ATLAS 810*PLUS*

User Manual

Part Number 1200265L1
Part Number 1200266L1

61200266L1-1A
July 1999

TRADEMARKS

Windows is a registered trademark of Microsoft Corporation.
DMS 100 is a registered trademark of Northern Telecom.
5ESS is a registered trademark of AT&T.
AT&T is a registered trademark.

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

ADTRAN Year 2000 (Y2K) Readiness Disclosure

ADTRAN has established a Year 2000 program to ensure that our products will correctly function in the new millennium. ADTRAN warrants that all products meet Year 2000 specifications regardless of model or revision. Information about ADTRAN's Year 2000 compliance program is available at the following:

Product Matrix	www.adtran.com/y2kfax.html
E-mail	year2000@adtran.com
Faxback Document Line	(256) 963-8200 *Y2K plans and product certifications are listed in the Product Matrix (see above).*
Y2K Project Line	(256) 963-2200

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

1. This equipment complies with Part 68 of the FCC rules. The required label is affixed to the bottom of the chassis.
2. 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 a compatible modular jack which is Part 68-compliant. See Chapter 2, *Installation*, for details.
3. If your telephone equipment (ATLAS) causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.
4. Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be given advance notice to give you an opportunity to maintain uninterrupted service.
5. If you experience trouble with this equipment (ATLAS), please contact ADTRAN at (256) 963-8000 for repair / warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or until you are sure the equipment is not malfunctioning.
6. This unit contains no user-serviceable parts.
7. The following information may be required when applying to your local telephone company for leased line facilities.

Service Type	REN/SOC	FIC	USOC
1.544 Mbps - SF	6.0N	04DU9-BN	RJ-48C
1.544 Mbps - SF and B8ZS	6.0N	04DU9-DN	RJ-48C
1.544 Mbps - ESF	6.0N	04DU9-1KN	RJ-48C
1.544 Mbps - ESF and B8ZS	6.0N	04DU9-1SN	RJ-48C
ISDN	6.0N	04DU9-ISN	RJ-48C

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.

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

WARNING *Change 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 voiceband analog signals and transmitted on the network.
- The affidavit shall affirm that either no encoded analog content or billing information is being transmitted or that the output of the device meets Part 68 encoded analog content or billing protection specifications.
- End user/customer will be responsible for filing an affidavit with the local exchange carrier when connecting unprotected customer premise equipment (CPE) to 1.544 Mbps or subrate digital services.
- Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirement for subrate services is waived.

Affidavit for Connection of Customer Premises Equipment to 1.544 Mbps and/or Subrate Digital Services

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

State of _____

County of _____

I, _____ (name), _____(business address),

_____ (telephone number) being duly sworn, state:

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

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

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

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

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

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

( ) B. A training course provided by the customer or authorized representative, using training mate-

rials 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:

_____

Canadian Equipment Limitations

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 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.

About this Manual

The ATLAS 810^{PLUS} system consists of the Base Unit and one or more option modules. (Each option module includes its own user manual which contains specific information about installing, configuring, and testing the option module; insert the option module manuals into this binder.) This ATLAS User Manual provides the information you need to install, configure, test, and troubleshoot the ATLAS 810^{PLUS} system; when applicable, this manual refers you to the individual option module user manual. The arrangement of this user manual allows you to quickly and easily find the information you need. An overview of the contents of this manual follows:

Introduction

- *Introduction* on page 1-1, familiarizes you with the ATLAS 810^{PLUS} Base Unit and provides some sample ATLAS 810^{PLUS} applications.

Getting Started

- Chapter 2, *Installation*, describes the rear panel layout and how to install the ATLAS 810^{PLUS}.
- Chapter 3, *Operation*, describes the front panel layout and different ways to operate the ATLAS 810^{PLUS}.

Reference Information

- Chapter 4, *Using the Front Panel*, describes how to use the front panel. This chapter also describes each menu option that is accessible through the front panel.
- Chapter 5, *Navigating the Terminal Menu*, describes how to navigate the terminal menu.
- Chapter 6, *Terminal Menu and System Control*, describes the terminal menus used for system control.
- Chapter 7, *Modules Terminal Menu*, describes the terminal menus used for module and T1 / PRI port control.
- Chapter 8, *Dedicated Maps Terminal Menu*, describes the terminal menus used for Dedicated Maps and provides some examples.
- Chapter 9, *Dial Plan Terminal Menu*, describes the terminal menus used for Dial Plans and provides some examples.

Working with the ATLAS 810^{PLUS}

- Chapter 10, *Updating Firmware*, provides step-by-step instruction on how to update the ATLAS 810^{PLUS} firmware.
- Chapter 11, *SNMP Management*, describes how to control the ATLAS 810^{PLUS} via SNMP.
- Chapter 12, *ADTRAN Utilities*, describes the SysLog, Telnet, VT-100, and TFTP Server programs delivered with the ATLAS 810^{PLUS}.

Appendices

- Appendix A, *System Event Logging*, describes the events monitored by the ATLAS 810^{PLUS}.
- Appendix B, *Troubleshooting*, describes how to diagnose different problems you may experience.
- Appendix C, *Warranty and Technical Support Information*, describes your warranty and how to contact technical support.
- Appendix D, *Acronyms and Abbreviations*, lists acronyms and abbreviations used for the ATLAS 810^{PLUS} and its option modules.
- Appendix E, *Glossary*, defines terms used with ATLAS 810^{PLUS} and its option modules.

