvd state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-Rcvd state.

**TOTAL TCP RESETS**
The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

**TCP CURRENT CONNECTIONS**
The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

**TCP SEGMENTS RECEIVED**
The total number of segments received, including those received in error. This count includes segments received on currently established connections.

**TCP SEGMENTS SENT**
The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

**TOTAL TCP RETRANSMITS**
The total number of segments retransmitted -- that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

**CLEAR COUNTS**
Selecting this activator clears the TCP statistics.
ROUTER > STATUS > IP STATS > TCP CONNS
View the TCP Conns Statistics from this menu. This table shows the different states of each TCP connection.

STATE
The possible states are **FREE**, **CLOSED**, **LISTEN**, **SYNC SENT**, **SYNC RECEIVED**, **ESTABLISHED**, **FINWAIT1**, **FINWAIT2**, **CLOSEWAIT**, **LASTACK**, **CLOSING**, and **TIMEWAIT**.

LOCAL IP ADDRESS
Local IP address of the TCP connection.

LOCAL PORT
Local port of the TCP connection.

REMOTE IP ADDRESS
Remote IP address of the TCP connection.

REMOTE PORT
Remote port of the TCP connection.

ROUTER > STATUS > ARP CACHE
This lists the contents of the unit’s ARP table. All resolved cache entries time out after 20 minutes. Unresolved entries time out in 3 minutes. The ARP cache can be cleared by pressing “f” while on the menu or by pressing “d” on the individual number for that entry.

ROUTER > STATUS > ARP CACHE > IP ADDRESS
IP address used for resolving MAC address.

ROUTER > STATUS > ARP CACHE > MAC ADDRESS
Ethernet address resolved (0=no resolution).

ROUTER > STATUS > ARP CACHE > TIME
Minutes since entry was first entered into the ARP cache.

SECURITY
Configure the **SECURITY FILTERS** and **RADIUS SERVER** parameters from this menu as shown in Figure 12.
Figure 12. 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.

The Filter Defines option applies to both Frame Relay and PPP operation.

SECURITY > FILTERS > FILTER DEFINES > MAC FILTER DEFINES
The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of the unit are defined here. Up to 32 MAC defines can be specified.

NUM
Indicates the entry number in the MAC Filter Defines table.

NAME
Identifies the filter entry. Default is no entry in NAME field.

FILTER TYPE
Specifies a NORMAL or DEBUG filter. When a NORMAL filter is applied to an interface, traffic is blocked or forwarded according to the filter. When a DEBUG filter is applied, packets that match the filter are documented without affecting traffic flow. (Use the DEBUG filter with the Syslog or Terminal Mode logging to view the packet contents.)

SRC ADDR
48-bit MAC source address used for comparison. Values are in hexadecimal format. Default is 00:00:00:00:00:00.

SRC MASK
Bits in the MAC source address which are compared. Values are in hexadecimal format. Default is 00:00:00:00:00:00.

DEST ADDR
48-bit MAC destination address used for comparison. Values are in hexadecimal format. Default is 00:00:00:00:00:00.
**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.

**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**.

**NUM**
Indicates the entry number in the Pattern Filter Defines table.

**NAME**
Identifies the filter entry. Default is no entry in **NAME** field.

**FILTER TYPE**
Specifies a **NORMAL** or **DEBUG** filter. When a **NORMAL** filter is applied to an interface, traffic is blocked or forwarded according to the filter. When a **DEBUG** filter is applied, packets that match the filter are documented without affecting traffic flow. (Use the **DEBUG** filter with the Syslog or Terminal Mode logging to view the packet contents.)

**OFFSET**
Offset from beginning of packet of where to start the pattern comparison. Default is 0.

**PATTERN**
64 bits used for comparison. Values are in hexadecimal format. Default is **00:00:00:00:00:00:00:00**.

**MASK**
Bits in the pattern to be compared. Values are in hexadecimal format. Default is **00:00:00:00:00:00:00:00**.

**SECURITY > FILTERS > FILTER DEFINES > IP FILTER DEFINES**
The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.
NUM
Indicates the entry number in the IP Filter Defines table.

NAME
Identifies the filter entry. Default is no entry in name field.

FILTER TYPE
Specifies a NORMAL or DEBUG filter. When a NORMAL filter is applied to an interface, traffic is blocked or forwarded according to the filter. When a DEBUG filter is applied, packets that match the filter are documented without affecting traffic flow. (Use the DEBUG filter with the Syslog or Terminal Mode logging to view the packet contents.)

SRC ADDR
IP address compared to the source address. Value is in dotted decimal format. Default is 0.0.0.0.

SRC MASK
Bits which are used in the source comparison. Value is in dotted decimal format. Default is 0.0.0.0.

DEST ADDR
IP address compared to the destination address. Value is in dotted decimal format. Default is 0.0.0.0.

DEST MASK
Bits which are used in the destination comparison. Value is in dotted decimal format. Default is 0.0.0.0.

SRC PORT
IP source port number used for comparison. Value is in decimal format. Range: 0 - 65535. Default is 0.

SRC PORT COMP
Type of comparison that is performed. Default is NONE.

= means ports equal to
NOT = means port not equal to
> means port greater than
< means port less than
None - means the source port is not compared
**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 (ETH)**

Define the filters for the Ethernet interface from this menu.

**DEST PORT**

IP destination port number used for comparison. Value is in decimal format. Range: 0 - 65535. Default is 0.

**DEST PORT COMP**

Type of comparison that is performed. Default is **NONE**.

- = means ports equal to
- **NOT =** means port not equal to
- > means port greater than
- < means port less than
- **None** - means the source port is not compared

**PROTOCOL**

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

**PROTOCOL COMP**

Type of comparison that is performed. Default is **NONE**.

- = means ports equal to
- **NOT =** means port not equal to
- > means port greater than
- < means port less than
- **None** - means the source port is not compared

**TCP ESTAB**

- **Yes** - only when TCP established
- **No** - only when TCP not established
- **Ignore** - ignore TCP flags (def)
SECURITY > FILTERS > INTERFACES (ETH) > SUB-INTERFACE
The Ethernet sub-interface is 802.3[1.0]. This is a read-only field.

SECURITY > FILTERS > INTERFACES (ETH) > 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  All incoming packets from the WAN are not 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.

**HIT COUNT**

Displays the number of packets that match the criteria for the defined filter.

**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 > 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 defines in the list. Default is no entry in filter list name.

NEXT OPER
The next operation to use to combine with the next filter in the list (default is END):

- END: the last filter to combination.
- AND: logically AND this filter with the next filter in the list.
- OR: logically OR this filter with the next filter in the list.

HIT COUNT
Displays the number of packets that match the criteria for the defined filter.

SECURITY > RADIUS SERVER
The parameters for the RADIUS SERVER are configured in this menu.

Note
Telnet radius is only available in A.04 firmware or later.

SECURITY > RADIUS SERVER > Server 1
This is the IP address of the first RADIUS SERVER that the unit should attempt to communicate with when authenticating a Telnet session. Default is 0.0.0.0.

SECURITY > RADIUS SERVER > Server 2
This is the IP address of the second RADIUS SERVER that the unit should attempt to communicate with when the primary server does not respond. Default is 0.0.0.0.

SECURITY > RADIUS SERVER > Server 3
This is the IP address of the third RADIUS SERVER that the unit should attempt to communicate with when the primary server does not respond. Default is 0.0.0.0.

SECURITY > RADIUS SERVER > UDP PORT
This is the UDP port the unit should use when communicating with the RADIUS SERVER. The default is 1812, which the commonly used port.

SECURITY > RADIUS SERVER > SECRET
The RADIUS SERVER and unit share this text string. It is used by the RADIUS SERVER to authenticate the unit, the RADIUS client. The factory default is not to use a secret.
SECURITY > RADIUS SERVER > RETRY COUNT (1-10)

This is the number of times the unit should send a request packet 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 configuration fields only apply for T1 TDM applications.

The DS0 MAPS menu allows you to map data and voice ports to the network T1 time slots. You may edit either of the two maps at any time. If you make changes to the current map, only those DS0s that have changed will be updated (unchanged DS0s will not be affected.) The DS0 menu is shown in Figure 13.

Figure 13. DS0 Maps Menu
DS0 MAPS > ACTIVE MAP
Activates one of the two dedicated maps (Map 1 or Map 2), or the Dual T1 Map. In the Dual T1 mode, the built-in DSX-1 interface DSX[3] can be utilized as a secondary T1 connection. In Dual T1 mode, the second T1 is limited to voice connections on FXS and FXO modules. For example, the user may map all 24 DS0s on the network T1 to the router, and on the second T1 (DSX-1 interface) map all 24 DS0s to the FXS cards. Default is Map 1.

DS0 MAPS > APPLY TEMPLATE TO MAP 1
Choices are Current Map 1, Current Map 2, D4 Map, D1D Map, Full Router, and Clear Map. Default is Current Map 1. D4 Map automaps the voice port in a 1-to-1 configuration. D1D Map maps voice ports in an SLC-96 configuration. Full Router maps all 24 DS0s to the router at 64K. Clear Map clears the entire map.

DS0 MAPS > EDIT/VIEW MAP 1
Define map 1. The map allows the user to assign services and ports to the individual DS0s 1-24.

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 > SLOT
When you select this option, a list of all of the slots and the modules displays. This first option Open, when unassigns the slot if selected. For modules, the slot number and name are shown. For example, FXS indicates that an FXS card is installed. Use TA IAD to map network timeslot to the V.35 port or to the router. Pick the appropriate server, 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.
**DS0 Maps > Edit/View Map 1 > RBS**

Robbed Bit Signaling. Default is N/A. Once a slot and port are assigned, this will automatically change to **On** or **Off**. The unit automatically assigns **Off** where **RBS** is not an option. **On** preserves the signaling bits between the connections. **Off** ignores the signaling bits. For the **FXS**, **RBS** defaults to **On**. The **RBS** parameter remains at N/A for the **TA IAD**, because **RBS** is not applicable to data connections.

**Map 2 menus are identical to Map 1. Please use the menu explanations above for Map 2.**
4. APPENDICES (T1 TDM APPLICATIONS)

Appendix A. Configuring the Unit for Routing

Initial Setup
It is best to configure Total Access 850 TDM applications by following the order of the top-level menus. For example, first configure the system parameters using the System Info and System Config menus. Next, configure the Layer 1 parameters using the Interfaces menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the L2 Protocol menus. Follow the Layer 2 setup with the data “routing” menus (either Bridge or Router). Establish packet forwarding and blocking using the Security menus. Lastly, configure the physical mappings using the DS0 Maps menus.

The following example provides step by step instructions for configuring the Total Access 850 T1 TDM system (Interfaces through DS0 Maps) for a standard routing application. System Info and System Config parameters should be set according to your system need. Refer to System Info on page 73 and System Config on page 75 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Network T1 menus beginning on page 94*
*Ethernet menus beginning on page 101*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select Interfaces.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the Config menu for the T1 interface and press &lt;Enter&gt;.</td>
</tr>
<tr>
<td>3</td>
<td>Right arrow to select Format and choose ESF or SF.</td>
</tr>
<tr>
<td>4</td>
<td>Set the Line Code to B8ZS or AMI.</td>
</tr>
<tr>
<td>5</td>
<td>Set the Equalization or line build out. The default setting of 0 dB is usually sufficient.</td>
</tr>
<tr>
<td>6</td>
<td>Set the CSU LPBK option to Enable, Disable, or Disable All based on whether looping to this unit from another unit will be allowed.</td>
</tr>
</tbody>
</table>

*Note* This format must match the format used by the other units in the network.

*Note* This line code must match the line code used by the other units in the network.
2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

Layer 2 Frame Relay Protocol menus beginning on page 121
Layer 2 PPP Protocol menus beginning on page 118
Layer 2 Ethernet menus beginning on page 144

### Ethernet Interface Setup Instructions

Most applications should not require a manual setup for the Ethernet interface. By default, the Ethernet interface is configured to auto-detect the data rate (as either 10 or 100 Mbps). The following steps disable the auto-negotiation parameter and manually configure the interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>INTERFACES</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>ETH</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Use the right arrow to select <strong>AUTONEGOTIATION</strong> and press <strong>&lt;ENTER&gt;</strong>. Use the down arrow to choose <strong>OFF</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Select the <strong>DATA RATE</strong> field and specify either <strong>10BASET</strong> or <strong>100BASET</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Select the <strong>DUPLEX TYPE</strong> field and specify either <strong>HALF DUPLEX</strong> or <strong>FULL DUPLEX</strong>.</td>
</tr>
</tbody>
</table>

### Layer 2 Protocol (FRE) Configuration – T1 Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>L2 PROTOCOL</strong> and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Use the arrow keys to select the <strong>PROTOCOL</strong> field for the <strong>T1</strong> interface. Press <strong>&lt;ENTER&gt;</strong>. Select <strong>FRE</strong> from the list of available protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>T1</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Set the <strong>MAINTENANCE PROTOCOL</strong> to <strong>ANNEX D (ANSI)</strong>, <strong>ANNEX A</strong> (q933a), <strong>LMI</strong>, or <strong>STATIC</strong> (no sig).</td>
</tr>
</tbody>
</table>

**Note**

The **MAINTENANCE PROTOCOL** should be set based on the Frame Relay switch.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Down arrow and press <strong>&lt;ENTER&gt;</strong> on <strong>DLCI MAPPING</strong>. Press the right arrow key to create an entry. To create additional entries, highlight the <strong>NUM</strong> field and press the <strong>&lt;I&gt;</strong> key. To delete an entry, highlight the <strong>NUM</strong> field for the entry to delete and press the <strong>&lt;D&gt;</strong> key.</td>
</tr>
<tr>
<td>6</td>
<td>Set <strong>ACTIVE</strong> to <strong>YES</strong>.</td>
</tr>
</tbody>
</table>
### Layer 2 Protocol (FRE) Configuration – T1 Interface (Continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Set DLCI to the DLCI number. This DLCI should match what is programmed in the network Frame Relay switch.</td>
</tr>
<tr>
<td>8</td>
<td>Set mode to ROUTE IP. Using this menu you also have the option to route only IP packets and bridge all other data packets (ROUTE IP/BRIDGE OTHER) or bridge all data packets on this PVC (BRIDGE ALL).</td>
</tr>
<tr>
<td>9</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>

### Layer 2 Protocol (PPP) Configuration – T1 Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select L2 PROTOCOL and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>2</td>
<td>Use the arrow keys to select the PROTOCOL field for the T1 interface. Press &lt;ENTER&gt;. Select PPP from the list of available protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Highlight the CONFIG menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>4</td>
<td>Set mode to ROUTE IP. Using this menu you also have the option to route only IP packets and bridge all other data packets (ROUTE IP/BRIDGE OTHER) or bridge all data packets on this connection (BRIDGE ALL).</td>
</tr>
<tr>
<td>5</td>
<td>Highlight AUTHENTICATION and press &lt;ENTER&gt; to change options related to how the link is established. Default is TX METHOD = NONE and RX METHOD = NONE. If TX METHOD and RX METHOD are set to any option other than NONE, TX/RX USERNAME and PASSWORD options appear. The Total Access 850 supports various combinations of PAP, CHAP, and EAP for PPP authentication. Refer to L2 Protocol (T1 TDM–T1–PPP) &gt; Config &gt; Authentication on page 118 for more details.</td>
</tr>
<tr>
<td>6</td>
<td>Left arrow out of the AUTHENTICATION menus, highlight the PPP menu, and press &lt;ENTER&gt;. Use the PPP menus to configure parameters associated with the PPP link. Refer to L2 Protocol (T1 TDM–T1–PPP) &gt; Config on page 118 for more details.</td>
</tr>
<tr>
<td>7</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>

### Layer 2 Protocol Configuration – Ethernet Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select L2 PROTOCOL and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the CONFIG menu for the ETH (Ethernet) interface and press &lt;ENTER&gt;.</td>
</tr>
</tbody>
</table>
3. Setting the Router Options

For more details on the configuration parameters discussed in this section, refer to the following pages:

Router Ethernet Interface Configuration menus beginning on page 148
Router Network Interface Configuration menus beginning on page 148
Router Default Gateway menus beginning on page 157

### Layer 2 Protocol Configuration – Ethernet Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Set mode to <strong>ROUTE IP</strong>. Using this menu you also have the option to route only IP packets and bridge all other data packets (<em>ROUTE IP/BRIDGE OTHER</em>) or bridge all data packets on this connection (<em>BRIDGE ALL</em>). Refer to <em>L2 Protocol (ALL–ETH–802.3) &gt; Config &gt; Mode</em> on page 144 for more details.</td>
</tr>
<tr>
<td>4</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>