Notes, cautions, and warnings provide other significant information. They are easily identified, as shown below:

Notes provide additional useful information.

Cautions signify information that could prevent service interruptions.

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

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

PRODUCT OVERVIEW

The ATLAS 810^{PLUS} is a modular, highly scalable platform that provides robust solutions for the wide area communication needs of medium-to-large corporations and network access providers. ATLAS is an Integrated Access System with the most extensive support of dedicated bandwidth management and access switching in the industry.

The ATLAS 810^{PLUS} is a high performance version of the ATLAS 800^{PLUS}. The ATLAS 810^{PLUS} contains a high-performance CPU and powerful communications drivers which allow the support of optional applications such as frame relay.

With the ATLAS 810^{PLUS}, you can consolidate your voice, data, and video applications into a single platform while optimizing wide area bandwidth and reducing equipment costs. The ATLAS 810^{PLUS} architecture and the chassis' eight expansion slots allow for a variety of modules, making it one of the most versatile access systems on the market. With the appropriate modules installed, the ATLAS 810^{PLUS} functions as follows:

- A Frame Relay Switch
- A Digital Access Cross-Connect System (DACS)
- A T1 Bandwidth Manager
- An ISDN Access Switch
- A Remote Access Manager

ATLAS 810^{PLUS} BASE UNIT

The ATLAS 810^{PLUS} architecture includes a packet switching and a circuit switching bussing scheme. The result is a highly scalable system capable of supporting bandwidth requirements up to 34 T1/E1 or Primary Rate ISDN (PRI) circuits. Designed for standalone or rackmount installations, the ATLAS 810^{PLUS} Base Unit provides two network interfaces, each independently configurable for T1, DSX-1, or PRI operation. Eight expansion slots accommodate hot-swappable modules for a variety of applications. A 10BaseT connection for remote access and network management is standard with the ATLAS 810^{PLUS} Base Unit.

The ATLAS modules include the following:

- HDLC Module
- Quad T1/PRI Module
- Octal Basic Rate ISDN Module
- T3 Module
- Async-232 Module
- Modem-16 Module

Frame Relay

Frame relay is a packet-switched service that allows efficient transfer of bursty traffic in a WAN environment. It offers lower-cost data transfer when compared to typical point-to-point applications. Using virtual connections within the frame relay network and combining those into a single physical connection at each location result in lower cost. Frame relay providers use a frame relay switch to route the data on each virtual circuit to the appropriate destination. Figures 1-1 and 1-2 illustrate a conversion from a typical point-to-point application to a frame relay application.