### Router Options – Ethernet Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>ROUTER</strong> and press <code>&lt;ENTER&gt;</code>.</td>
</tr>
<tr>
<td>2</td>
<td>Use the right arrow key to highlight <strong>CONFIG</strong> and press <code>&lt;ENTER&gt;</code>.</td>
</tr>
<tr>
<td>3</td>
<td>Select <strong>INTERFACES</strong> and press <code>&lt;ENTER&gt;</code>. Use the right arrow key to highlight the <strong>SETUP</strong> field for the <strong>ETH</strong> (Ethernet) interface and press <code>&lt;ENTER&gt;</code>.</td>
</tr>
<tr>
<td>4</td>
<td>Highlight the <strong>PRIMARY IP</strong> field and press <code>&lt;ENTER&gt;</code>.</td>
</tr>
<tr>
<td>5</td>
<td>Set the <strong>IP ADDRESS</strong> of the Ethernet port.</td>
</tr>
<tr>
<td>6</td>
<td>Set the <strong>SUBNET MASK</strong> for the Ethernet port.</td>
</tr>
<tr>
<td>7</td>
<td>By default, RIP is disabled on the Ethernet interface. If RIP needs to be enabled, highlight the <strong>RIP</strong> field and press <code>&lt;ENTER&gt;</code>. Set the appropriate <strong>VERSION</strong>, <strong>RIP METHOD</strong>, <strong>DIRECTION</strong>, and <strong>V2 SECRET</strong> (where applicable) to configure RIP on the interface. For more details, refer to <strong>Router &gt; Config &gt; Interfaces (ETH) &gt; Sub-Interface</strong> on page 148.</td>
</tr>
<tr>
<td>8</td>
<td>Press the left arrow key to return to the Ethernet sub-interface menu (displays <strong>PRIMARY IP</strong> and <strong>SECONDARY IP</strong>).</td>
</tr>
<tr>
<td>9</td>
<td>If your application requires additional secondary IP address, highlight the <strong>SECONDARY IP</strong> field and press <code>&lt;ENTER&gt;</code>. The Total Access 850 supports up to 5 additional LAN segments. Enter each additional secondary IP address and corresponding subnet mask. To add a new IP address entry, highlight the <strong>NUM</strong> field and press the <code>&lt;I&gt;</code> key. To delete an existing entry, highlight the <strong>NUM</strong> field for the entry to delete and press the <code>&lt;D&gt;</code> key.</td>
</tr>
<tr>
<td>10</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>
4. Mapping the DS0s

For more details on the configuration parameters discussed in this section, refer to the following pages:

DS0 Map menus beginning on page 180
## DS0 Mapping Instructions

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>DS0 MAPS</strong>.</td>
</tr>
</tbody>
</table>
| 2    | Verify that the **ACTIVE MAP** is set to either **MAP 1** or **MAP 2**. This is the map that is actively running on the unit. The unit has the ability to store two maps.  
  - To edit the current map, press `<ENTER>` on **EDIT/VIEW MAP 1** to view the map. (If Map 1 is the Active Map)  
  - To edit the standby map, press `<ENTER>` on **EDIT/VIEW MAP 2** to view the map. (If Map 2 is the Active Map) |
|      | **NOTE** The **DS0** listed on the left side of the menu corresponds to **DS0s (1 through 24)** on the network T1 interface. At least one **DS0** must be mapped to the **ROUTER** to utilize the Total Access 850 for routing purposes. |
| 3    | Scroll down to the DS0 that will be mapped. (Any DS0 can be mapped to the router.) |
| 4    | Set the **SERVICE** for the DS0 that you are mapping to **TA IAD**. |
| 5    | Set the **PORT** of the DS0 that you are mapping to **ROUTER 64K** or **ROUTER 56K**. |
| 6    | Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map. |
| 7    | Make sure the **ACTIVE MAP** is set to the correct map (the map you want running) before exiting the **DS0 MAPS** menu. |
| 8    | Left arrow back to the main menu. |
Appendix B. Configuring the Unit for Bridging

Initial Setup
It is best to configure Total Access 850 TDM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus. Follow the Layer 2 setup with the data “routing” menus (either **BRIDGE** or **ROUTER**). Establish packet forwarding and blocking using the **SECURITY** menus. Lastly, configure the physical mappings using the **DS0 MAPS** menus.

The following example provides step by step instructions for configuring the Total Access 850 T1 TDM system (**INTERFACES** through **DS0 MAPS**) for a standard bridging application. System Info and System Config parameters should be set according to your system need. Refer to **System Info** on page 73 and **System Config** on page 75 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

- **Network T1 menus beginning on page 94**
- **Ethernet menus beginning on page 101**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>INTERFACES</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>T1</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Right arrow to select <strong>FORMAT</strong> and choose <strong>ESF</strong> or <strong>SF</strong>.</td>
</tr>
</tbody>
</table>

*This format must match the format used by the other units in the network.*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Set the <strong>LINE CODE</strong> to <strong>B8ZS</strong> or <strong>AMI</strong>.</td>
</tr>
</tbody>
</table>

*This line code must match the line code used by the other units in the network.*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Set the <strong>EQUALIZATION</strong> or line build out. The default setting of <strong>0 dB</strong> is usually sufficient.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Set the <strong>CSU LPBK</strong> option to <strong>ENABLE</strong>, <strong>DISABLE</strong>, or <strong>DISABLE ALL</strong> based on whether looping to this unit from another unit will be allowed.</td>
</tr>
</tbody>
</table>
2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

Layer 2 Frame Relay Protocol menus beginning on page 121
Layer 2 PPP Protocol menus beginning on page 118
Layer 2 Ethernet menus beginning on page 144

---

**Ethernet Interface Setup Instructions**

Most applications should not require a manual setup for the Ethernet interface. By default, the Ethernet interface is configured to auto-detect the data rate (as either 10 or 100 Mbps). The following steps disable the auto-negotiation parameter and manually configure the interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>INTERFACES</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>ETH</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Use the right arrow to select <strong>AUTONEGOTIATION</strong> and press <strong>&lt;ENTER&gt;</strong>. Use the down arrow to choose <strong>OFF</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Select the <strong>DATA RATE</strong> field and specify either <strong>10BASET</strong> or <strong>100BASET</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Select the <strong>DUPLEX TYPE</strong> field and specify either <strong>HALF DUPLEX</strong> or <strong>FULL DUPLEX</strong>.</td>
</tr>
</tbody>
</table>

---

**Layer 2 Protocol (FRE) Configuration – T1 Interface**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>L2 PROTOCOL</strong> and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Use the arrow keys to select the <strong>PROTOCOL</strong> field for the <strong>T1</strong> interface. Press <strong>&lt;ENTER&gt;</strong>. Select <strong>FRE</strong> from the list of available protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>T1</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Set the <strong>MAINTENANCE PROTOCOL</strong> to <strong>ANNEX D (ANSI)</strong>, <strong>ANNEX A</strong> (q933a), <strong>LMI</strong>, or <strong>STATIC</strong> (no sig).</td>
</tr>
</tbody>
</table>

**Note**

The **MAINTENANCE PROTOCOL** should be set based on the Frame Relay switch.

| 5    | Down arrow and press **<ENTER>** on **DLCI MAPPING**. Press the right arrow key to create an entry. To create additional entries, highlight the **NUM** field and press the **<I>** key. To delete an entry, highlight the **NUM** field for the entry to delete and press the **<D>** key. |
| 6    | Set **ACTIVE** to **YES**. |
**Layer 2 Protocol (FRE) Configuration – T1 Interface (Continued)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Set DLCI to the DLCI number. This DLCI should match what is programmed in the network Frame Relay switch.</td>
</tr>
<tr>
<td>8</td>
<td>Set mode to <strong>BRIDGE ALL</strong>. Using this menu you also have the option to route only IP packets and bridge all other data packets (<strong>ROUTE IP/BRIDGE OTHER</strong>) or route all IP data packets on this PVC (<strong>ROUTE IP</strong>).</td>
</tr>
<tr>
<td>9</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>

**Layer 2 Protocol (PPP) Configuration – T1 Interface**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>L2 PROTOCOL</strong> and press <code>&lt;ENTER&gt;</code>.</td>
</tr>
<tr>
<td>2</td>
<td>Use the arrow keys to select the <strong>PROTOCOL</strong> field for the <strong>T1</strong> interface. Press <code>&lt;ENTER&gt;</code>. Select <strong>PPP</strong> from the list of available protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>T1</strong> interface and press <code>&lt;ENTER&gt;</code>.</td>
</tr>
<tr>
<td>4</td>
<td>Set mode to <strong>BRIDGE ALL</strong>. Using this menu you also have the option to route only IP packets and bridge all other data packets (<strong>ROUTE IP/BRIDGE OTHER</strong>) or route all IP data packets on this connection (<strong>ROUTE IP</strong>).</td>
</tr>
<tr>
<td>5</td>
<td>Highlight <strong>AUTHENTICATION</strong> and press <code>&lt;ENTER&gt;</code> to change options related to how the link is established. Default is <strong>TX METHOD = NONE</strong> and <strong>RX METHOD = NONE</strong>. If <strong>TX METHOD</strong> and <strong>RX METHOD</strong> are set to any option other than <strong>NONE</strong>, <strong>TX/RX USERNAME</strong> and <strong>PASSWORD</strong> options appear. The Total Access 850 supports various combinations of PAP, CHAP, and EAP for PPP authentication.</td>
</tr>
<tr>
<td>6</td>
<td>Left arrow out of the <strong>AUTHENTICATION</strong> menus, highlight the <strong>PPP</strong> menu, and press <code>&lt;ENTER&gt;</code>. Use the PPP menus to configure parameters associated with the PPP link. Refer to <strong>L2 Protocol (T1 TDM–T1–PPP) &gt; Config</strong> on page 118 for more details.</td>
</tr>
<tr>
<td>7</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>

**Layer 2 Protocol Configuration – Ethernet Interface**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>L2 PROTOCOL</strong> and press <code>&lt;ENTER&gt;</code>.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>ETH</strong> (Ethernet) interface and press <code>&lt;ENTER&gt;</code>.</td>
</tr>
<tr>
<td>3</td>
<td>Set mode to <strong>BRIDGE ALL</strong>. Using this menu you also have the option to route only IP packets and bridge all other data packets (<strong>ROUTE IP/BRIDGE OTHER</strong>) or route all IP data packets on this connection (<strong>ROUTE IP</strong>). Refer to <strong>L2 Protocol (ALL–ETH–802.3) &gt; Config</strong> on page 144 for more details.</td>
</tr>
<tr>
<td>4</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>
3. **Verifying the Bridge Options**

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Bridge menus beginning on page 145*

<table>
<thead>
<tr>
<th>Bridge Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
</tbody>
</table>

4. **Mapping the DS0s**

For more details on the configuration parameters discussed in this section, refer to the following pages:

*DS0 Map menus beginning on page 180*

<table>
<thead>
<tr>
<th>DS0 Mapping Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td><strong>5</strong></td>
</tr>
<tr>
<td><strong>6</strong></td>
</tr>
<tr>
<td><strong>7</strong></td>
</tr>
<tr>
<td><strong>8</strong></td>
</tr>
</tbody>
</table>
Appendix C. Configuring the Unit for Voice Applications

Initial Setup
It is best to configure Total Access 850 TDM applications by following the order of the top-level menus. For example, first configure the system parameters using the SYSTEM INFO and SYSTEM CONFIG menus. Next, configure the Layer 1 parameters using the INTERFACES menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the L2 PROTOCOL menus. Follow the Layer 2 setup with the data “routing” menus (either BRIDGE or ROUTER). Establish packet forwarding and blocking using the SECURITY menus. Lastly, configure the physical mappings using the DS0 MAPS menus.

The following example provides step by step instructions for configuring the Total Access 850 T1 TDM system (INTERFACES through DS0 MAPS) for a standard voice application. System Info and System Config parameters should be set according to your system need. Refer to System Info on page 73 and System Config on page 75 for more details.

1. Setting up the Interfaces
For more details on the configuration parameters discussed in this section, refer to the following pages:

   Network T1 menus beginning on page 94
   FXS menus beginning on page 103

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select INTERFACES.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the CONFIG menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>3</td>
<td>Right arrow to select FORMAT and choose ESF or SF.</td>
</tr>
<tr>
<td>4</td>
<td>Set the LINE CODE to B8ZS or AMI.</td>
</tr>
<tr>
<td>5</td>
<td>Set the EQUALIZATION or line build out. The default setting of 0 dB is usually sufficient.</td>
</tr>
<tr>
<td>6</td>
<td>Set the CSU LPBK option to ENABLE, DISABLE, or DISABLE ALL based on whether looping to this unit from another unit will be allowed.</td>
</tr>
</tbody>
</table>

This format must match the format used by the other units in the network.

This line code must match the line code used by the other units in the network.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>INTERFACES</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the <strong>CONFIG</strong> menu for the FXS interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
</tbody>
</table>
| 3    | Right arrow to select **MODE** and choose **LOOP START**, **GROUND START**, **TANDEM (E&M)**, **TR08 SINGLE**, **TR08 UVG**, or **DPO**.  
  *This mode should be set based on the network configuration and the operation of each FXS port. All FXS ports are independent and do not need to have the same mode.* |
| 4    | Set the **Tx (dB)** or transmit direction level for each port. The default value is recommended. |
| 5    | Set the **Rx (dB)** or received direction level for each port. The default value is recommended. |
| 6    | Set the **SVC MODE** to **IN SERVICE** to activate the port. |
| 7    | Set the **LINE Z** (line impedance) of each port based on the size of the network. The default value is recommended. |
| 8    | Set the **MSG IND** to **DISABLE** or **ENABLE**. When set to **ENABLE**, talk path is always open, even in on-hook conditions, in order for FXS message tones to pass through. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID. |
| 9    | Configure the on-hook battery voltage using the **BATT MODE** field. For most IAD installs, the FXS loop is short with 6 to 7 V present on tip / ring. To reduce power dissipated during off-hook conditions, the battery is lowered for short loop lengths. When set to **AUTO SWITCH**, the IAD uses a higher on-hook battery voltage (48-52 V). When off-hook, it automatically switches to low battery (24-26 V) to minimize power dissipation. When set to **LOW BATTERY** mode, the higher battery is not used and the voltage is a constant 26 V even while on-hook. The tip/ring voltage is reduced to 26 V when using the **LOW BATTERY** mode. |
| 10   | Specify the interval of battery removal during a forward disconnect state using the **FWD DISC TIMER** field. Choices are **FOLLOW SWITCH** (default), **500MS**, **750MS**, **1000MS**, and **2000MS**. When using ATM mode, there is an additional choice of **IGNORE SWITCH**. If the timer is set to **FOLLOW SWITCH**, the Total Access 850 will follow the switch at all times; this is normal operation. If a time period has been selected, the Total Access 850 will remove battery for the specified time period OR as long as the switch requests battery removal, whichever is longer. For example, if the timer expires but the switch continues to request battery removal, the Total Access 850 will follow the switch and continue to remove battery. For ATM mode, if the timer is set to **IGNORE SWITCH**, the IAD will never remove battery. |
2. Mapping the DS0s

For more details on the configuration parameters discussed in this section, refer to the following pages:

DS0 Map menus beginning on page 180

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select DS0 MAPS.</td>
</tr>
</tbody>
</table>
| 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) |
| 3    | Scroll down to the DS0 that will be mapped. |
| 4    | Set the SERVICE for the DS0 that you are mapping to FXS. |
| 5    | Set the PORT of the DS0 that you are mapping. The port number entered must match the voice port the DS0 is being mapped to. RBS (robbed bit signaling) will automatically turn on when a port number has been selected. |
| 6    | Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map. |
| 7    | Make sure the ACTIVE MAP is set to the correct map (the map you want running) before exiting the DS0 MAPS menu. |
| 8    | Left arrow back to the main menu. |
Appendix D. Configuring the Unit for DSX-1 Applications

The Total Access 600 Series systems are available with an integrated DSX-1 interface for both voice and data applications. Regardless of the application (either voice or data), the Total Access 850 has the ability to map DS0s from the network T1 to DS0s on the DSX-1 interface (cross-connect) without affecting the data present on the DS0s. This feature allows the Total Access 850 to support voice with dedicated signaling channels (ISDN), voice with in-channel signaling information (Robbed Bit Signaling (RBS) to a PBX, key system, etc.), as well as clear channel data to an external T1 router.

Initial Setup

It is best to configure Total Access 850 TDM applications by following the order of the top-level menus. For example, first configure the system parameters using the SYSTEM INFO and SYSTEM CONFIG menus. Next, configure the Layer 1 parameters using the INTERFACES menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the L2 PROTOCOL menus. Follow the Layer 2 setup with the data “routing” menus (either BRIDGE or ROUTER). Establish packet forwarding and blocking using the SECURITY menus. Lastly, configure the physical mappings using the DS0 MAPS menus.

The following example provides details for configuring the Total Access 850 to pass analog voice over the DSX-1 interface (using RBS), digital voice (fractional PRI with D-Channel), and data bandwidth. The Total Access 850 provides a single DSX-1 interface, so it is unlikely that your application will require all three features on the DSX-1 interface simultaneously; therefore ignore any steps that do not pertain to your application.

Perform the following steps in order to configure the applications (INTERFACES through DS0 MAPS). SYSTEM INFO and SYSTEM CONFIG parameters should be set according to your system need. Refer to System Info on page 73 and System Config on page 75 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

Network T1 menus beginning on page 94
DSX-1 menus beginning on page 109

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select INTERFACES.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the CONFIG menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>3</td>
<td>Right arrow to select FORMAT and choose ESF or SF.</td>
</tr>
<tr>
<td>4</td>
<td>Set the LINE CODE to B8ZS or AMI.</td>
</tr>
</tbody>
</table>

This format must match the format used by the other units in the network.
2. Mapping the DS0s

For more details on the configuration parameters discussed in this section, refer to the following pages:

*DS0 Map menus beginning on page 180*
## DS0 Mapping Instructions

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>DS0 MAPS</strong>.</td>
</tr>
</tbody>
</table>
| 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)  
   
   *The DS0 listed on the left side of the menu corresponds to DS0s on the network T1 interface. The PORT number identifies the DS0 on the DSX-1 interface. The DS0 and PORT do not need to match; DS0s can be cross-connected from the network T1 to any DS0 on the DSX-1 interface.* |
| 3    | Scroll down to the DS0 that will be mapped. (Any DS0 can be mapped to the DSX-1 interface.) |
| 4    | Set the **SERVICE** for the DS0 that you are mapping to **DSX-1**. |
| 5    | Set the **PORT** of the DS0 that you are mapping. The port number entered specifies the DS0 on the DSX-1 interface and can be set to any available DS0. When mapping voice circuits with dedicated signaling channels, be sure to map the signaling channel to the proper DS0 on the DSX-1 interface. For example, ISDN D channel signaling is normally carried on DS0 24. Unless the equipment connected to the Total Access 850 DSX-1 interface has been specifically programmed, it will expect a D channel on DS0 24. Map DS0 24 to Port 24 to provide the D channel in the appropriate timeslot. |
| 6    | Set **RBS** to **OFF** or **ON** depending on the application. When passing voice circuits with in-channel signaling through to the DSX-1 interface, signaling bits are preserved by setting **RBS to ON**. For clear channel service to the DSX-1 interface (for voice circuits with a dedicated signaling channel and all data) set **RBS to OFF** (which ignores the signaling bits). |
| 7    | Map all the DS0s as desired, and exit this menu by pressing the left arrow button. Your changes will automatically save when exiting the map. |
| 8    | Make sure the **ACTIVE MAP** is set to the correct map (the map you want running) before exiting the **DS0 MAPS** menu. |
| 9    | Left arrow back to the main menu. |
5. APPENDICES (T1 ATM APPLICATIONS)

The following example is for configuring T1 units with ATM firmware. However, all units using ATM firmware (SDSL, ADSL, SHDSL) may be configured in the same manner. To configure ATM Voice applications with other network types, disregard the T1 Interface Setup Instructions and configure your network interface as needed.

Appendix A. Voice Gateway Quick Start Procedure (Voice Turn Up)

A typical VoATM application (see Figure 7) uses a Total Access 850 connected to an ATM network. For voice applications, a Voice Gateway is needed to interface with the PSTN. Jetstream, Tollbridge, CopperCom, and LES-CAS are popular Gateway types.

![Figure 7. Application Diagram](image)

To configure a Total Access 850 for use with the Voice Gateway, you need to know the VPI and VCI used on the ATM network to access the Gateway from this Total Access 850. You also need to know the format for **IDLE CELLS** and whether **DATA SCRAMBLING** is used on this ATM network. The following procedure will help you navigate the Total Access 850 menus for configuring the necessary elements for VoATM with the Voice Gateway.

Perform the following steps in order to configure the application.

**Initial Setup**

It is best to configure Total Access 850 ATM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus.
The following example provides step by step instructions for configuring the Total Access 850 T1 ATM system (INTERFACES and L2 PROTOCOL) for a standard voice application. System Info and System Config parameters should be set according to your system need. Refer to System Info on page 73 and System Config on page 75 for more details.

1. Setting up the Interfaces

For more details on the configuration parameters discussed in this section, refer to the following pages:

*Network T1 menus beginning on page 94*
*FXS menus beginning on page 103*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select INTERFACES.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the CONFIG menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>3</td>
<td>Right arrow to select FORMAT and choose ESF or SF.</td>
</tr>
</tbody>
</table>

**NOTE**
This format must match the format used by the other units in the network.

| 4    | Set the LINE CODE to B8ZS or AMI.                                      |

**NOTE**
This line code must match the line code used by the other units in the network.

| 5    | Set the EQUALIZATION or line build out. The default setting of 0 dB is |
|      | usually sufficient.                                                    |

<p>| 6    | Set the CSU LPBK option to ENABLE, DISABLE, or DISABLE ALL based on    |
|      | whether looping to this unit from another unit will be allowed.       |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>INTERFACES</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>FXS</strong> interface and press &lt;<strong>ENTER</strong>&gt;.</td>
</tr>
<tr>
<td>3</td>
<td>Right arrow to select <strong>MODE</strong> and choose <strong>LOOP START</strong>, <strong>GROUND START</strong>, <strong>TANDEM (E&amp;M)</strong>, <strong>TR08 SINGLE</strong>, <strong>TR08 UVG</strong>, or <strong>DPO</strong>. <strong>&lt;NOTE&gt;</strong>&lt;br&gt;This mode should be set based on the network configuration and the operation of each FXS port. All FXS ports are independent and do not need to have the same mode.**&lt;NOTE&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Set the <strong>Tx</strong> (dB) or transmit direction level for each port. The default value is recommended.</td>
</tr>
<tr>
<td>5</td>
<td>Set the <strong>Rx</strong> (dB) or received direction level for each port. The default value is recommended.</td>
</tr>
<tr>
<td>6</td>
<td>Set the <strong>SVC MODE</strong> to <strong>IN SERVICE</strong> to activate the port.</td>
</tr>
<tr>
<td>7</td>
<td>Set the <strong>LINE Z</strong> (line impedance) of each port based on the size of the network. The default value is recommended.</td>
</tr>
<tr>
<td>8</td>
<td>Set the <strong>MSG IND</strong> to <strong>DISABLE</strong> or <strong>ENABLE</strong>. When set to <strong>ENABLE</strong>, talk path is always open, even in on-hook conditions, in order for FXS message tones to pass through. Disabling this feature will allow higher on-hook voltage but will not allow on-hook messaging other than caller ID.</td>
</tr>
<tr>
<td>9</td>
<td>Configure the on-hook battery voltage using the <strong>BATT MODE</strong> field. For most IAD installs, the FXS loop is short with 6 to 7 V present on tip / ring. To reduce power dissipated during off-hook conditions, the battery is lowered for short loop lengths. When set to <strong>AUTO SWITCH</strong>, the IAD uses a higher on-hook battery voltage (48-52 V). When off-hook, it automatically switches to low battery (24-26 V) to minimize power dissipation. When set to <strong>LOW BATTERY</strong> mode, the higher battery is not used and the voltage is a constant 26 V even while on-hook. The tip/ring voltage is reduced to 26 V when using the <strong>LOW BATTERY</strong> mode.</td>
</tr>
<tr>
<td>10</td>
<td>Specify the interval of battery removal during a forward disconnect state using the <strong>FWD DISC TIMER</strong> field. Choices are <strong>FOLLOW SWITCH</strong> (default), <strong>500MS</strong>, <strong>750MS</strong>, <strong>1000MS</strong>, and <strong>2000MS</strong>. When using ATM mode, there is an additional choice of <strong>IGNORE SWITCH</strong>. If the timer is set to <strong>FOLLOW SWITCH</strong>, the Total Access 850 will follow the switch at all times; this is normal operation. If a time period has been selected, the Total Access 850 will remove battery for the specified time period OR as long as the switch requests battery removal, whichever is longer. For example, if the timer expires but the switch continues to request battery removal, the Total Access 850 will follow the switch and continue to remove battery. For ATM mode, if the timer is set to <strong>IGNORE SWITCH</strong>, the IAD will never remove battery.</td>
</tr>
</tbody>
</table>
2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

Layer 2 ATM Network T1 menus beginning on page 129

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select L2 PROTOCOL and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>2</td>
<td>Use the arrow keys to select the PROTOCOL field for the T1 interface. Press &lt;ENTER&gt;. Select ATM from the list of available protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Use the arrow keys to select the CONFIG menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>4</td>
<td>Highlight the ATM CONFIG menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>5</td>
<td>Enter the IDLE CELLS format for your network.</td>
</tr>
<tr>
<td>6</td>
<td>Set DATA SCRAMBLING appropriately for your network.</td>
</tr>
<tr>
<td>7</td>
<td>Back all the way out to one level to the PVC CONFIG menu, and press &lt;ENTER&gt;. Enter the VPI and VCI values for communicating with that Gateway. (From this menu, the appropriate Voice information for working with the Voice Gateway is entered by selecting VOICE under the CONNECTION field.)</td>
</tr>
</tbody>
</table>
Select **SETUP**, and from the **SETUP** menu, enter the Gateway type under **CALL CONTROL** and enter the VPI and VCI values for communicating with that Gateway. For this application, **CALL CONTROL** and virtual identifier (VPI and VCI) values should be set appropriately for your network.

To verify correct setup, use the **PVC STATUS** menu (under the **STATUS** menu located at **L2 PROTOCOL [0] > STATUS**) to look at the current status of the voice connection. Under **STATUS**, view information about the voice PVC along with information about the POTS ports available on the unit.
Appendix B. RFC1483 Quick Start (IP Routing)

The Total Access 850 allows for complete integration of voice and data delivery from one compact platform (see Figure 10). Once you have completed the voice turn up procedure from the previous example, adding data to the circuit requires some additional setup.

To configure a Total Access 850 for IP routing, you need to know the VPI and VCI values for the data circuit on your network. You also need the IP address of the next hop router in the circuit.

Perform the following steps in order to configure the application.

**Initial Setup**

It is best to configure Total Access 850 ATM applications by following the order of the top-level menus. For example, first configure the system parameters using the **SYSTEM INFO** and **SYSTEM CONFIG** menus. Next, configure the Layer 1 parameters using the **INTERFACES** menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the **L2 PROTOCOL** menus. Follow the Layer 2 setup with the data “routing” menus (either **BRIDGE** or **ROUTER**). Finally, establish packet forwarding and blocking using the **SECURITY** menus.

The following example provides step by step instructions for configuring the Total Access 850 T1 ATM system (**INTERFACES** and **L2 PROTOCOL**) for a standard routing application. System Info and System Config parameters should be set according to your system need. Refer to **System Info** on page 73 and **System Config** on page 75 for more details.

**1. Setting up the Interfaces**

For more details on the configuration parameters discussed in this section, refer to the following pages:

- Network T1 menus beginning on page 94
- Ethernet menus beginning on page 101
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>INTERFACES</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>T1</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Right arrow to select <strong>FORMAT</strong> and choose <strong>ESF</strong> or <strong>SF</strong>.</td>
</tr>
</tbody>
</table>

**NOTE**

*This format must match the format used by the other units in the network.*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Set the <strong>LINE CODE</strong> to <strong>B8ZS</strong> or <strong>AMI</strong>.</td>
</tr>
</tbody>
</table>

**NOTE**

*This line code must match the line code used by the other units in the network.*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Set the <strong>EQUALIZATION</strong> or line build out. The default setting of <strong>0 dB</strong> is usually sufficient.</td>
</tr>
<tr>
<td>6</td>
<td>Set the <strong>CSU LPBK</strong> option to <strong>ENABLE</strong>, <strong>DISABLE</strong>, or <strong>DISABLE ALL</strong> based on whether looping to this unit from another unit will be allowed.</td>
</tr>
</tbody>
</table>

---

**Ethernet Interface Setup Instructions**

Most applications should not require a manual setup for the Ethernet interface. By default, the Ethernet interface is configured to auto-detect the data rate (as either 10 or 100 Mbps). The following steps disable the auto-negotiation parameter and manually configure the interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>INTERFACES</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>ETH</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Use the right arrow to select <strong>AUTONEgotIATION</strong> and press <strong>&lt;ENTER&gt;</strong>. Use the down arrow to choose <strong>OFF</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Select the <strong>DATA RATE</strong> field and specify either <strong>10BaseT</strong> or <strong>100BaseT</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Select the <strong>DUPLEX TYPE</strong> field and specify either <strong>HALF DUPLEX</strong> or <strong>FULL DUPLEX</strong>.</td>
</tr>
</tbody>
</table>
2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

Layer 2 ATM Network Interface Protocol menus beginning on page 129

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select L2 PROTOCOL and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>2</td>
<td>Use the arrow keys to select the PROTOCOL field for the T1 interface. Press &lt;ENTER&gt;. Select ATM from the list of available protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Use the arrow keys to select the CONFIG menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>4</td>
<td>Highlight the ATM CONFIG menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>5</td>
<td>Enter the IDLE CELLS format for your network.</td>
</tr>
<tr>
<td>6</td>
<td>Set DATA SCRAMBLING appropriately for your network.</td>
</tr>
<tr>
<td>7</td>
<td>Back all the way out to one level to the PVC CONFIG menu, and press &lt;ENTER&gt;. Enter the VPI and VCI values for communicating with that Gateway. Select ROUTER under the CONNECTION field.</td>
</tr>
<tr>
<td>8</td>
<td>Select the SETUP menu and configure the virtual circuit for IP or PPP operation. (Our example selects IP.) Refer to L2 Protocol (T1 ATM–T1–ATM) &gt; Config &gt; PVC Config &gt; Connection on page 131 for more details.</td>
</tr>
<tr>
<td>9</td>
<td>Set mode to ROUTE IP. Using this menu you also have the option to route only IP packets and bridge all other data packets (ROUTE IP/BRIDGE OTHER) or bridge all data packets on this connection (BRIDGE ALL). Refer to L2 Protocol (T1 ATM–T1–ATM) &gt; Config &gt; PVC Config &gt; Setup (Router) on page 131 for more details.</td>
</tr>
<tr>
<td>10</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>
3. Setting the Router Options

For more details on the configuration parameters discussed in this section, refer to the following pages:

- Router Ethernet Interface Configuration menus beginning on page 148
- Router Network Interface Configuration menus beginning on page 148
- Router Default Gateway menus beginning on page 157

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select ROUTER and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>2</td>
<td>Use the right arrow key to highlight CONFIG and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>3</td>
<td>Select INTERFACES and press &lt;ENTER&gt;. Use the right arrow key to highlight the SETUP field for the ETH (Ethernet) interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>4</td>
<td>Highlight the PRIMARY IP field and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>5</td>
<td>Set the IP ADDRESS of the Ethernet port.</td>
</tr>
<tr>
<td>6</td>
<td>Set the SUBNET MASK for the Ethernet port.</td>
</tr>
<tr>
<td>7</td>
<td>By default, RIP is disabled on the Ethernet interface. If RIP needs to be enabled, highlight the RIP field and press &lt;ENTER&gt;. Set the appropriate VERSION, RIP METHOD, DIRECTION, and V2 SECRET (where applicable) to configure RIP on the interface. For more details, refer to Router &gt; Config &gt; Interfaces (ETH) &gt; Sub-Interface on page 148.</td>
</tr>
<tr>
<td>8</td>
<td>Press the left arrow key to return to the Ethernet sub-interface menu (displays PRIMARY IP and SECONDARY IP).</td>
</tr>
<tr>
<td>9</td>
<td>If your application requires additional secondary IP address, highlight the SECONDARY IP field and press &lt;ENTER&gt;. The Total Access 850 supports up to 5 additional LAN segments. Enter each additional secondary IP address and corresponding subnet mask. To add a new IP address entry, highlight the NUM field and press the &lt;I&gt; key. To delete an existing entry, highlight the NUM field for the entry to delete and press the &lt;D&gt; key.</td>
</tr>
<tr>
<td>10</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select ROUTER and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>2</td>
<td>Use the right arrow key to highlight CONFIG and press &lt;ENTER&gt;.</td>
</tr>
</tbody>
</table>
### Router Options – T1 Interface (L2 Protocol = ATM) *(Continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Select <strong>INTERFACES</strong> and press <strong>&lt;ENTER&gt;</strong>. Use the right arrow key to highlight the <strong>SETUP</strong> field for the <strong>T1</strong> interface and press <strong>&lt;ENTER&gt;</strong>. Each virtual circuit on the <strong>T1</strong> interface defined in the <strong>PVC CONFIG</strong> has a separate listing in the <strong>ROUTER INTERFACES</strong> table.</td>
</tr>
<tr>
<td>4</td>
<td>Set <strong>ACTIVE</strong> to <strong>YES</strong> to activate the virtual circuit.</td>
</tr>
<tr>
<td>5</td>
<td>Enter the appropriate <strong>VPI</strong> and <strong>VCI</strong> values.</td>
</tr>
<tr>
<td>6</td>
<td>Select the desired <strong>ADDRESS MODE</strong>. Refer to <em>Address Mode</em> on page 151 for more details.</td>
</tr>
<tr>
<td>7</td>
<td>Enter the Total Access 850 <strong>LOCAL IP ADDRESS</strong> and corresponding <strong>IP NETMASK</strong> for the selected virtual circuit.</td>
</tr>
<tr>
<td>8</td>
<td>Enter the IP address for the next hop router in the <strong>FAR-END IP ADDRESS</strong> field.</td>
</tr>
<tr>
<td>9</td>
<td>For NAT configuration, refer to <em>Appendix C. RFC1483 Quick Start (IP Routing with NAT)</em> on page 209.</td>
</tr>
<tr>
<td>10</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>

### Router Options – Setting the Default Gateway

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select <strong>ROUTER</strong> and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Use the right arrow key to highlight <strong>CONFIG</strong> and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Select <strong>ROUTES</strong> and press <strong>&lt;ENTER&gt;</strong>. Set the <strong>DEFAULT GATEWAY</strong> field to the appropriate IP address.</td>
</tr>
<tr>
<td>4</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>
Appendix C. RFC1483 Quick Start (IP Routing with NAT)

To illustrate the use of NAT, consider the example from Appendix B. RFC1483 Quick Start (IP Routing) on page 204. To add NAT to the IP routing example, use the NAT menus.