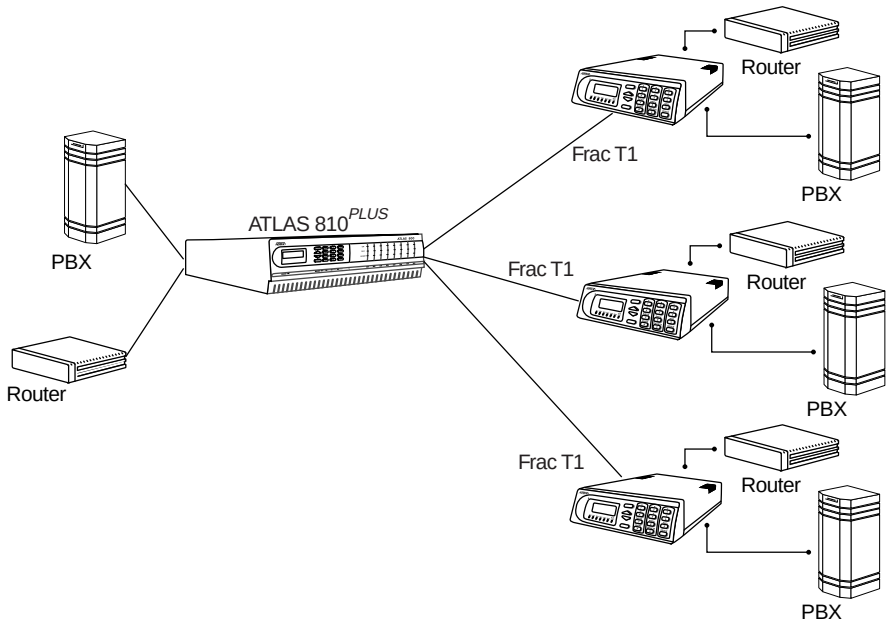


Figure 1-1. Point-to-Point Circuit

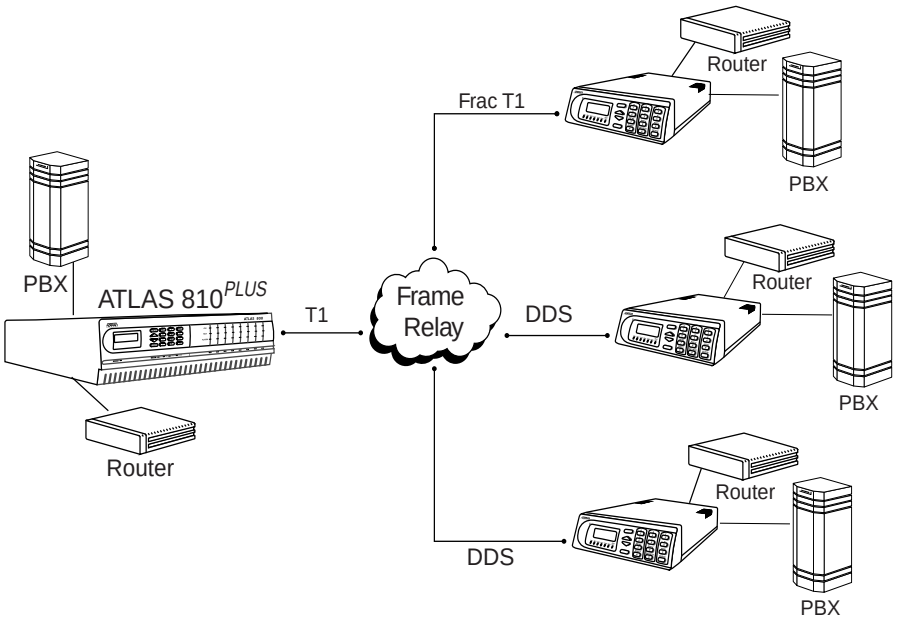


Figure 1-2. Frame Relay Circuit

The Frame Relay / Router upgrade option adds the capability for the ATLAS series of Integrated Access Devices to act as a voice / data FRAD, a frame relay switch, and an IP router in addition to the current available bandwidth manager and switch applications.

Dedicated and Switched Connection Maps in a Single Platform

The ATLAS 810*PLUS* allocates dedicated bandwidth according to any of up to five unique connection maps. Any DS0 on any T1 circuit can be mapped to any other DS0 on up to 34 T1 circuits in the system. Dedicated connection maps can be manually invoked or automatically implemented based on the time of day and day of the week.

Additionally, the ATLAS 810*PLUS* can be configured to switch dialup calls to specific ports or DS0s based on the number that is dialed. Switched connection mapping is supported for dialup calls placed over basic rate ISDN, primary rate ISDN, or channelized T1.

Signaling Conversion for Maximum Interoperability

The ATLAS 810*PLUS* can convert between Robbed Bit Signaling and ISDN D channel signaling, giving you the flexibility to get the speed and reliability of ISDN, while preserving your investment in non-ISDN equipment. ATLAS can also convert between D4 and ESF frame formats as well as AMI and B8ZS line coding, providing interoperability with legacy equipment.

Flexible Network Management and Maintainability

Several network management methods are available for the ATLAS 810*PLUS*, including SNMP support. VT 100 and Telnet are also offered, providing detailed system configuration through an easy-to-use menu system. The terminal interface is secured by six levels of password protection with varying degrees of management privileges. The terminal interface is accessed locally or remotely using either the EIA-232 Chain In port on the rear of the unit or the Telnet interface. The 10BaseT interface on the Base Unit provides an Ethernet connection for SNMP and Telnet connections.

Additionally, T-Watch PRO, ADTRAN's Microsoft® Windows®-based GUI management system, allows end-to-end management with downstream ADTRAN T1 products. User configurations can be preserved in non-volatile memory and duplicated for managing multiple ATLAS implementations. ATLAS also supports FLASH upgrades for future enhancements. You can remotely download software using TFTP or XMODEM.

The ATLAS 810*PLUS*front panel contains an extensive array of LEDs for alarm and status information pertaining to the system and the individual modules.

Several test capabilities allow you to diagnose the health of your T1, PRI, or BRI circuits without additional test equipment. Standard Bantam test jacks located on the ATLAS 810*PLUS* rear panel also allow you to use external test equipment to monitor traffic. Tests include local, remote, and V.54 loopbacks utilizing the 511, QRSS, all zeros, and all ones test patterns.

Digital Access Cross-Connect System (DACS)

Inherent in the ATLAS 810*PLUS* architecture is the ability to cross connect, or DACS, up to thirty-four T1 circuits. DACSing allows the assignment and redistribution, or grooming, of any DS0 on any T1 circuit to any other DS0 on any of the thirty-four T1 circuits in the system. For optimizing network resources, any of five dedicated connection maps can be invoked manually or automatically, based on the time of day and day of the week (see Figure 1-3).

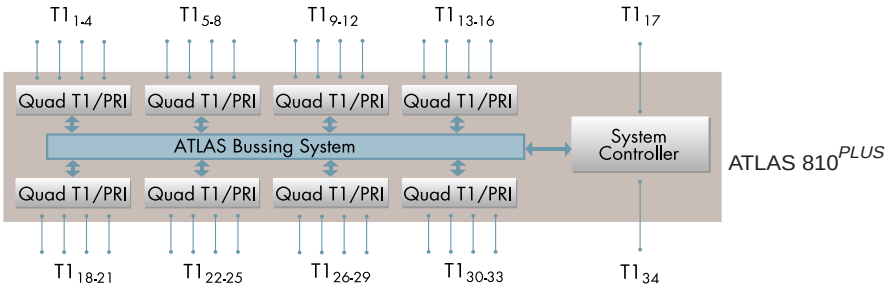


Figure 1-3. Digital Access Cross-Connect System (DACS)

T1 Bandwidth Manager

As a T1 Bandwidth Manager, ATLAS 810^{PLUS} combines the functions of a T1 CSU / DSU, an intelligent channel bank, a T1 Multiplexer, and DACS into a single platform. The Bandwidth Manager supports a wide range of data applications including T1 "drop and insert," channel grooming, and wide area data transport. ATLAS is ideal for point-to-point configurations or access to public networks. For optimization of existing equipment and network resources, ATLAS can be paired with ADTRAN's TSU product offerings to support a variety of data and analog voice applications (see Figure 1-4).

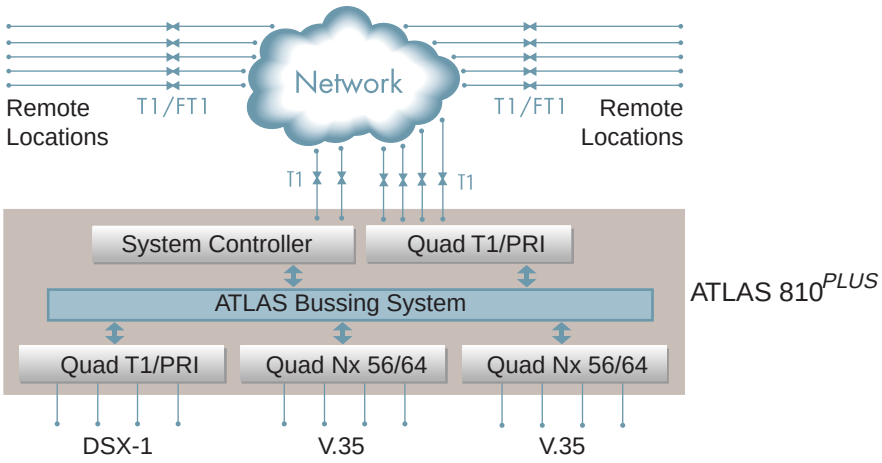


Figure 1-4. T1 Bandwidth Management

ISDN Access Switch

The ATLAS 810^{PLUS} includes an advanced access architecture for switching dialup calls to specific ports or DS0s. As an access switch functioning in a user-to-user network and user-to-user mode, ATLAS consolidates multiple basic rate ISDN (BRI) connections onto T1 / PRI access lines. Additionally, BRI-to-BRI, BRI-to-PRI, and PRI-to-PRI switching are supported. ATLAS also converts between ISDN D channel (PRI or BRI) and T1 Robbed Bit Signaling, allowing a non-ISDN PBX to access a more efficient ISDN facility. For network optimization, when bandwidth is not being used for switched applications such as video conferencing, switched connection mapping dynamically allocates bandwidth to the PBX for voice traffic. Call Filtering allows you to program the call types that will be answered and / or originated on a per-user basis.

WAN Overbooking

The WAN Overbooking feature of ATLAS 810^{PLUS} allows you to oversubscribe switched bandwidth for situations where simultaneous access to the network by every subscriber is not required. WAN Overbooking reduces telecommunications expenses while still giving your subscriber base the connectivity they require. Local subscriber-to-subscriber connections are made without accessing the network at all, resulting in even more efficient use of wide area bandwidth (see Figure 1-5 on page 1-6).

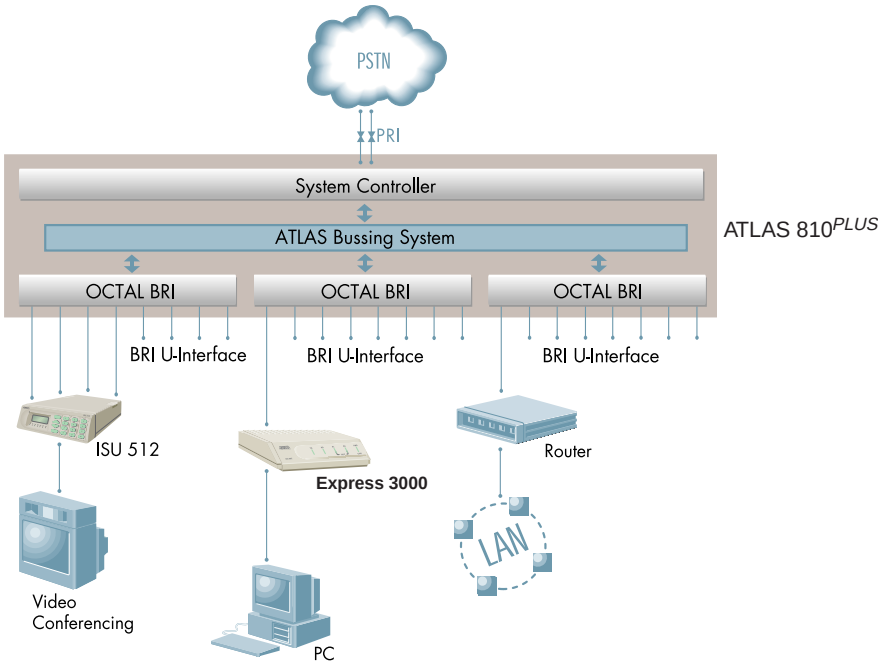


Figure 1-5. WAN Overbooking

ATLAS 810*PLUS* FEATURES

Configuration and Management

- VT-100 Emulation
- T-Watch PRO, Microsoft Windows-based GUI
- SNMP, per MIB II (RFC1213), DS1 MIB (RFC1406), and ADTRAN private MIBs
- Telnet
- Six levels of password protection and privileges