For more details on the configuration parameters discussed in this section, refer to the following pages:

Router Network Interface Configuration menus beginning on page 148

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The NAT menu is found under ROUTER &gt; CONFIGURATION &gt; INTERFACES &gt; SETUP &gt; NAT. The NAT menu can easily be accessed by pressing &lt;CTRL+N&gt;.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong> The network interface will not appear if a virtual circuit is not defined using the L2 PROTOCOL menus.</td>
</tr>
<tr>
<td>2</td>
<td>From the NAT menu, set PORT TRANSLATION to ENABLED. (This will enable translation and populate the corresponding NAT menu options.)</td>
</tr>
<tr>
<td>3</td>
<td>Set PUBLIC IP ADDRESS MODE to either INTERFACE or SPECIFIED.</td>
</tr>
<tr>
<td></td>
<td>• INTERFACE (default) configures NAT to use the IP address already assigned to the interface. (In other words, the interface address and the NAPT address are the same.)</td>
</tr>
<tr>
<td></td>
<td>• SPECIFIED allows you to define a different IP address for the NAPT address (public address for private addresses to be translated into).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>From the TRANSLATION TABLE menu, create a new entry by using the right arrow to enter the table. Additional entries can be created by highlighting the first entry index number and pressing the &lt;I&gt; key. Entries can be deleted by highlighting the selected entry index number and pressing the &lt;D&gt; key.</td>
</tr>
<tr>
<td>5</td>
<td>Create specific NAT translations based on your application.</td>
</tr>
<tr>
<td></td>
<td><strong>PUBLIC IP ADDRESS MODE</strong> Use the configured interface IP address as the NAPT address or use SPECIFIED to set a different public address to be used for the translation.</td>
</tr>
<tr>
<td></td>
<td><strong>PROTOCOL MODE</strong> Protocol for this translation. (TCP, UCP, ICMP, TCP or UDP, TCP UDP or ICMP, All, Specified, and NONE.)</td>
</tr>
<tr>
<td></td>
<td><strong>PRIVATE ADDRESS MODE</strong> SPECIFIED or ANY INTERNAL. Choosing SPECIFIED brings up the PRIVATE ADDRESS option.</td>
</tr>
<tr>
<td></td>
<td><strong>TRANSLATE BODY</strong> 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.</td>
</tr>
</tbody>
</table>
Appendix D. RFC 1483 Quick Start (Bridging)

Initial Setup
It is best to configure Total Access 850 ATM applications by following the order of the top-level menus. For example, first configure the system parameters using the System Info and System Config menus. Next, configure the Layer 1 parameters using the Interfaces menu. Once the Layer 1 information is configured, proceed to the Layer 2 setup using the L2 Protocol menus. Follow the Layer 2 setup with the data “routing” menus (either Bridge or Router). Finally, establish packet forwarding and blocking using the Security menus.

The following example provides step by step instructions for configuring the Total Access 850 T1 ATM system (Interfaces and L2 Protocol) for a standard bridging application. System Info and System Config parameters should be set according to your system need. Refer to System Info on page 73 and System Config on page 75 for more details.

1. Setting up the Interfaces
For more details on the configuration parameters discussed in this section, refer to the following pages:

   Network T1 menus beginning on page 94
   Ethernet menus beginning on page 101

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the main menu, select Interfaces.</td>
</tr>
<tr>
<td>2</td>
<td>Highlight the Config menu for the T1 interface and press &lt;ENTER&gt;.</td>
</tr>
<tr>
<td>3</td>
<td>Right arrow to select Format and choose ESF or SF.</td>
</tr>
</tbody>
</table>

   **Note** This format must match the format used by the other units in the network.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Set the Line Code to B8ZS or AMI.</td>
</tr>
</tbody>
</table>

   **Note** This line code must match the line code used by the other units in the network.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Set the Equalization or line build out. The default setting of 0 dB is usually sufficient.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Set the CSU LPBK option to Enable, Disable, or Disable All based on whether looping to this unit from another unit will be allowed.</td>
</tr>
</tbody>
</table>
2. Configuring the Layer 2 Protocol

For more details on the configuration parameters discussed in this section, refer to the following pages:

Layer 2 ATM Network Interface Protocol menus beginning on page 129

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>From the main menu, select <strong>INTERFACES</strong>.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Highlight the <strong>CONFIG</strong> menu for the <strong>ETH</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Use the right arrow to select <strong>AUTONEGOTIATION</strong> and press <strong>&lt;ENTER&gt;</strong>. Use the down arrow to choose <strong>OFF</strong>.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Select the <strong>DATA RATE</strong> field and specify either <strong>10BASET</strong> or <strong>100BASET</strong>.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Select the <strong>DUPLEX TYPE</strong> field and specify either <strong>HALF DUPLEX</strong> or <strong>FULL DUPLEX</strong>.</td>
</tr>
</tbody>
</table>

---

Layer 2 Protocol (ATM) Configuration – T1 Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>From the main menu, select <strong>L2 PROTOCOL</strong> and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Use the arrow keys to select the <strong>PROTOCOL</strong> field for the <strong>T1</strong> interface. Press <strong>&lt;ENTER&gt;</strong>. Select <strong>ATM</strong> from the list of available protocols.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Use the arrow keys to select the <strong>CONFIG</strong> menu for the <strong>T1</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Highlight the <strong>ATM CONFIG</strong> menu for the <strong>T1</strong> interface and press <strong>&lt;ENTER&gt;</strong>.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Enter the <strong>IDLE CELLS</strong> format for your network.</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Set <strong>DATA SCRAMBLING</strong> appropriately for your network.</td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>Back all the way out to one level to the <strong>PVC CONFIG</strong> menu, and press <strong>&lt;ENTER&gt;</strong>. Enter the VPI and VCI values for communicating with that Gateway. Select <strong>ROUTER</strong> under the <strong>CONNECTION</strong> field.</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>Select the <strong>SETUP</strong> menu and configure the virtual circuit for <strong>IP</strong> or <strong>PPP</strong> operation. (Our example selects <strong>IP</strong>.) Refer to L2 Protocol (T1 ATM–T1–ATM) &gt; Config &gt; PVC Config &gt; Setup (Router) on page 131 for more details.</td>
</tr>
</tbody>
</table>
3. Verifying the Bridge Options

For more details on the configuration parameters discussed in this section, refer to the following pages:

Bridge menus beginning on page 145

**Layer 2 Protocol (ATM) Configuration – T1 Interface (Continued)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Set mode to <strong>ROUTE IP</strong>. Using this menu you also have the option to route only IP packets and bridge all other data packets (<strong>ROUTE IP/BRIDGE OTHER</strong>) or bridge all data packets on this connection (<strong>BRIDGE ALL</strong>). Refer to <em>L2 Protocol (T1 ATM–T1–ATM) &gt; Config &gt; PVC Config &gt; Setup (V35)</em> on page 133 for more details.</td>
</tr>
<tr>
<td>10</td>
<td>Left arrow back to the main menu to save the changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
</tbody>
</table>
### DETAIL LEVEL PROCEDURES

<table>
<thead>
<tr>
<th>DLP-1</th>
<th>Connecting a VT100 Terminal or PC to the CRAFT Port</th>
<th>215</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP-2</td>
<td>Logging in to the System</td>
<td>217</td>
</tr>
<tr>
<td>DLP-3</td>
<td>Setting IP Parameters for the Total Access 850</td>
<td>219</td>
</tr>
<tr>
<td>DLP-4</td>
<td>Verifying Communications Over an IP LAN</td>
<td>221</td>
</tr>
<tr>
<td>DLP-5</td>
<td>Connecting to the Total Access 850 Using Telnet</td>
<td>225</td>
</tr>
<tr>
<td>DLP-6</td>
<td>Adding/Removing Users and Changing Password Security Levels</td>
<td>229</td>
</tr>
<tr>
<td>DLP-7</td>
<td>Updating the Firmware using TFTP</td>
<td>233</td>
</tr>
<tr>
<td>DLP-8</td>
<td>Updating the Firmware using XMODEM</td>
<td>237</td>
</tr>
<tr>
<td>DLP-9</td>
<td>Saving the Current Configuration Using TFTP</td>
<td>239</td>
</tr>
<tr>
<td>DLP-10</td>
<td>Loading a Configuration Using TFTP</td>
<td>241</td>
</tr>
<tr>
<td>DLP-11</td>
<td>Saving and Transferring a Current Configuration Using XMODEM</td>
<td>245</td>
</tr>
<tr>
<td>DLP-12</td>
<td>Loading a Configuration Using XMODEM</td>
<td>247</td>
</tr>
<tr>
<td>DLP-13</td>
<td>Saving and Loading Text Configuration using Terminal Command Line</td>
<td>249</td>
</tr>
<tr>
<td>DLP-14</td>
<td>A.03 to A.04 Firmware Upgrade</td>
<td>253</td>
</tr>
<tr>
<td>DLP-15</td>
<td>Using the ADTRAN Utility Syslog</td>
<td>257</td>
</tr>
<tr>
<td>DLP-16</td>
<td>Connecting the Alarm Contacts and the External Input</td>
<td>261</td>
</tr>
<tr>
<td>DLP-17</td>
<td>Configuring the Total Access 850 for Dual T1 Maps</td>
<td>265</td>
</tr>
</tbody>
</table>
DLP-1  Connecting a VT100 Terminal or PC to the CRAFT Port

Introduction

Total Access 850 shelf management and provisioning are facilitated by a series of intuitive menus that are accessible on a computer screen. Connecting either a VT100 terminal or a PC emulating a VT100 terminal to the RJ-45 CRAFT port on the rear of the unit or the DB-9 CRAFT interface on the RCU faceplate allows access to the menus and management features of Total Access 850. This section specifies how to connect the VT100 terminal or PC to the Total Access 850.

The front CRAFT interface for the Total Access 850 is located on the faceplate of the RCU and is a DB-9 connector. Access can also be made to the Total Access 850 from the back of the unit through the RJ-45 interface labeled CRAFT, located on the back of the unit. A special ADTRAN adapter is required for access to this rear port.

Prerequisite Procedures

The Total Access 850 must be powered for terminal communication to function.

Tools and Materials Required

• VT100 compatible terminal or computer with terminal emulation software. A VT100 emulation program is provided with your shipment as part of the ADTRAN Utilities software suite.
• Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
• DB-9 male to DB-9 female serviceable (customer-provided) for connecting to the RCU faceplate CRAFT port
• DB-9 female to RJ-45 female adapter (ADTRAN proprietary) for connecting to the CRAFT port on the rear of the unit.

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

Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Connecting a VT100 terminal to Total Access 850:
   - Set the parameters of the VT100 terminal or PC to:
     - 9600 baud rate
     - 8 data bits
     - No parity
     - 1 stop bit
     - No flow control
   - If the terminal has a parallel setting, disable it and use the serial port.

   Using the RCU CRAFT Port
   - Plug the DB-9 male end of the data cable into the Total Access 850 CRAFT port on the front of the RCU. Make the connection to the VT100 terminal as appropriate for your equipment.

   Using the rear CRAFT Port
   - Plug the RJ-45 end of the data cable into the Total Access 850 CRAFT port on the back of the unit. Make the connection to the VT100 terminal as appropriate for your equipment.

2. Connect a PC emulating a VT-100 terminal to Total Access 850.
   Most personal computers (PCs) or laptops can run communications software that emulates a VT100 terminal. Examples include Windows programs such as Terminal® or Hyperterminal®. However, there are many other adequate, commercially available software packages which will allow your PC or laptop to emulate a VT100 terminal.
   - Set the parameters of the communications software to:
     - 9600 baud rate
     - 8 data bits
     - No parity
     - 1 stop bit
     - No flow control
   - Set the PC for direct connect on the appropriate com port (instead of dial up connection).

   Using the RCU CRAFT Port
   - Plug the DB-9 male end of the data cable into the Total Access 850 CRAFT port on the front of the unit. Make connection to the PC or laptop as appropriate for your equipment.

   Using the rear CRAFT Port
   - Plug the RJ-45 end of the data cable into the Total Access 850 CRAFT port on the back of the unit. Make connection to the PC or laptop as appropriate for your equipment.

You are now ready to log in to the Total Access 850, as described in DLP-2, Logging in to the System.
DLP-2  Logging in to the System

Introduction

Once connected to the Total Access 850, you must login to the system to gain access to the management and provisioning functions. This DLP assumes you are connected to the Total Access 850 and provides specific steps for logging into the system.

Prerequisite Procedures

Complete DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port.

---

**WARNING**

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

---

**CAUTION**

Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.

---

**NOTE**

After the IP parameters have been provisioned (see DLP-3, Setting IP Parameters for the Total Access 850), you can also log in via Telnet.
Perform the steps below in the order listed.

1. After connecting to the system, press any key to display the Login screen shown here. The blinking cursor at the Login field indicates that a password must be entered.

2. Enter the password for the Total Access 850 at the Login field. There is no manufacturer's default password; press <Enter> to enter the Total Access 850 menus.

3. Upon entering the correct password, the Total Access 850 main menu is displayed as shown below.

4. You are now logged in to the Total Access 850 menu system.
DLP-3  Setting IP Parameters for the Total Access 850

Introduction

The Total Access 850 comes pre-programmed for default Telnet access. The following IP parameters apply:

- IP Address: 10.0.0.1
- Subnet Mask: 255.255.255.0
- User: guest
- Password: password

For security purposes, change the default Telnet password during the initial unit configuration. (Refer to System Config > Management > Telnet Access > User List on page 77 for more details.)

If the Total Access 850 is connected to an IP network for Telnet, TFTP, or SNMP management, there are several IP parameters which must be set for the unit to communicate with the network. These parameters are described in this DLP along with the procedures for setting them.

Please see your Network Administrator for the proper assignment of the following parameters: IP ADDRESS, SUBNET MASK, and DEFAULT GATEWAY.

Prerequisite Procedures

This procedure assumes that the Total Access 850 unit is connected to an IP network and is powered up.

Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the Total Access 850 (customer-provided)
- DB-9 male to DB-9 female adapter (customer-provided) for connecting to the RCU faceplate CRAFT port
- DB-9 female to RJ-45 female adapter (ADTRAN proprietary) for connecting to the CRAFT port on the rear of the unit

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

Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Connect the Total Access 850 unit to your VT100 system (details found in DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port).
2. Log in to the system.
3. From the ROUTER/CONFIG menu, select the INTERFACES option and press <Enter>.
4. Select SETUP for the ETH interface, then PRIMARY IP.
5. Highlight the IP ADDRESS field and press <Enter>. Enter the appropriate IP address (as given by your system administrator).
6. Highlight the SUBNET MASK field and press <Enter>. Enter the appropriate subnet mask (as given by your system administrator).
7. Highlight the DEFAULT GATEWAY field and press <Enter>. Enter the appropriate default gateway (as given by your system administrator).
8. Press the left arrow key to highlight the PRIMARY IP submenu. This action saves your changes and requires confirmation.
9. Escape out to the ROUTER menu and log off by pressing <CTRL+L>. 
DLP-4  Verifying Communications Over an IP LAN

Introduction

When the Ethernet port is connected to a local area network (LAN), test steps must be performed on the Total Access 850 to ensure that the unit is communicating properly over the network. This procedure outlines those steps.