Software Upgrade

- Flash memory
- TFTP download
- XMODEM via control port

Signaling Support

- ISDN D Channel
- Robbed bit, E&M, Ground Start, Loop Start
- Convert between Robbed Bit Signaling and ISDN D Channel
- Direct Inward Dialing

ISDN Switch Types

- 5ESS™, DMS-100™, National ISDN, 4ESS™

Dedicated Connection Maps

- Up to five connection maps
- Time of day / day of week configurable
- Preserves signaling through cross-connect
- No effect on nonconfigured channels

Switched Connection Maps

- Inbound and outbound call filtering and blocking

Testing

- Local and remote: payload / line, V.54
- Patterns: 511, QRSS, all ones, all zeros

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

Chapter 2 Installation

INSPECT THE ADTRAN SHIPMENT

Before installing the ATLAS 810*PLUS*, carefully inspect the ATLAS 810*PLUS* Base Unit for shipping damage. If you suspect damage, file a claim immediately with the carrier and then contact ADTRAN Technical Support (see *Warranty and Technical Support Information* on page C-1). If possible, keep the original shipping container for returning the ATLAS 810*PLUS* for repair or for verification of damage during shipment.

Contents of ADTRAN Shipments

Your ADTRAN shipment includes the following items:

- The ATLAS 810*PLUS* Base Unit
- The ATLAS 810*PLUS* *User Manual*
- Power cord (AC unit only) - ADTRAN P/N 3127031
- Network cables (2) - ADTRAN P/N 3125M008
- Rackmount brackets (left and right)
- RJ45—DB-25 adapter (modem and direct)
- RJ-45 control port cable (1) - ADTRAN P/N 3127004
- DSX-1 crossover cable (1) - ADTRAN P/N 3125M010
- RJ-48—DB-15 adapter (1)
- ADTRAN Utilities diskettes (3)

Customers must supply the 10BaseT cable.

CHECK THE POWER CONNECTION

Check the power connection appropriate to your power supply (AC or DC.)

AC Powered Unit

The AC powered ATLAS 810^{PLUS} (P / N 1200265L1) comes equipped with a detachable 8-foot power cord with a 3-prong plug for connecting to a grounded power receptacle.

Power to the ATLAS 810^{PLUS} must be from a grounded 115 VAC, 60 Hz or 220 VAC, 50-60 Hz source.

DC Powered Unit

The DC powered ATLAS 810^{PLUS} (P / N 1200266L1) comes equipped with a terminal block on the rear of the unit. The power source should be connected to the terminal block according to the polarity markings on the unit. For example, a -48 V source would be connected with the -48 V return connected to the (+) terminal and the -48 VDC attached to the (-) terminal. Power must be from a DC power source in the range of 42 to 57 VDC, capable of delivering up to 7 A of current.

- *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).*
- *The branch circuit overcurrent protection shall be a fuse or circuit breaker rated minimum 48 V, maximum 20 A.*
- *A readily accessible disconnect device that is suitably approved and rated shall be incorporated into the fixed wiring.*

GROUNDING INSTRUCTIONS

This section provides grounding instruction information from the Underwriters' Laboratory UL 1950 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.

REVIEW THE REAR PANEL DESIGN

The ATLAS 810*PLUS* rear panel contains eight slots for housing option modules which provide a variety of additional resources and data ports. All slots are functionally identical except slots 7 and 8, which can also accommodate an optional power supply for redundancy. See Figure 2-1 (AC powered unit) and Figure 2-2 (DC powered unit).

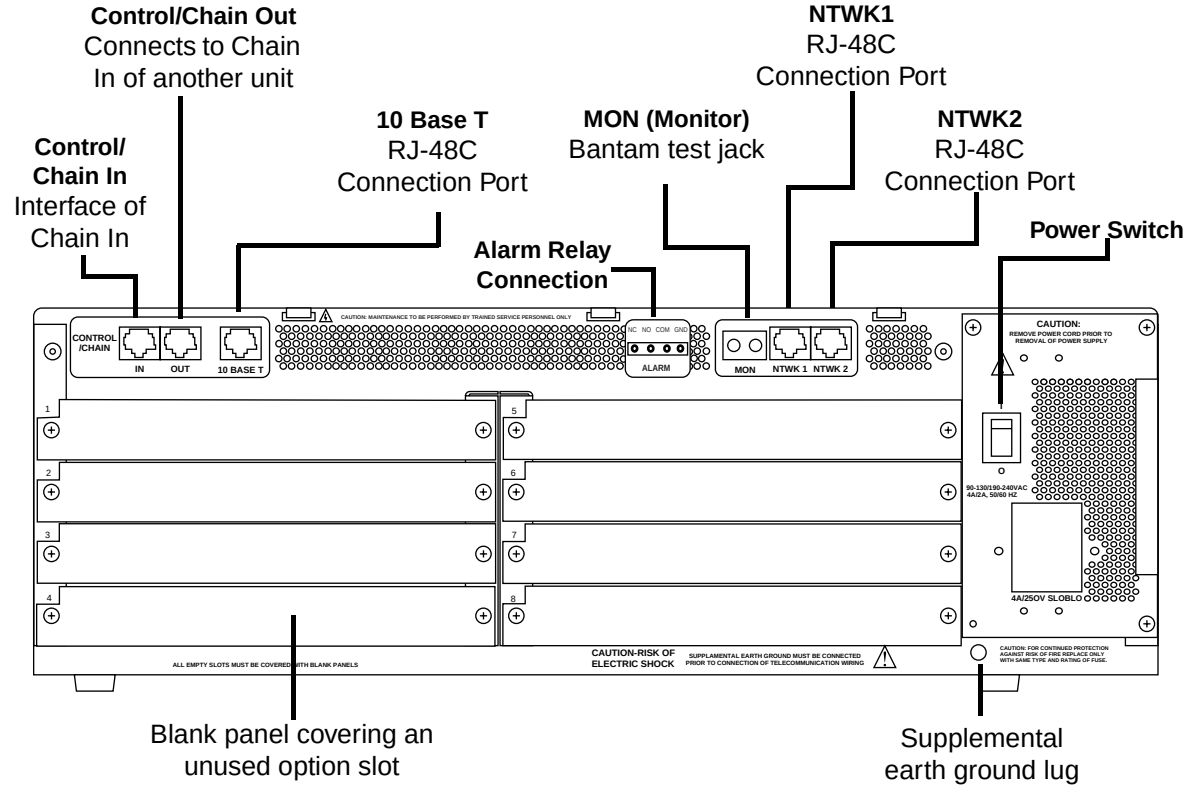


Figure 2-1. AC Powered ATLAS 810*PLUS* Rear Panel

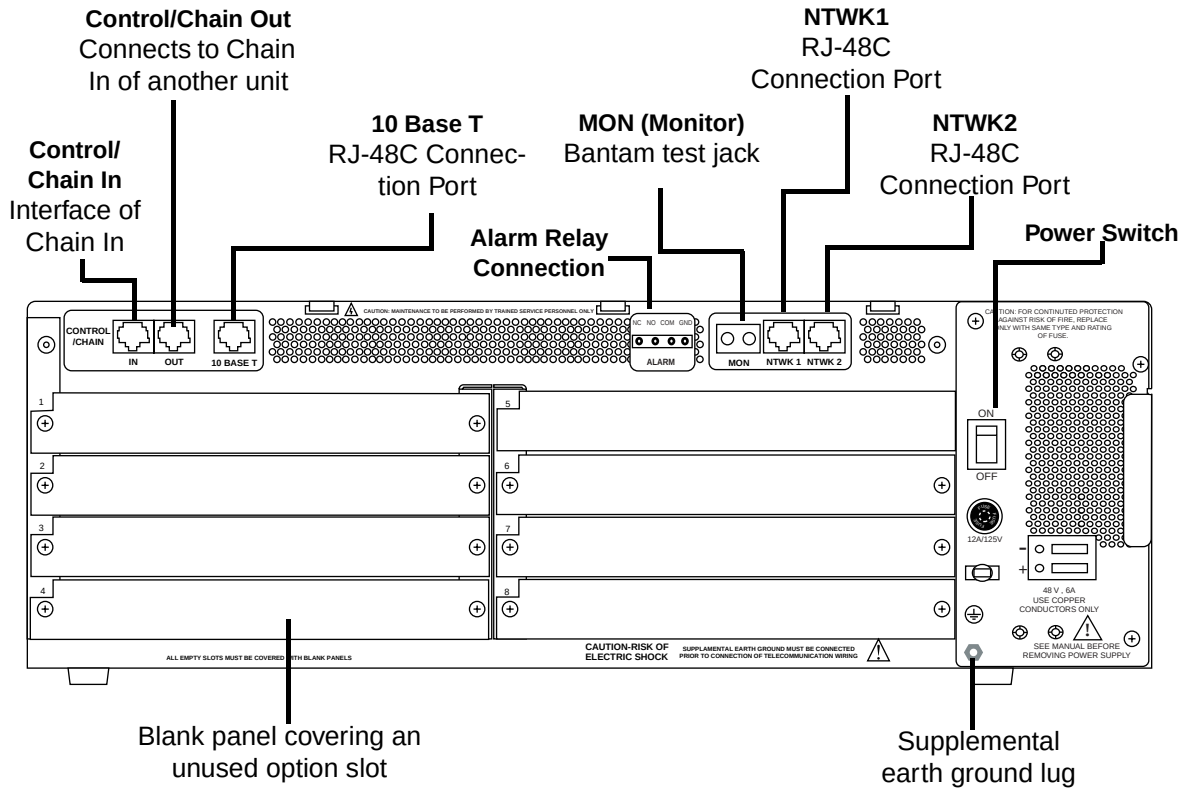


Figure 2-2. DC Powered ATLAS 810*PLUS* Rear Panel

Control/Chain In Port

The Control / Chain In port (EIA-232) connects to a computer or modem (Control In) or to another ATLAS 810*PLUS* Base Unit (Chain In). The control port input provides the following functions:

- Accepts EIA-232 input from a PC or a modem for control of the ATLAS 810*PLUS*.
- Attaches to another ATLAS 810*PLUS* (chain input).
- Operates at 2400, 9600, 19200, or 38400 bps.
- Acts as input for PC control or as input for a chained connection.
- Acts as an interface for flash memory software downloads using XMODEM.

Connection

The Control / Chain In connection follows with the pinout shown in Table 2-1.