Prerequisite Procedures

Before beginning this procedure, the unit should be physically connected to the LAN and the provisioning tasks detailed in DLP-3, Setting IP Parameters for the Total Access 850, should be complete.

Tools and Materials Required

- Access to a PC or other computer connected to the LAN

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

CAUTION  Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Verify the Total Access 850 IP address.

   If you do not already have the IP Address for the Total Access 850, obtain it from the network administrator or manually check for the address in the ROUTER CONFIG/INTERFACE/SETUP/PRIMARY IP/IP ADDRESS menu of the Network Management interface.

   **NOTE** You must log in with a security level of 2 to modify the IP parameters on the Total Access 850. (See DLP-2, Logging in to the System for more details.)

2. Ping the Total Access 850 unit from a remote computer on the network.

   Using a remote computer system connected to the LAN, perform an ICMP Ping on the IP Address of the Total Access 850. Verify that the unit responds properly.

   If the Total Access 850 fails to respond, try the following:
   - Verify that the proper IP Address, Subnet Mask, and Default Gateway are provisioned in the unit (see DLP-2, Logging in to the System, for details).
   - Verify that the Total Access 850 is properly cabled into the LAN and that the Ethernet cable is properly seated in the RJ-45 LAN jack on the rear of the unit.
   - Verify the link light on the RCU is lit. If not lit, check the cabling between the hub and the shelf.
   - If the Total Access 850 is connected to a hub or other network device that provides a carrier sense light for each port, verify that the carrier sense light for the port to which the Total Access 850 is connected is lit. If this light is not lit, check the cabling between the hub and the shelf.
   - Verify the IP Address, Subnet Mask, and Default Gateway on the remote computer system.
   - Use Ethernet straight-through cable for connection to hub or switch. Use Ethernet crossover if connecting to 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, press `<CTRL+C>` to get the program to stop.

3. Telnet to the Total Access 850.
From the same computer used in the previous step, Telnet to the Total Access 850 and verify that the Telnet session is properly opened (see DLP-5, Connecting to the Total Access 850 Using Telnet). Once the Telnet session is established, press <CTRL+L> to logout and close the session.

**NOTE**

Refer to the documentation of the computer system if you are unsure how to perform a Telnet. Most computers running a networked version of Microsoft Windows™ or UNIX allow a Telnet to be performed by simply typing `Telnet <IP Address>` at a command line prompt. Telnet is a utility common on many local area networks that allows remote access to another computer or piece of equipment.
### DLP-5  Connecting to the Total Access 850 Using Telnet

#### Introduction

The Total Access 850 comes pre-programmed for default Telnet access. The following IP parameters apply:

- IP Address: 10.0.0.1
- Subnet Mask: 255.255.255.0
- User: guest
- Password: password

For security purposes, change the default Telnet password during the initial unit configuration. (Refer to System Config > Management > Telnet Access > User List on page 77 for more details.)

If the Total Access 850 is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. This procedure details the steps which must be performed to Telnet into the unit.

#### Prerequisite Procedures

Complete DLP-3, Setting IP Parameters for the Total Access 850 and DLP-4, Verifying Communications Over an IP LAN.

#### Tools and Materials Required

- Access to a PC or other computer connected to the LAN.

---

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

**CAUTION** Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Connect the computer to the Total Access 850 RCU faceplate CRAFT or rear CRAFT port (details in DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port).

2. Log in to the unit.

3. Select the **SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS** menu and set the **TELNET ACCESS** to **ON**.

4. Under the **SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS** menu, select the **TELNET USER LIST**; press <Enter>. The following screen appears.

![Image of Telnet User List](image)

5. Use the right arrow key to select the **NAME** field; press <Enter>. Enter a username to use for Telnet logins.

6. Use the right arrow key to select **PASSWORD**; press <Enter>. Enter a password to use for Telnet logins.

7. Use the right arrow key to select **IDLE TIME (MINS)**; press <Enter>. This field defines the amount of time in minutes the Telnet session may be idle before the user is logged off. The range is 1-255 and the default value is 10 minutes. Enter the appropriate **IDLE TIME**.

8. Use the right arrow key to select **LEVEL**; press <Enter>. Select the appropriate security level. (Reference DLP-6, Adding/Removing Users and Changing Password Security Levels, for security level definitions.)

9. Press the left arrow key until prompted to save the Telnet changes. Respond with **Y** to confirm the request.

10. This completes the addition of one Telnet user. Repeat steps 1-11 for each additional Telnet user access.

11. Press **<CTRL+L>** to log off the Total Access 850 terminal menu system.
12. From a remote computer system connected to the LAN, Telnet to the Total Access 850.

Refer to the documentation of the computer system if you are unsure how to perform a Telnet. Most computers running a networked version of Microsoft Windows™ or UNIX allow a Telnet to be performed by simply typing “Telnet <IP Address>” at a command line prompt. Telnet is a utility common on many local area networks that allows remote access to another computer or piece of equipment.

The following screen appears.

13. Enter the user name assigned in step 5 and press enter. The following screen appears.
14. Enter the password assigned in step 6.

After entering the correct password, the Total Access 850 main menu is displayed (see below):

![Telnet Connection Screen]

15. After completing your configuration changes they are automatically saved (or manually save them by pressing `<CTRL+W>`), press `<CTRL+L>` to log off the menus, and close the Telnet window.
DLP-6 Adding/Removing Users and Changing Password Security Levels

Introduction

Password security levels only apply to users connecting to the Total Access 850 system through Telnet access. All connections made through the CRAFT interface ALWAYS have maximum security rights.

All menu items in the Total Access 850 are protected by passwords of varying security levels. By assigning different passwords to different security levels, the Total Access 850 System Administrator can control which users can view or change various menu items. You can assign multiple passwords at the same access level. This way, different users with the same access privileges can have different passwords. This procedure details the steps which must be performed to add/remove user profiles and assign password security levels in the Total Access 850.

Tools and Materials Required

- VT100 compatible terminal or PC with VT100 terminal emulation software

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

Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Connect to the Total Access 850 using either the 10BASET, rear CRAFT, or RCU faceplate CRAFT interfaces.

   If you are not already connected to the unit’s RCU faceplate CRAFT or rear CRAFT interface (either with a VT100 compatible terminal or with a PC running VT100 emulation software), follow the procedure in DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port.

   Alternately, if the unit is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. Use the procedures in DLP-3, Setting IP Parameters for the Total Access 850 and DLP-5, Connecting to the Total Access 850 Using Telnet, to connect to the 10BASET interface.

2. Log in to the unit using the read-write password (see DLP-2, Logging in to the System, for more details).

   Password security levels only apply to users connecting to the Total Access 850 system through Telnet access. All connections made through the CRAFT interface ALWAYS have maximum security rights.

3. Go to the SYSTEM CONFIG/MANAGEMENT/TELNET ACCESS menu, select the USER LIST menu, and press <Enter>.

4. Add a new user profile and password by selecting the first column (0) and pressing <I> (for insert).

5. Give the new user profile a name by selecting the NAME field, pressing <Enter>, and typing the user defined name.

6. Personalize the password for the appropriate level by selecting the PASSWORD field, pressing <Enter>, then typing the appropriate password. You will have to type the new password again to confirm it.

   Passwords for the Total Access 850 system are case sensitive. There is no default password for a new user (i.e., you can configure a user as blank with no password). The current password displays as a series of asterisks (********).

7. Select the IDLE TIME field and press <Enter>. This field defines the amount of time in minutes the session may be idle before the user is logged off. The range is 1-255 and the default value is 10.
8. Determine the password level for the corresponding label. The Total Access 850 contains seven different password levels. The following chart gives a brief description of each level.

<table>
<thead>
<tr>
<th>Select Level...</th>
<th>If you want the user to....</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATUS</td>
<td>Have read-only permission for all menu items - <strong>minimum rights</strong></td>
</tr>
<tr>
<td>VOICE</td>
<td>Have read permission for all menu items and permission to use test commands</td>
</tr>
<tr>
<td>ROUTER</td>
<td>Have access to all commands except passwords, flash download, authentication methods, interface configurations, and Telnet security levels.</td>
</tr>
<tr>
<td>CONFIG</td>
<td>Have access to all commands except passwords, flash download, authentication methods, and Telnet security levels.</td>
</tr>
<tr>
<td>SUPPORT</td>
<td>Have access to all commands except passwords and Telnet security levels.</td>
</tr>
<tr>
<td>FULL</td>
<td>Have permission to edit every menu item, including creating and editing passwords -- <strong>maximum rights</strong></td>
</tr>
<tr>
<td>ROUTER ONLY</td>
<td>Have read access to all menu items and write access to only the router menu.</td>
</tr>
</tbody>
</table>

9. Assign the password level to the appropriate label by selecting the **LEVEL** field and choosing the level decided upon in Step 8.
DLP-7  Updating the Firmware using TFTP

Introduction

The Total Access 850 supports firmware updates using TFTP or XMODEM. (Use the 10/100BASET Ethernet port and TFTP from a network server, or use XMODEM and the RCU faceplate CRAFT or rear CRAFT interfaces.) This DLP provides the steps for a successful firmware upgrade using the 10/100BASET Ethernet port and a TFTP server. (See DLP-8, Updating the Firmware using XMODEM, for instructions on using XMODEM.)

Tools and Materials Required

- A PC with Telnet client software
- A TFTP server accessible on the local network

A TFTP server is provided as part of the ADTRAN Utilities software suite supplied with your shipment.

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

CAUTION  Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Connect to the Total Access 850 using the **10/100BASET** interface.
   
   If you are not already connected to the unit’s **ETHERNET** port using Telnet client software, use the procedure in DLP-5, *Connecting to the Total Access 850 Using Telnet*, to connect to the unit.

2. Log in to the unit using the read-write password (see DLP-2, *Logging in to the System* for details).

3. Verify the TFTP server is running on the network. The user may ping the TFTP server from the Total Access 850 to verify communication.

   **NOTE**

   An A TFTP server ships as part of the ADTRAN Utilities. If using ADTRAN Utilities, choose
   START > PROGRAMS > ADTRAN UTILITIES > TFTP SERVER to start the server.

4. Download the firmware upgrade file to your computer.

   **NOTE**

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

5. Go to the **SYSTEM UTILITY** menu and select the **UPDATE FIRMWARE** menu; press <Enter>.

6. Go to the **TRANSFER METHOD** menu and select **TFTP**.

7. Set the **TFTP SERVER ADDRESS** to the IP address of the machine running the TFTP server program.

   **NOTE**

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

8. Enter the filename of the update file into the **TFTP SERVER FILENAME** field. If the file is located in a directory other than **ADTNUTIL**, the entire path and filename are required.
9. Select **START TRANSFER** to start the update. Enter **Y** to confirm the upgrade.

Prior to the start of the upgrade, the transfer status will display **IDLE**. During the TFTP upload process, various status messages display in **CURRENT UPDATE STATUS** to indicate progress. The following table describes these messages.

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transferring... [X KB]</td>
<td>Indicates communication with the TFTP network server has been established and the update file is being transferred between the Total Access 850 and the TFTP network server.</td>
</tr>
<tr>
<td>Flash Programmed Successfully</td>
<td>The unit has been upgraded successfully.</td>
</tr>
<tr>
<td>Loaded code ver x.x.x chksum = xxxx</td>
<td>Unit displays the version and checksum of the upgraded code.</td>
</tr>
<tr>
<td>Resetting ....</td>
<td>Unit is power cycling.</td>
</tr>
<tr>
<td>RECV Error</td>
<td>Unit will display this message if server filename is incorrect.</td>
</tr>
<tr>
<td>Can not start tftp client <strong>Reload</strong></td>
<td>Unit will display this message if TFTP server address is incorrect.</td>
</tr>
<tr>
<td>Transfer aborted</td>
<td>User has selected <strong>ABORT TRANSFER.</strong></td>
</tr>
</tbody>
</table>

10. When the update has successfully completed, **FLASH PROGRAMMED SUCCESSFULLY** displays briefly in the **TRANSFER STATUS** field. This will be followed by a **LOADED CODE VER X.X.X CHKSUM = XXXX** message. Finally the **TRANSFER STATUS** field displays **RESETTING ...**

The Total Access 850 will restart immediately and resume operation. After giving the unit sufficient time to reboot, the user may Telnet back into the unit and log in.
DLP-8  Updating the Firmware using XMODEM

Introduction
The Total Access 850 supports firmware updates using TFTP or XMODEM. (Use the 10/100BASET Ethernet port and TFTP from a network server, or use XMODEM and the rear CRAFT or RCU faceplate CRAFT interface.) This procedure outlines the steps for a successful firmware upgrade using the rear CRAFT or RCU faceplate CRAFT interface and XMODEM software. (See DLP-7, Updating the Firmware using TFTP, for instructions on using TFTP.)

Tools and Materials Required
• VT100 compatible terminal or computer with terminal emulation software
• XMODEM software

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

CAUTION  Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Updating Firmware via the Console Menus

Perform the steps below in the order listed.

1. Connect to the Total Access 850 using the RCU faceplate CRAFT (DB-9) or rear CRAFT (RJ-45) interface. Selecting a higher baud rate connection makes the file transfer process faster. Verify that the baud rate setting on the Total Access 850 matches the VT100 emulation software COM port settings.
   
   If you are not already connected to the shelf’s RCU faceplate CRAFT or rear CRAFT interface (either with a VT100 compatible terminal or with a PC running VT100 emulation software), follow the procedure in DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port. Connecting to the RCU faceplate CRAFT or rear CRAFT interface limits the upgrade procedure to XMODEM only.

2. Log in to the unit.

3. Go to the SYSTEM UTILITY menu and select the UPGRADE FIRMWARE menu; press <Enter>.

4. Go to the TRANSFER METHOD menu and select XMODEM.

5. Select START TRANSFER to start the update process. Enter Y to confirm the upgrade.

6. From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. If necessary, refer to the terminal emulation software documentation for help.
   
   Also, when specifying the filename, ensure that the file transferred is the one provided by ADTRAN, otherwise, the update will not complete successfully. This may take several minutes.
   
   Because XMODEM data is being transferred in-band through the menu interface, the VT100 menus of the Total Access 850 will be inoperable from the RCU faceplate CRAFT or rear CRAFT interface. You can cancel the update at any time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)

7. When the update process has successfully completed, the following messages will display:
   
   Verifying downloaded FLASH image...
   
   Erasing FLASH...
   
   Programming FLASH...
   
   FLASH programmed successfully.

   The Total Access 850 will restart immediately and the user may then log back into the system.

   Alternately, if the unit is part of a management cluster connected to the local network, you may use a PC connected to the network to Telnet into the unit. By utilizing the ETHERNET port, the Total Access 850 may be quickly upgraded using TFTP, provided there is a TFTP server on the local network. The Total Access 850 ships with ADTRAN Utilities software, which includes a TFTP server. See DLP-7, Updating the Firmware using TFTP, for more details.
DLP-9  Saving the Current Configuration Using TFTP

Introduction

The Total Access 850 supports configuration transfers from the unit (via the 10/100BASET Ethernet port) to a TFTP server located on the network. This DLP provides the steps to follow for a successful configuration transfer using the 10/100BASET Ethernet port and a TFTP Server.

Tools and Materials Required

• A PC with a Telnet client software
• A TFTP Server accessible on the local network (A TFTP server is provided with the unit as part of the ADTRAN Utilities software.)

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

CAUTION  Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Connect to the Total Access 850 using the 10/100BASET interface.
   If you are not already connected to the unit’s 10/100BASET port using Telnet client software, use the procedure in DLP-5, Connecting to the Total Access 850 Using Telnet, to connect to the unit.
2. Log in to the unit using the read-write password (see DLP-2, Logging in to the System, for details).
3. Verify the TFTP server is running on the network.

   **NOTE**
   A TFTP server ships as part of the ADTRAN Utilities. If using ADTRAN Utilities, choose **START > PROGRAMS > ADTRAN UTILITIES > TFTP SERVER** to start the server.

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

   **CAUTION**
   If you are using the ADTRAN TFTP server, the IP address displays in the **STATUS** field. For other TFTP servers, please refer to the appropriate documentation.