Connector type RJ-48C
Part number AMP# 555164-2

Table 2-1. Control/Chain In Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis
2	RTS	Request to send - flow control
3	RXDATA	Data received by the ATLAS 810*PLUS*
4	DTR	Data terminal ready
5	TXDATA	Data transmitted by the ATLAS 810*PLUS*
6	CD	Carrier detect
7	UNUSED	—
8	CTS	Clear to send - flow control

Control/Chain Out Port

The Control / Chain Out port (RJ-48C) connects to another ATLAS 810*PLUS* Chain In connector. The Control / Chain Out port output provides the following:

- EIA-232 output to chain control to other ATLAS 810*PLUS* Base Units
- 2400, 9600, 19200, or 38400 bps operation
- Automatic setup; no user input required

Connection

The Control / Chain Out connection follows, with the pinout shown in Table 2-2 on page 2-6.

Connector type RJ-48C
Part number AMP# 555164-2

Table 2-2. Control/Chain Out Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis. Connects to GND of next unit (pin1).
2	UNUSED	—
3	TX DATA	Data transmitted to chained units by the ATLAS 810^{PLUS}. Connects to RX DATA of the next unit (Chain In pin 3).
4	UNUSED	—
5	RX DATA	Data received from chained units by the ATLAS 810^{PLUS}. Connects to TX DATA of the next unit (Chain In pin 5).
6,7,8	UNUSED	—

Ethernet 10BaseT Connection

The 10BaseT Ethernet port (RJ-48C) provides an Ethernet LAN connection, which is used for TFTP, SNMP, and Telnet connection.

Connection

The network connection follows, with the pinout shown in Table 2-3.

Connector type (USOC) RJ-48C
Part number AMP# 555164-2

Table 2-3. Ethernet 10BaseT Pinout

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

Alarm Relay Connection

This connection alerts the user when a selected alarm condition exists. The four-pin, removable terminal block connects with external wiring. To make the appropriate connections, remove the block, connect wiring as needed, and return the terminal block to the connector socket. Clear the alarm condition by pressing the Alarm Cut-Off (ACO) switch located on the font panel of the ATLAS 810^{PLUS}.

After the appropriate connections have been made, tighten the screws using a flathead screwdriver before reinserting the terminal block into the rear panel of the ATLAS 810^{PLUS}.

Connection

Table 2-4 shows the pinout for the Alarm Relay connector.

Table 2-4. Alarm Relay Connector Pinout

Pin	Name	Description
1	Normally Closed (NC)	Opens when a selected alarm condition is present.
2	Normally Open (NO)	Closes when a selected alarm condition is present.
3	Common (COM)	Common connection between external circuitry and NC or NO terminal.
4	Chassis Ground (GND)	

Mon

The MON (monitor) test jack provides a bridged access jack for non-intrusive monitoring of the T1 circuits receiving data. When connected to this jack, the test equipment should be configured for a bridged termination.

Network Connection

The two eight-pin modular jacks labeled **NTWK 1** and **NTWK 2** provide the network connection. The two Network Interface (NI) ports comply with the applicable ANSI and AT&T® standards. The NIs provide the following functions:

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

Connection

The network connection follows, with the pinout shown in Table 2-5.

Connector type (USOC) RJ-48C
Part number AMP# 555164-2

Table 2-5. Network Pinout

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

Option Slots

Figure 2-3 shows the option slot numbering designation, as viewed from the rear of the ATLAS 810^{PLUS}. All slots are functionally identical except slots 7 and 8, which can also accommodate an optional power supply for redundancy.

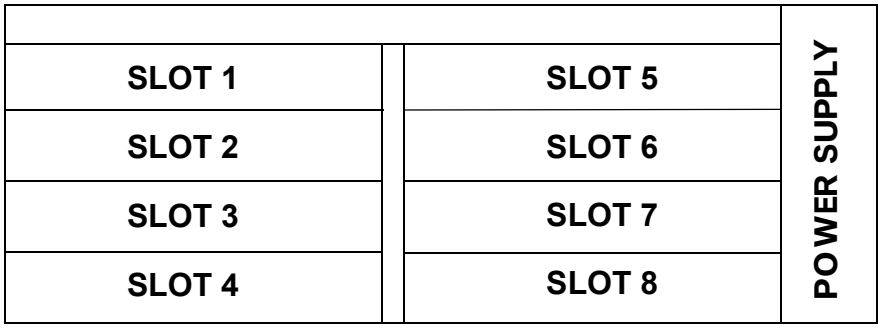


Figure 2-3. ATLAS 810^{PLUS} Slot Designation (Rear View)

INSTALL ANY OPTION MODULES

After installing the base ATLAS 810^{PLUS} Base Unit and connecting the required cables, you can install your choice of option modules. Instructions for installing option modules are given in the user manuals for the chosen modules.

POWER-UP

As shipped, the ATLAS 810^{PLUS} is set to factory default conditions. After installing the Base Unit and any option modules, the ATLAS 810^{PLUS} is ready for power-up.

Chapter 3 Operation

OVERVIEW

To fully operate the ATLAS 810^{PLUS}, you must connect to the terminal menu using VT-100 terminal emulation or a Telnet session. For limited configuration control, use T-Watch PRO. The following sections provide an overview of these methods of operating the ATLAS 810^{PLUS}.