7. Change **TFTP SERVER FILENAME** to a unique filename (for example, ta850.cfg). This will be the name of the configuration file saved to the remote server.
   Some TFTP servers constrain the format of the filename depending on the operating system of the server. For example, a TFTP server running on a PC under Windows 3.1 may only permit 8.3 format filenames (8 characters, period and three extension characters).
8. Select the **SAVE CONFIG REMOTELY** menu field and press **<Enter>**. Respond with **Y** to confirm the request.
9. View **CURRENT TRANSFER STATUS** to verify the progress of the current transfer. During a successful transfer, you will first see **DOWNLOAD: COPYING INTERNAL CONFIG**, and then **DOWNLOAD IN PROGRESS**.
10. When the transfer process has successfully completed, **IDLE** displays in the **CURRENT TRANSFER STATUS** field and **DOWNLOAD COMPLETE** displays in the **PREVIOUS TRANSFER STATUS** field.

   **WARNING**
   TFTP is not secure. No passwords are required for client access. Anyone can access files through the IP port on the server machine if they know the target filename.
DLP-10 Loading a Configuration Using TFTP

Introduction

The Total Access 850 supports configuration uploads from a unit (via the 10/100BASET Ethernet port) to a TFTP server located on the network. This DLP provides the steps to follow for a successful configuration upload using the 10/100BASET Ethernet port and a TFTP Server.

Tools and Materials Required

- A PC with a Telnet client software
- A TFTP Server accessible on the local network (A TFTP server is provided with the unit as part of the ADTRAN Utilities software.)

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

CAUTION Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Connect to the Total Access 850 using the \texttt{10/100BASET} interface.
   
   If you are not already connected to the unit's \texttt{10/100BASET} port using Telnet client software, use the procedure in DLP-5, \textit{Connecting to the Total Access 850 Using Telnet}, to connect to the unit.

2. Log in to the unit using the read-write password (see DLP-2, \textit{Logging in to the System}, for details).

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

   \begin{note}
   A TFTP server ships as part of the ADTRAN utilities. If using ADTRAN utilities, choose \texttt{START} \textgreater \texttt{PROGRAMS} \textgreater \texttt{ADTRAN UTILITIES} \textgreater \texttt{TFTP SERVER} to start the server.
   \end{note}

4. Go to the \texttt{SYSTEM UTILITY} menu and select the \texttt{CONFIGURATION TRANSFER} menu; press \texttt{<Enter>}.

5. Verify the \texttt{TRANSFER METHOD} is set to \texttt{TFTP}.

   \begin{warning}
   TFTP is \textbf{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.
   \end{warning}

6. Set the \texttt{TFTP SERVER IP ADDRESS} to the IP address of the machine running the TFTP Server Program.

   \begin{caution}
   \textit{If you are using the ADTRAN TFTP server, the IP address displays in the \texttt{STATUS} field. For other TFTP servers, please refer to the appropriate documentation.}
   \end{caution}

7. Change \texttt{TFTP SERVER FILENAME} to a unique filename. (This will be the name of the configuration file retrieved from the remote server.) If the ADTRAN Utilities TFTP server is used and no path is specified, the configuration file is retrieved from the default \texttt{ADTNUTIL} directory. To retrieve a configuration file from a particular folder, enter the entire filename including path.

   Some TFTP servers constrain the format of the filename depending on the operating system of the server. For example, a TFTP server running on a PC under Windows 3.1 may only permit 8.3 format filenames (8 characters, period and three extension characters).

8. Select the \texttt{LOAD AND USE CONFIG} menu field and press \texttt{<Enter>}. Respond with \texttt{Y} to confirm the request.

   \begin{warning}
   The Total Access 850 system is rebooted immediately after a configuration is successfully loaded. No additional confirmation is requested, and any online sessions will be terminated.
   \end{warning}

9. View \texttt{CURRENT TRANSFER STATUS} to verify the progress of the current upload.
10. When the upload process has successfully completed, **IDLE** displays in the **CURRENT TRANSFER STATUS** field and **DOWNLOAD COMPLETE** displays in the **PREVIOUS TRANSFER STATUS** field.

11. After an appropriate length of time, the user may Telnet back into the unit.
DLP-11 Saving and Transferring a Current Configuration Using XMODEM

Introduction
The Total Access 850 supports configuration transfers from the unit via the rear CRAFT or RCU faceplate CRAFT interfaces using a VT100 terminal or terminal emulator (with XMODEM). This DLP provides the steps for a successful configuration transfer using either the rear CRAFT or RCU faceplate 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.

**CAUTION**
Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the following steps in the order listed.

1. Connect to the Total Access 850 using the rear CRAFT (RJ-45) port on the back of the Total Access 850 or the RCU faceplate CRAFT (DB-9) interface.

If you are not already connected to the unit’s rear CRAFT or RCU faceplate CRAFT interface, either with a VT100 compatible terminal or with a PC running VT100 emulation software, follow the procedure in DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port. Connecting to the rear CRAFT or RCU faceplate CRAFT interface limits the configuration transfer procedure to XMODEM only.

2. Log in to the unit.

3. Go to the SYSTEM UTILITY menu and select CONFIGURATION TRANSFER menu; press <Enter>.

4. Set the TRANSFER METHOD menu to XMODEM.

5. Select SAVE CONFIG REMOTELY to start the transfers. Enter Y to confirm the transfer and prepare the Total Access 850 for the transfer download.

The following message is displayed: This will begin sending a copy of the current system configuration.

6. Configure the VT100 terminal or terminal emulation software to RECEIVE (and prompt for a filename).

7. View the CURRENT TRANSFER STATUS to verify the progress of the current transfer.

8. From the terminal emulation software, begin the XMODEM transfer by using the appropriate command sequence. For Windows HyperTerminal, select TRANSFER>RECEIVE FILE. Enter the filename (including path) and select XMODEM as the transfer method.

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

   **NOTE**

   When specifying the filename, ensure that the saved file has a .cfg extension; otherwise, the file may not be available for uploading into other Total Access 850 units.

   Because XMODEM data is being transferred inband through the menu interface, the VT100 menus of the Total Access 850 will be inoperable from the rear CRAFT or RCU faceplate CRAFT interfaces. You can cancel the update at any time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)

9. When the transfer has successfully completed, IDLE displays in the CURRENT TRANSFER STATUS field and XMODEM DOWNLOAD COMPLETE displays in the PREVIOUS TRANSFER STATUS field.
DLP-12 Loading a Configuration Using XMODEM

Introduction
The Total Access 850 supports configuration uploads from a unit via the rear CRAFT or RCU faceplate CRAFT interface using a VT100 terminal or terminal emulator (with XMODEM). This DLP provides the steps for a successful configuration upload using either the rear CRAFT or RCU faceplate CRAFT port and XMODEM protocol.

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.

**CAUTION** Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the following steps in the order listed.

1. Connect to the Total Access 850 using the rear CRAFT (RJ-45) or the RCU faceplate CRAFT (DB-9) interface located on the front of the RCU. If you are not already connected to the unit’s rear CRAFT or RCU faceplate CRAFT interface, either with a VT100 compatible terminal or with a PC running VT100 emulation software, follow the procedure in DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port. Connecting to the rear CRAFT or RCU faceplate CRAFT interface limits the configuration transfer procedure to XMODEM only.

2. Log in to the unit using the read-write password (see DLP-2, Logging in to the System, for details).

3. Go to the System Utility menu and select Configuration Transfer menu; press <Enter>

4. Set the Transfer Method menu to XMODEM.

5. Select Load and Use Config to start the transfer. Enter Y to confirm the transfer and prepare the Total Access 850 for the transfer download.

The Total Access 850 system is rebooted immediately after a configuration is successfully loaded. No additional confirmation is requested, and any online sessions will be terminated.

When the Total Access 850 is ready to receive the XMODEM configuration file, the menu screen clears and displays **Awaiting XMODEM Upload....<CTRL+X> Twice to Cancel**. If this does not appear, please review the preceding steps above for possible configuration errors.

6. From the terminal emulation software, begin the XMODEM transfer by using the appropriate command sequence. For Windows HyperTerminal, select Transfer>Send File. Enter the filename (including path) and select XMODEM as the transfer method. Total Access 850 configuration files should have a .cfg extension. If necessary, refer to the terminal emulation software documentation for help.

Because XMODEM data is being transferred inband through the menu interface, the VT100 menus of the Total Access 850 will be inoperable during this procedure from the rear CRAFT or RCU faceplate CRAFT interfaces. You can cancel the update at any time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)

7. View Current Transfer Status to verify the progress of the current upload.

8. When the transfer is complete, the Total Access 850 reboots and the Login screen appears. The unit is now operational.
DLP-13 Saving and Loading Text Configuration using Terminal Command Line

Introduction

The Total Access 850 RCU has the ability to download a text file which contains the configuration of the entire unit. This configuration may then be altered in a text editor and uploaded to any Total Access 850 RCU.

This DLP will explain how to save and load the text configuration file for the ADTRAN Total Access 850.

Prerequisite Procedures

You must connect to the Total Access 850 with a VT100 terminal session (reference DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port).

WARNING

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

CAUTION

Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

**Saving the router’s configuration**

1. Establish a connection to the router with the VT100 terminal software either through the rear **CRAFT** or RCU faceplate **CRAFT** port.
2. From the main menu, select **SYSTEM UTILITY**, then **TERMINAL MODE**; press `<Enter>`.
3. The following screen appears.

4. At the terminal prompt, type **DOWNLOAD**; press `<Enter>`. The following screen appears.

   ![Screen capture of terminal session](image)

   *Perform the steps below in the order listed.

   Do not enter further key commands until completing Step 5.*
5. Enable "capture" or "logging" in the terminal software, saving it to a file on your computer.
6. Press the **SPACE BAR** to continue. The 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 designated file.)
7. When the configuration stops printing, end the capture. The router's configuration is now saved to the designated file.
8. At the terminal prompt, type **EXIT** to enter the configuration menu of the router.

---

### Loading a configuration into the router

The following steps explain the process for uploading the text file back into the Total Access 850 RCU. These text files can be the entire configuration, or just partial commands that affect specific configuration changes. The uploading steps are the same, regardless of the size of the file.

1. Establish a connection to the router with the VT100 terminal software either through the rear CRAFT or RCU faceplate CRAFT port.
2. From the main menu, select **SYSTEM UTILITY**, then **TERMINAL MODE**; press **<Enter>**.
3. In the terminal software, initiate a SEND TEXT FILE or SEND CFG FILE using the saved configuration file.
4. Once the file transfer is complete, type **SAVE** to save the configuration in the unit. Type **EXIT** to enter the configuration menu of the router.

---

### Entering commands at the command prompt

Precede each instruction with a ">" when manually entering commands at the command prompt. After entering commands, type **SAVE** at the command prompt. (This applies **ALL** commands to current operation and saves all changes.) To save the changes to flash only (without affecting current operation), return to the menu system and press **<CTRL+W>**.

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

```plaintext
>sysconfig t1_timing_mode network (sets timing to recover from the network) or
>sysconfig t1_timing_mode internal (sets timing to internal Total Access 850 oscillator) or
>sysconfig t1_timing_mode dsx-1 (sets timing to recover from the DSX-1 interface).
```
DLP-14 A.03 to A.04 Firmware Upgrade

Introduction

The Total Access line of Integrated Access Devices includes both the ATM and TDM versions of the Total Access 850. Until now, the Total Access TDM units have been running firmware version A.03.xx. Recently, A.04.xx has been released to support the TDM Total Access IADs. The development of A.04.xx code is a significant step in the evolution of the Total Access product line, as it allows all Total Access family members to share the same base code. This means that features and fixes are more easily implemented and are propagated across the product line.

The two possible A.03 to A.04 upgrade paths are described in this DLP.

The choice of upgrade path will determine whether the unit's configuration is saved.

Since the A.03 and A.04 firmware loads are significantly different, the text configuration files for the two revisions are also different. It is recommended that the customer save a text configuration file for both the A.03 revision (prior to the upgrade) and for the A.04 revision (after completion of the upgrade). Refer to DLP-9, Saving the Current Configuration Using TFTP, DLP-11, Saving and Transferring a Current Configuration Using XMODEM, or DLP-13, Saving and Loading Text Configuration using Terminal Command Line, for further instructions on how to save the configuration.

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.03.90 (Transition Build) firmware from the ADTRAN website (http://www.ADTRAN.com).

For the Total Access 850 units, select SERVICE/SUPPORT > TECHNICAL SUPPORT > TOTAL ACCESS PRODUCTS > TOTAL ACCESS 850.

If further assistance is required, contact ADTRAN Technical Support at 1-888-4ADTRAN.
Tools and Materials Required

- VT100 compatible terminal or computer with terminal emulation software
- Appropriate cable to connect terminal to the unit (customer-provided)
- DB-9 male to DB-9 female cable (customer provided) for connecting to the CRAFT port on the front of the RCU
- DB-9 female to RJ-45 female adapter (customer provided) for connecting to the CRAFT port on the rear of the unit

Perform the steps below in the order listed.

Upgrade From A.03 to A.03.90 (Transition Build) to A.04

1. Upgrade the firmware from A.03 to A.03.90 (Transition Build) firmware. See DLP-7 (TFTP) or DLP-8 (XMODEM) for instructions on how to perform this upgrade.

2. Once the upgrade to A.03.90 is complete, immediately upgrade the unit to A.04. See DLP-7 (TFTP) or DLP-8 (XMODEM) for instructions on how to perform this upgrade.

   Upgrading from A.03 to A.03.90 (Transition Build) to A.04 will save the unit's configuration.

Upgrade From A.03 to A.04 Directly

1. Upgrade the firmware from A.03 to A.04 firmware. See DLP-7 (TFTP) or DLP-8 (XMODEM) for instructions on how to perform this upgrade.

2. The unit must then be factory defaulted by one of the following methods:
   - Select SYSTEM UTILITY>TERMINAL MODE. At the > prompt, type fac. You will then see "Restore Factory Defaults and Reset Unit? (press 'y')." Press the y key to confirm default. The unit will then automatically reset.

3. If connected to the RCU faceplate CRAFT or rear CRAFT port, set DIP-switch 2 (on the RCU) to the on position and power reset the unit. You will then be prompted to confirm the factory default.

   DIP-switch services are not available on 3rd Generation RCUs.

   To avoid a configuration loss in the event of a power failure, return DIP-switch 2 to the off position before resuming normal operation.
4. Reconfigure the unit for the specific application.

**NOTE**

Upgrading from A.03 to A.04 directly (or from A.04 to A.03 directly) will erase the unit's configuration.
DLP-15 Using the ADTRAN Utility Syslog

Introduction
The Total Access 850 Syslog Utility records various message types at settable threshold levels to an external Syslog server (software supplied with the Total Access 850 system ADTRAN Utilities).

Prerequisite Procedures
This procedure assumes that the Total Access 850 unit is connected to an IP network and is powered up.

Tools and Materials Required
- Syslog server (provided on Total Access 850 System CD in ADTRAN Utilities)

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

**CAUTION**
Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Setting up the Total Access 850 to use Syslog:

1. Log in to the system with maximum rights (see DLP-2, Logging in to the System). Once you have logged into the Total Access 850, go to System Config/Syslog. Set the options as follows:
   - **Syslog IP**: Enter the IP address of the PC where the Syslog host resides
   - **Syslog Format**: Specify the Syslog format as either **ADTRAN** (to work with ADTRAN Utilities) or **UNIX** (to work with a standard UNIX Syslog server)
   - **Syslog Facility**: Specify the facility destination of log events; Options are **Local0** to **Local7**

Setting Up the Syslog Host:

1. On your PC, go to **Start/Programs/ADTRAN Utilities/Syslog**. When the Syslog window opens, you will see **Local0** through **Local7** listed on the left. This should correspond with the **Host Facility** specified in the Total Access 850. The Syslog program must be open on your PC in order for it to record Total Access 850 information. The Syslog files can be viewed through the Syslog window, and they are also available under the ADTRAN Utilities Folder named **LocalX.txt**, where **X** can equal 0 through 7. You can also view the **LocalX.txt** file by clicking on **Edit Log**.

![Syslog Window Screenshot](image)
The **MONITOR** feature allows all Syslog messages to be prefiltered by **SYSTEM NAME**, **SOURCE**, **SLOT**, and **PORT** before displaying these messages to the user and logging the message to the pre-designated monitor log file. Various filter options may be defined by selecting **SOURCE**. The figure below shows the **SOURCE FILTER** window. When the **MONITOR** button is selected, the file will be logged to **LOCAL8.TXT**. To look at the text file, click on the **EDIT LOG** button on the left side of the Syslog screen. Only the **SOURCE** options that are selected with an ‘x’ will be displayed in the Syslog file. In this example, all options are displayed.
• Under the **LOG FILES** menu option, the user may erase log files, define Red events, set priorities, and clear Red events. The **ERASE LOG FILES** option erases the specified text log file.

• **DEFINE RED EVENTS** allows the user to predefine a message priority condition so that if the condition occurs, the file is highlighted in red. In the figure below, any **CRITICAL** or **MAJOR** condition causes any **LOCAL0** through **LOCAL7** facility to become highlighted in red if it receives a critical or major alarm.

• The **PROPERTIES** menu allows the user to specify the types of messages to be logged to an ASCII text file. Mark the lowest priority Syslog message you want to log to the Syslog server text file. For example, the figure below shows that all messages will be logged to the text file.

• The **HELP** menu also explains these features. Click on **HELP/CONTENTS/SYSLOG HOST DAEMON** for further explanation of Syslog features.
DLP-16 Connecting the Alarm Contacts and the External Input

Introduction

Alarm connections alert the user when a selected alarm condition exists. Pressing the Alarm Cut-Off (ACO) switch on the front panel of the Total Access 850 PSU clears the alarm. This procedure details the steps which must be performed to use the Total Access 850 alarm connections and the ACO switch.

This procedure should be performed at installation on each Total Access 850 shelf that is wired out to external office alarm equipment.

Prerequisite Procedures

Before beginning this procedure, the Total Access 850 should be mounted in its permanent location.

Tools and Materials Required

- Wire strippers
- Small Phillips screwdriver
- 22 or 24 AWG 2-conductor twisted pair cross-connect wire
- VT100 terminal or PC with VT100 terminal emulation software

WARNING

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

Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
1. Backplane alarm connections (P5) are labeled as shown in the table below and illustrated in the figure.

<table>
<thead>
<tr>
<th>P3 Wire-Wrap Connections</th>
<th>T1 Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>R1</td>
</tr>
<tr>
<td>2</td>
<td>T1</td>
</tr>
<tr>
<td>3</td>
<td>R</td>
</tr>
<tr>
<td>4</td>
<td>T</td>
</tr>
<tr>
<td>5</td>
<td>Gnd</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P5 Wire-Wrap Connections</th>
<th>Alarm Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-48 ALM</td>
</tr>
<tr>
<td>2</td>
<td>MJVR</td>
</tr>
<tr>
<td>3</td>
<td>MJV</td>
</tr>
<tr>
<td>4</td>
<td>MJR</td>
</tr>
<tr>
<td>5</td>
<td>MJ</td>
</tr>
</tbody>
</table>

To customer designed remote alarms

You will have to remove the cover to access the contacts. Refer to the Total Access 850 rear view illustration on the next page.
2. Alarm relay contacts are open during normal operation. The alarm relay contacts close in the event of a local alarm condition or the receipt of an alarm from the T1 Carrier.

3. In a carrier alarm condition such as a Red, Yellow, or Blue (unframed all 1s), various alarm contacts in the PSU close.

4. Carrier alarm conditions cause the Total Access 850 to initiate trunk processing. The following chain of events then occur:
   • MJ will be directly shorted to MJR.
   • MJV will be directly shorted to MJVR.

5. Contacts MJ and MJR can be overridden manually during an alarm condition by pressing the ACO pushbutton on the PSU faceplate.

6. If the 3-Amp power fuse on the PSU trips, the -48 ALM relay will close, providing a -48 VDC signal on that pin. This alarm cannot be overridden by the ACO pushbutton. Refer to the table below for alarm notifications.

<table>
<thead>
<tr>
<th>Alarm Condition</th>
<th>Relays Activated</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED ALARM</td>
<td>MJR</td>
</tr>
<tr>
<td>YELLOW ALARM</td>
<td>X</td>
</tr>
<tr>
<td>AIS ALARM</td>
<td>X</td>
</tr>
<tr>
<td>PSU POWER FUSE FAILS</td>
<td>X</td>
</tr>
<tr>
<td>ALARMS ACO DEACTIVATES</td>
<td>X</td>
</tr>
</tbody>
</table>

Note: ACO will not deactivate MJR after a power fuse failure.
DLP-17 Configuring the Total Access 850 for Dual T1 Maps

Introduction

The Total Access 850 with firmware A.04.02 or higher has a Dual T1 Map feature that allows two network T1 connections for the termination of data and voice applications. The primary network T1 Map can be configured for internal router usage (FT1/24 DS0s maximum) and to any access module installed. The DSX Map can be used for FXS/FXO modules in slots 1-6 only. There are several steps that must be followed in order for the Dual T1 Map to be configured successfully. These steps are described in this DLP.

Prerequisite Procedures

This procedure assumes that the user has access to the Total Access 850 system menus.

Refer to DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port, for details on making a terminal connection to the Total Access 850.

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

Electronic modules can be damaged by static electrical discharge. Before handling modules, put on an antistatic discharge wrist strap to prevent damage to electronic 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.
Perform the steps below in the order listed.

1. Connect the Total Access 850 unit to your VT100 system (details found in DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port).
2. Log in to the system with maximum rights (details are in DLP-2, Logging in to the System).
3. From the DS0 MAPS menu, select the ACTIVE MAP option and press <Enter>.
4. From the DS0 MAPS > ACTIVE MAPS menu, select the DUAL T1 MAP option; press <Enter>. Select “Y” for yes to confirm the Active Map change and press <Enter>. The following screen appears.

The second T1 connected to the DSX port may only be used for voice connections (FXS/FXO). The second T1 must be connected to the integrated DSX port, not the DSX-1 Card.

Figure 1. Dual T1 Map
5. Edit the Primary T1 Map by pressing `<Enter>` on **Edit/View T1 Map** [+]. The following screen appears.

![Primary T1 Map Screen](image)

**Figure 2. Primary T1 Map**

*The T1 Map can be mapped to the internal router or other available access module.*
6. Edit the Secondary T1 Map (DSX Map) by pressing <Enter> on **Edit/View DSX Map** [+] . The following screen appears.

![DSX Map](image)

**Figure 3. DSX Map**

*The DSX Map can be mapped to the FXS and FXO access modules only.*

7. Left arrow back to **DS0 Maps** and log off by pressing <CTRL+L>.
ADTRAN UTILITIES

This section provides instructions for configuring and using the ADTRAN Utilities software programs including Telnet, VT100, Syslog, and TFTP.

ADTRAN delivers several PC software utilities with the Total Access 850. These utilities are located on the CD-ROM that came with your shipment. The utilities make it easier to interface with the terminal menu and transfer configuration files to and from TFTP servers. The utilities all run on Microsoft Windows 3.1 or higher. The following sections describe the Syslog, Telnet, VT100, and TFTP Server utilities.

Review the readme file (Readme.txt) on the CD-ROM for the latest information about the utilities.

CONTENTS

Telnet Utility ................................................................. 250
  Session Menu ............................................................... 251
  Edit Menu ................................................................. 252
  Options Menu .............................................................. 252
  Capture Menu .............................................................. 252
  Help Menu ................................................................. 253

VT100 Utility ................................................................. 253
  Session Menu ............................................................... 254
  Edit Menu ................................................................. 254
  Port Menu ................................................................. 254
  Options Menu .............................................................. 254
  Capture Menu .............................................................. 255
  Help Menu ................................................................. 255

TFTP Server ................................................................. 255
  Server Menu ............................................................... 256
  Print Log ................................................................. 256
  Help ................................................................. 257

Status Field ................................................................. 257

Meter Field ................................................................. 257

Log Field ................................................................. 257

FIGURES

Figure 1. Telnet Menu Tree .................................................. 250
Figure 2. VT100 Menu Tree ................................................... 253
Figure 3. TFTP Server Interface Menu Tree ................................. 255
Figure 4. TFTP Server Interface ............................................. 256
1. **TELNET UTILITY**

Access the Telnet program remotely through the Ethernet port. For a detailed description of how to work within the terminal menu, refer to *Navigating the Terminal Menu* on page 67 (in the User Interface Guide section of this manual). The Telnet menus include **SESSION, EDIT, OPTIONS, CAPTURE, and HELP** (see the menu tree in Figure 1).

---

**Figure 1. Telnet Menu Tree**

<table>
<thead>
<tr>
<th>Session</th>
<th>Host Name</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconnect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transfer Cfg</td>
<td></td>
<td>Add New</td>
</tr>
<tr>
<td>Exit</td>
<td></td>
<td>Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connect</td>
</tr>
<tr>
<td>Edit</td>
<td>Copy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paste</td>
<td></td>
</tr>
<tr>
<td>Telnet Options</td>
<td></td>
<td>Background</td>
</tr>
<tr>
<td></td>
<td>Colors</td>
<td>Bold</td>
</tr>
<tr>
<td></td>
<td>Local Echo</td>
<td>Text</td>
</tr>
<tr>
<td></td>
<td>Auto Repeat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>File</td>
<td>Start Cfg Capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stop Cfg Capture</td>
</tr>
<tr>
<td>Capture</td>
<td>Buffer Size</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Save Buffer As</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Screen Capture</td>
</tr>
<tr>
<td>Help</td>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>About</td>
<td></td>
</tr>
</tbody>
</table>
Session Menu
Click on SESSION to open the Telnet session.

Connect
Opens dialog box for setting HOST NAME and PORT parameters for a Telnet session. Also lets you EDIT ENTRY, ADD NEW entry, and DELETE stored entries. When the parameters are set, click CONNECT to make the connection. Click CANCEL to end the session.

Host Name
Accepts and stores host names. You may enter either a name, an IP address, or a domain name directly from this field. Click on the drop-down arrow to display a complete list of previously stored host names.

Port
Provides several port options. You may enter port numbers directly into this field to connect to non-standard ports or select the drop-down combo-box to display the following options:

TELNET establishes a Telnet session
ECHO provides a loopback for troubleshooting
DISCARD bit bucket; discards data
DAYTIME returns the time
CHARGEN displays as a unique character stream; used for self-tests

Edit Entry
Changes either the unit name or the IP address of each host. Press either Tab, Return, or a period (.) after each number in the IP address to move to the next field. If you press Return or enter a period while the cursor is located in an IP field, that field entry is deleted.

Add New
Prompts you for the same information as the EDIT ENTRY dialog box for new host. When enabled, the USE DNS (Domain Name Server) feature allows users to request DOMAIN LOOK UP via a DNS server on the network, rather than specifying an IP address. The name then appears in the HOST NAME field.

Delete
Removes a host name from the list; select the host name you want to remove, and, at the prompt, click DELETE.

Connect
Establishes the Telnet session.
Disconnect
Terminates the Telnet session.

To re-establish the session, select CONNECT from SESSION MENU or press ENTER three times. This action restores the previous connection.

Transfer Cfg
This feature is used with ADTRAN products to send configuration files to the unit.

Exit
Ends the Telnet session and closes the Telnet screen.

Edit Menu
Provides COPY and PASTE commands.

Options Menu
Provides viewing alternatives for the terminal screen.

Colors
Three options change the color of the background window (BACKGROUND), bold highlights (BOLD), and text (TEXT).

Local Echo
Echoes each character that you enter.

AutoRepeat
Repeats characters you select from the keyboard, if you hold down the key.

Capture Menu
Provides options for capturing screen images.

File
Sends screen options data to a file in the format options listed below:

Start Cfg Capture
Used with the ADTRAN product line to start sending the scrolling screen capture to a file storage location.

Stop Cfg Capture
Used with the ADTRAN product line to stop sending the scrolling screen capture to a file storage location.

Buffer Size
Disables terminal window scroll bars when set to zero. (This is the normal setting for Total Access 850.) This number represents the number of lines to capture in the memory buffer.

Save Buffer As
Save screen capture to a file.

Screen Capture
Copies the text on the current Telnet screen to the clipboard. You can open any word processor and paste the clipboard contents into the program. This option is helpful when debugging.
Help Menu
Provides online help for using the ADTRAN Utilities.

Contents
Opens the online help.

IP Status
Displays the local port address and the status of the connection.

About
Displays version and owner information.

2. VT100 UTILITY
Use the VT100 to configure an Total Access 850 which is directly connected to a PC. The VT100 display is almost identical to the Telnet display. For a detailed description of how to work within the terminal menu, refer to Navigating the Terminal Menu on page 67 (in the User Interface Guide section of this manual). If you need help setting up the Total Access 850 for a VT100 session, refer to DLP-1, Connecting a VT100 Terminal or PC to the CRAFT Port. VT100 menus include SESSION, EDIT, PORT, OPTIONS, CAPTURE, and HELP (see the menu tree in Figure 2).

<table>
<thead>
<tr>
<th>Session</th>
<th>Connect</th>
<th>Disconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File Transfer</td>
<td>XMODEM CRC</td>
</tr>
<tr>
<td></td>
<td>Exit</td>
<td>ASCII Cfg Files</td>
</tr>
<tr>
<td>Edit</td>
<td>Copy</td>
<td>Paste</td>
</tr>
<tr>
<td>Port</td>
<td>Settings</td>
<td></td>
</tr>
<tr>
<td>VT100 Options</td>
<td>Refresh Screen</td>
<td>Transmit Wakeup</td>
</tr>
<tr>
<td></td>
<td>Connect</td>
<td>Transmit Refresh</td>
</tr>
<tr>
<td></td>
<td>Colors</td>
<td>Local Echo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Auto Repeat</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>File</td>
<td>Start Cfg Capture</td>
</tr>
<tr>
<td></td>
<td>Buffer Size</td>
<td>Stop Cfg Capture</td>
</tr>
<tr>
<td></td>
<td>Save Buffer As Screen Capture</td>
<td></td>
</tr>
<tr>
<td>Help</td>
<td>Contents</td>
<td>About</td>
</tr>
</tbody>
</table>

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 an Total Access 850.

**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 272).

**Port Menu**
Changes serial COM port **SETTINGS**. Provides data rate settings from 300-57600 bps.

**Options Menu**
Provides terminal screen commands.

**Refresh Screen**
Redraws the screen.

**Connect**
Provides the options **TRANSMIT WAKEUP** and **TRANSMIT REFRESH**.

**Transmit Wakeup**
Provides a control sequence that puts the Total Access 850 Control Port online in terminal mode.

**Transmit Refresh**
Provides a control sequence to refresh the screen automatically when connecting. (This is the default setting for the Total Access 850.)

**Colors**
Identical to Telnet **COLORS MENU** (see Colors on page 272).

**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 272).

Help Menu
Provides online help and information about the version number.

Contents
Opens online help.

About
Displays version and owner information.

3. TFTP SERVER
The TFTP Server utility transfers Total Access 850 configuration files to and from a TFTP server (see Figure 3 for the menu tree). You can install this program on a PC running any version of Microsoft Windows. The configuration of an Total Access 850 can be saved offline as a backup file. The saved file may also be used to send the same configuration to multiple Total Access 850 units. Transfer configuration files using the TFTP protocol (a TCP/IP user protocol) via the Ethernet port. The Total Access 850 must have a valid IP address, subnet mask, and default gateway (if required), and be connected to an Ethernet network before proceeding. Figure 4 shows the TFTP server interface. For information on transferring and saving configurations using TFTP, refer to DLP-9, Saving the Current Configuration Using TFTP.

Files must be placed in the Application directory where you installed the product. Received files are also placed here.
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 an Total Access 850 unit’s transferred configuration to allow sending identical configurations to multiple units. When you start this program, a port is automatically opened.

**Server Menu**
Provides enable, disable, abort, and exit options.

**Enable**
Enables the TFTP server. The IP address displays in the Status field and **Server Ready** displays in the Log field.

**Disable**
Disables the TFTP server. When you select this option, the message **Port Closed** displays in the STATUS field and in the LOG field.

**Abort**
Terminates a transfer that is in progress.

**Exit**
Terminates active transfers and closes the TFTP window.

**Print Log**
Provides print options.

...to Clipboard
Copies the information in the LOG field to the clipboard. You can then open any word processor and paste the information into the program for review.

...to Printer
Sends the information in the LOG field to the default printer.

**Clear Log**
Deletes the information stored in the LOG field.
**Help**
Provides online help and version information.

**Contents**
Opens online help.

**About**
Displays version and owner information.

4. **STATUS FIELD**
This field displays general information about port and transfer status. This field is read-only. The unlabeled field in the center of the screen displays prompts about the status of active transfers, such as bytes transferred and received.

5. **METER FIELD**
The **XMIT** meter provides a visual record of the transfer progress.

6. **LOG FIELD**
This field displays a record of all of the events that occur during the time the TFTP Server is enabled. Use the scroll bar to move up and down the list. To clear the information in this field, select **CLEAR LOG** from the **PRINT LOG** menu. Save this information to a file before deleting it with the **TO CLIPBOARD** command.
MIBS

This section is divided into two parts: (1) SNMP information for TDM units and (2) SNMP information for ATM units. Each section details the Management Information Bases (MIBs) supported, MIB Compilation Order, Traps Supported, and MIB Variables supported.

CONTENTS

MIBs Supported by TDM Units ................................................................. 258
MIB Compilation Order For TDM Units ..................................................... 259
Traps Supported by TDM Units ............................................................... 259
MIB Variables Supported by TDM Units .................................................... 260
MIBs Supported by ATM Units ............................................................... 260
MIB Compilation order for ATM Units ..................................................... 261
Traps Supported by ATM Units ............................................................... 261
MIB Variables Supported by ATM Units .................................................... 261
For this section, TDM units refers to Total Access 850 units running A.04 firmware or later. ATM units refers to Total Access 850 units running C.02 firmware or previous.

The TDM units support SNMP Version 2. The ATM units support SNMP Version 1.

1. MIBS SUPPORTED BY TDM UNITS

**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
- adladSys.mi2  ADTRAN-ADIADSYS-MIB
- adladRtr.mi2  ADTRAN-ADIADROUTER-MIB
- adladVoi.mi2  ADTRAN-ADIADVOCIE-MIB

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

All TDM MIBs are SNMPv2.
2. **MIB COMPILATION ORDER FOR TDM UNITS**

IANAifType-MIB
PerfHist-TC-MIB
SNMPv2-MIB (if not included with SNMP manager)
IF-MIB
IP-MIB
IP-FORWARD-MIB
FRAME-RELAY-DTE-MIB
DS1-MIB
DS0-MIB
DS0BUNDLE-MIB
EtherLike-MIB
CIRCUIT-IF-MIB
ADTRAN-MIB
ADTRAN-IADSYS-MIB
ADTRAN-IADROUTER-MIB

3. **TRAPS SUPPORTED BY TDM UNITS**

| From RFC1215-MIB:         | coldStart                           |
|                          | linkDown                             |
|                          | linkUp                               |
|                          | authenticationFailure                |
| From ADTRAN-IADSYS-MIB:  | adladWanDown - 1003203               |
|                          | adladWanUp - 1003204                 |
|                          | adladBatteryAlarmAct - 1003207       |
|                          | adladBatteryAlarmDeact - 1003208     |
| (T1 WAN interface only): | adladDs1RedAlarmON - 1003209         |
|                          | adladDs1YellowAlarmON - 1003210      |
|                          | adladDs1BlueAlarmON - 1003211        |
|                          | adladDs1RedAlarmOFF - 1003212        |
|                          | adladDs1YellowAlarmOFF - 1003213     |
|                          | adladDs1RedAlarmON - 1003209         |
|                          | adladDs1YellowAlarmON - 1003210      |
|                          | adladDs1BlueAlarmON - 1003211        |
|                          | adladDs1RedAlarmOFF - 1003212        |
|                          | adladDs1YellowAlarmOFF - 1003213     |
|                          | adladDs1BlueAlarmOFF - 1003211       |
|                          | adladDs1SEF - 1003215                |
|                          | adladDs1FS - 1003216                 |
# Section 7 MIBs

## Total Access 850 System Manual

### 4. MIB VARIABLES SUPPORTED BY TDM UNITS

SNMPv2 states the supported MIB variables by the following method:

The unit will have a MIB called TA 6XX.mi2 that will describe the SNMP variables supported. This MIB will contain an Agent Capabilities module that will describe the SNMP variables supported.

### 5. MIBs Supported by ATM Units

| (T1 WAN interface only): | adladDs1CRC - 1003217  
adladDs1LCV - 1003218  
adladDs1SLP - 1003219 |
|-------------------------|------------------------|
| From ADTRAN-IADVOCED-MIB: | adladVoiceTestStatusActive - 1003401  
adladVoiceTestStatusClear - 1003402  
adladVoiceAlarmBitActive - 1003403  
adladVoiceAlarmBitInactive - 1003404  
adladVoiceGatewayDown - 1003405  
adladVoiceGatewayUp - 1003406  
adladVoiceLifeLineActivated - 1003407  
adladVoiceLifeLineDeactivated - 1003408 |

---

**Standard RFC MIBs:**
- RFC1213.mib  
- RFC1406.mib  
- RFC1695.mib

**RFC1213-MIB**

**DS1-MIB (T1 interface only):**
- RFC1213-MIB  
- RFC1406-MIB  
- RFC1695-MIB

**ATM-MIB**

**Enterprise MIBs:**
- Adtran.mib  
- adtartr_trap.mib

**ADTRAN-MIB**

**ADTRAN-ADTARTR_TRAP-MIB**

---

**NOTE**

*RFC1155-SMI, RFC1212-MIB, and RFC1215-MIB are also needed and should come standard with any SNMP Management software.*

---

**NOTE**

*All ATM MIBs are SNMPv1.*
6. **MIB COMPILATION ORDER FOR ATM UNITS**

   RFC1213-MIB
   RFC1406-MIB
   RFC1695-MIB
   ADTRAN-MIB
   ADTRAN-ADTARTR-TRAP-MIB

7. **TRAPS SUPPORTED BY ATM UNITS**

<table>
<thead>
<tr>
<th>From ADTARTR_TRAP MIB:</th>
</tr>
</thead>
<tbody>
<tr>
<td>coldStart</td>
</tr>
<tr>
<td>linkUp</td>
</tr>
<tr>
<td>linkDown</td>
</tr>
<tr>
<td>authenticationFailure</td>
</tr>
<tr>
<td>adTARouterWanDown - 6645503</td>
</tr>
<tr>
<td>adTARouterWanUp - 6645504</td>
</tr>
<tr>
<td>adTARouterBatteryAlarmAct - 6645507</td>
</tr>
<tr>
<td>adTARouterBatteryAlarmDeact - 6645508</td>
</tr>
<tr>
<td>adTARouterVoiceGatewayDown - 6645509</td>
</tr>
<tr>
<td>adTARouterVoiceGatewayUp - 6645510</td>
</tr>
<tr>
<td>adTARouterLifeLineActivated - 6645511</td>
</tr>
<tr>
<td>adTARouterLifeLineDeactivated - 6645512</td>
</tr>
</tbody>
</table>

8. **MIB VARIABLES SUPPORTED BY ATM UNITS**

   *ATM units do not support write access for SNMP (except for sysName, sysLocation, and sysContact).*

   **system:**
   - sysDescr: RO
   - sysObjectID: RO
   - sysUpTime: RO
   - sysContact: RW
   - sysName: RW
   - sysLocation: RW
   - sysServices: RO

   **interfaces:**
   - ifIndex: RO
   - ifDescr: RO
   - ifType: RO
ifMtu RO
ifSpeed RO
ifPhysAddress RO
ifOperStatus RO
ifInOctets RO
ifInUcastPkts RO
ifInNUcastPkts RO
ifInDiscards RO
ifInErrors RO
ifInUnknownProtos RO
ifOutOctets RO
ifOutUcastPkts RO
ifOutNUcastPkts RO
ifOutDiscards RO
ifOutErrors RO
ifSpecific RO

ip:
ipForwarding RO
ipDefaultTTL RO
ipInReceives RO
ipInHdrErrors RO
ipInAddrErrors RO
ipForwDatagrams RO
ipInUnknownProtos RO
ipInDiscards RO
ipInDelivers RO
ipOutRequests RO
ipOutDiscards RO
ipOutNoRoutes RO
ipReasmOKs RO
ipReasmFails RO
ipFragOKs RO
ipFragFails RO
ipFragCreates RO

ipAddrTable:
### ipAddrEntry
- ipAdEntAddr: RO
- ipAdEntIfIndex: RO
- ipAdEntNetMask: RO
- ipAdEntBcastAddr: RO
- ipAdEntReasmMaxSize: RO

### ipRouteTable:
- ipRouteEntry
  - ipRouteDest: RO
  - ipRouteIfIndex: RO
  - ipRouteMetric1: RO
  - ipRouteMetric2: RO
  - ipRouteMetric3: RO
  - ipRouteMetric4: RO
  - ipRouteNextHop: RO
  - ipRouteType: RO
  - ipRouteProto: RO
  - ipRouteAge: RO
  - ipRouteMask: RO
  - ipRouteMetric5: RO
  - ipRouteMetricInfo: RO

### ipNetToMediaTable:
- ipNetToMediaEntry
  - ipNetToMediaIfIndex: RO
  - ipNetToMediaPhysAddress: RO
  - ipNetToMediaNetAddress: RO
  - ipNetToMediaType: RO
  - ipRoutingDiscards: RO

### icmp:
- icmpInMsgs: RO
- icmpInErrors: RO
- icmpInDestUnreachs: RO
- icmpInTimeExcds: RO
- icmpInParmProbs: RO
- icmpInSrcQuenchs: RO
- icmpInRedirects: RO
- icmpInEchos: RO
- icmpInEchoReps: RO
- icmpInTimestamps: RO
- icmpInTimestampReps: RO
<table>
<thead>
<tr>
<th>MIB Name</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmpInAddrMasks</td>
<td>RO</td>
</tr>
<tr>
<td>icmpInAddrMaskReps</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutMsgs</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutErrors</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutDestUnreachs</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutTimeExcds</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutParmProbs</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutSrcQuenchs</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutRedirects</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutEchos</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutEchoReps</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutTimestamps</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutTimestampReps</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutAddrMasks</td>
<td>RO</td>
</tr>
<tr>
<td>icmpOutAddrMaskReps</td>
<td>RO</td>
</tr>
</tbody>
</table>
### tcp:
- tcpRtoAlgorithm: RO
- tcpRtoMin: RO
- tcpRtoMax: RO
- tcpMaxConns: RO
- tcpActiveOpens: RO
- tcpPassiveOpens: RO
- tcpAttemptFails: RO
- tcpEstabResets: RO
- tcpCurrEstab: RO
- tcpInSegs: RO
- tcpOutSegs: RO
- tcpRetransSegs: RO

### tcpConnTable
- tcpConnEntry
  - tcpConnState: RO
  - tcpConnLocalAddress: RO
  - tcpConnLocalPort: RO
  - tcpConnRemAddress: RO
  - tcpConnRemPort: RO

### tcpInErrs: RO
### tcpOutRsts: RO

### udp:
- udpInDatagrams: RO
- udpNoPorts: RO
- udpInErrors: RO
- udpOutDatagrams: RO
- udpLocalAddress: RO
- udpLocalPort: RO

### udpTable
- udpEntry
  - udpEntryLocalAddress: RO
  - udpLocalPort: RO
**egp:**

- egpInMsgs  RO
- egpInErrs  RO
- egpOutMsgs RO
- egpOutErrors RO
- egpNeighState RO
- egpNeighAddr  RO
- egpNeighAs  RO
- egpNeighInMsgs RO
- egpNeighInErrs RO
- egpNeighOutMsgs RO
- egpNeighOutErrs RO
- egpNeighInErrMsgs RO
- egpNeighOutErrMsgs RO
- egpNeighStateUps RO
- egpNeighStateDowns RO
- egpNeighIntervalHello RO
- egpNeighIntervalPoll RO
- egpNeighMode  RO

**dsx1:**

- dsx1ConfigTable
  - dsx1ConfigEntry
    - dsx1LineIndex  RO
    - dsx1IfIndex  RO
    - dsx1TimeElapsed  RO
    - dsx1ValidIntervals RO
    - dsx1LineType  RO
    - dsx1LineCoding  RO
    - dsx1SendCode  RO
    - dsx1CircuitIdentifier  RO
    - dsx1LoopbackConfig  RO
    - dsx1LineStatus  RO
    - dsx1SignalMode  RO
    - dsx1TransmitClockSource  RO
    - dsx1Fdl  RO
### dsx1CurrentTable

<table>
<thead>
<tr>
<th>dsx1CurrentEntry</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>dsx1CurrentIndex</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentSESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentSEFs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentUASs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentCSSs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentPCVs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentLESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentBESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1CurrentLCVs</td>
<td>RO</td>
</tr>
</tbody>
</table>

### dsx1IntervalTable

<table>
<thead>
<tr>
<th>dsx1IntervalEntry</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>dsx1IntervalIndex</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalNumber</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalSESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalSEFs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalUASs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalCSSs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalPCVs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalLESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalBESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1IntervalLCVs</td>
<td>RO</td>
</tr>
</tbody>
</table>

### dsx1TotalTable

<table>
<thead>
<tr>
<th>dsx1TotalEntry</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>dsx1TotalIndex</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalSESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalSEFs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalUASs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalCSSs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalPCVs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalLESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalBESs</td>
<td>RO</td>
</tr>
<tr>
<td>dsx1TotalLCVs</td>
<td>RO</td>
</tr>
</tbody>
</table>
### dsx1FracTable

**dsx1FracEntry**
- **dsx1FracIndex** (RO)
- **dsx1FracNumber** (RO)
- **dsx1FractIfIndex** (RO)

### snmp:

- **snmpInPkts** (RO)
- **snmpOutPkts** (RO)
- **snmpInBadVersions** (RO)
- **snmpInBadCommunityNames** (RO)
- **snmpInBadCommunityUses** (RO)
- **snmpInASNParseErrs** (RO)
- **snmpInTooBigs** (RO)
- **snmpInNoSuchNames** (RO)
- **snmpInBadValues** (RO)
- **snmpInReadOnlys** (RO)
- **snmpInGenErrs** (RO)
- **snmpInTotalReqVars** (RO)
- **snmpInTotalSetVars** (RO)
- **snmpInGetRequests** (RO)
- **snmpInSetRequests** (RO)
- **snmpInGetRequests** (RO)
- **snmpInTraps** (RO)
- **snmpOutTooBigs** (RO)
- **snmpOutNoSuchNames** (RO)
- **snmpOutBadValues** (RO)
- **snmpOutGenErrs** (RO)
- **snmpOutGetRequests** (RO)
- **snmpOutGetNexts** (RO)
- **snmpOutSetRequests** (RO)
- **snmpOutGetRepsonses** (RO)
- **snmpOutTraps** (RO)
- **snmpEnableAuthenTraps** (RO)
### atm:

#### atmInterfaceTable
- atmInterfaceEntry
  - atmInterfaceMaxVpcs: RO
  - atmInterfaceMaxVccs: RO
  - atmInterfaceConfVpcs: RO
  - atmInterfaceConfVccs: RO
  - atmInterfaceMaxActiveVpiBits: RO
  - atmInterfaceMaxActiveVciBits: RO
  - atmInterfaceIlmiVpi: RO
  - atmInterfaceIlmiVci: RO
  - atmInterfaceAddressType: RO
  - atmInterfaceAdminAddress: RO
  - atmInterfaceMyNeighborIpAddress: RO
  - atmInterfaceMyNeighborIfName: RO

#### atmInterfaceTCTable
- atmInterfaceTCEntry
  - atmInterfaceOCDEvents: RO
  - atmInterfaceTCAlarmState: RO

#### atmTrafficDescrParamTable
- atmTrafficDescrParamEntry
  - atmTrafficDescrParamIndex: RO
  - atmTrafficDescrType: RO
  - atmTrafficDescrParam1: RO
  - atmTrafficDescrParam2: RO
  - atmTrafficDescrParam3: RO
  - atmTrafficDescrParam4: RO
  - atmTrafficDescrParam5: RO
  - atmTrafficDescrQosClass: RO
  - atmTrafficDescrRowStatus: RO

#### atmVclTable
- atmVclEntry
  - atmVclVpi: RO
  - atmVclVci: RO
  - atmVclAdminStatus: RO
  - atmVclOperStatus: RO
<table>
<thead>
<tr>
<th>MIB Name</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>atmVclLastChange</td>
<td>RO</td>
</tr>
<tr>
<td>atmVclReceiveTrafficDescrIndex</td>
<td>RO</td>
</tr>
<tr>
<td>atmVclTransmitTrafficDescrIndex</td>
<td>RO</td>
</tr>
<tr>
<td>atmVccAalType</td>
<td>RO</td>
</tr>
<tr>
<td>atmVccAal5CpcsTransmitSduSize</td>
<td>RO</td>
</tr>
<tr>
<td>atmVccAal5CpcsReceiveSduSize</td>
<td>RO</td>
</tr>
<tr>
<td>atmVccAal5EncapsType</td>
<td>RO</td>
</tr>
<tr>
<td>atmVclCrossConnectIdentifier</td>
<td>RO</td>
</tr>
<tr>
<td>atmVclRowStatus</td>
<td>RO</td>
</tr>
<tr>
<td>aal5VccTable</td>
<td></td>
</tr>
<tr>
<td>aal5VccEntry</td>
<td></td>
</tr>
<tr>
<td>aal5VccVpi</td>
<td>RO</td>
</tr>
<tr>
<td>aal5VccVci</td>
<td>RO</td>
</tr>
<tr>
<td>aal5VccCrcErrors</td>
<td>RO</td>
</tr>
<tr>
<td>aal5VccSarTimeOuts</td>
<td>RO</td>
</tr>
<tr>
<td>aal5VccOverSizedSDUs</td>
<td>RO</td>
</tr>
</tbody>
</table>