USING THE TERMINAL MENU

The terminal menu provides the primary means of monitoring and configuring the ATLAS 810^{PLUS}. The terminal menu interface uses the full capabilities of the VT-100 terminal to provide the quickest and most intuitive operation possible. (Access the terminal menu using a VT-100 terminal or a computer running VT-100 terminal-emulation software.) To receive the full benefit of the terminal menu interface, you should use a fully VT-100 compatible client. The *ADTRAN Utilities* floppy disks (that you can install on a PC) contain both a VT-100 client and a customized Telnet program. See *ADTRAN Utilities* on page 12-1 for details on the available programs.

The three basic connection methods supported by the ATLAS 810^{PLUS} are a a direct connection through the EIA-232 Chain In port (located on the rear panel), a direct connection through the EIA-232 CRAFT port (located on the front panel), and a Telnet session. The following sections describe using VT-100 terminal emulation (for either of the two EIA-232 ports) and establishing a Telnet session.

Using VT-100 Terminal Emulation

You can access the ATLAS 810^{PLUS} terminal menu, using VT-100 terminal emulation, from either the Chain In port on the rear panel or the CRAFT port on the front panel. Both of these ports provide an EIA-232 serial connection. The following Step / Action table provides instructions for setting up the ATLAS 810^{PLUS} for VT-100 terminal mode.

Instructions for Setting Up an ATLAS 810*PLUS* for VT-100 Terminal Mode	
Step	**Action**
1	Set the baud rate on the VT-100 terminal to 9600 baud (8/N/1).
2	Use the ADTRAN-provided VT-100 terminal adapter to connect the **COM** port of a VT-100 compatible terminal, or equivalent, to the eight-pin modular jack labeled **CONTROL/CHAIN IN** on the rear panel **or** labeled **CRAFT** on the front panel. *This connection provides both local and remote configuration.*
3	Repeatedly press **Enter** on the keyboard until the **Login** menu requiring a password appears.
4	If necessary, press **Ctrl-R** to refresh the display.

When you begin the VT-100 session, you will be prompted for a password. The default password is **password** (which is a Level 0 superuser password). You can change this password using the **Access Passwords** option, which is only accessible through the terminal menu. See *Access Passwords* on page 6-13 for details. After your password is accepted, define the IP Address of the ATLAS 810*PLUS* to which you want to connect. The following Step / Action chart describes this process.

Instructions for Defining the IP Address	
Step	**Action**
1	Obtain an IP address for the ATLAS 810*PLUS* from your LAN administrator.
2	Use the ADTRAN-provided VT-100 terminal adapter to connect the **COM** port of a VT-100 compatible terminal, or equivalent, to the eight-pin modular jack labeled **CONTROL/CHAIN IN** on the rear panel **or** labeled **CRAFT** on the front panel. *This connection provides both local and remote configuration.*
3	Repeatedly press **System** on the front panel until the **Login** menu appears. Enter your password.
4	When the terminal menu opens, navigate the following path: **ATLAS 810PLUS / System Config / Ethernet port / IP Address**
5	Key in the entire IP address, and then press **Enter**.

You will need a default gateway if the LAN contains multiple segments. Contact your LAN administrator for the appropriate address.

USING TELNET

To connect to the ATLAS 810^{PLUS} via Telnet, you must define the IP address, set the subnet mask, and, typically, set the default gateway IP address.

> **NOTE** *You must define the IP address before attempting to connect via Telnet. See Using VT-100 Terminal Emulation on page 3-1 for details on defining the IP address.*

> **NOTE** *You will need a default gateway if the LAN contains multiple segments. Contact your LAN administrator for the appropriate address.*

Starting a Telnet Session

When you begin the Telnet session, you will be prompted for a password. The default password is **password** (which is a Level 0 superuser password). You can change this password using the **Access Passwords** option, which is only accessible through the terminal menus. See *Access Passwords* on page 6-13 for details. The Telnet session will time out and display the Login prompt after a pre-defined time that is set in the **Session Timeout** option (see *Session Timeout* on page 6-8 for details).

> **NOTE** *Use the* **Max Telnet Sessions** *option to define the number of Telnet sessions that can be active at one time (see Max Telnet Sessions on page 6-8 for details).*

> **NOTE** *Microsoft Telnet version 1.0 does not implement full VT-100 emulation. However, many commercial Telnet clients for Microsoft Windows exist which fully implement VT-100. In addition, a freeware client, recommended for optimum performance, comes with the ATLAS 810^{PLUS}. See VT-100 Utility on page 12-8 for details.*

USING T-WATCH PRO

T-Watch PRO is the ADTRAN Microsoft Windows management software program designed to control TSU units from a remote PC. It provides limited control over the configuration of the ATLAS 810^{PLUS} using a graphic interface. Currently, you can choose ATLAS 810^{PLUS} from a list of products, and T-Watch PRO automatically initiates a Telnet session by which you can connect to and manage the ATLAS 810^{PLUS} Base Unit. At this time, T-Watch PRO automatically receives SNMP traps from an ATLAS 810^{PLUS}.

Chapter 4 Using the Front Panel

OVERVIEW

The front panel contains the System LED, the Alarm Cut-off (ACO) switch, and the CRAFT port. The front panel also contains controller and module status LEDs that provide visual information about the ATLAS 810^{PLUS} Base Unit and any option module that may be installed. Figure 4-1 identifies the System LED, the ACO switch, the CRAFT port, and the LEDs.

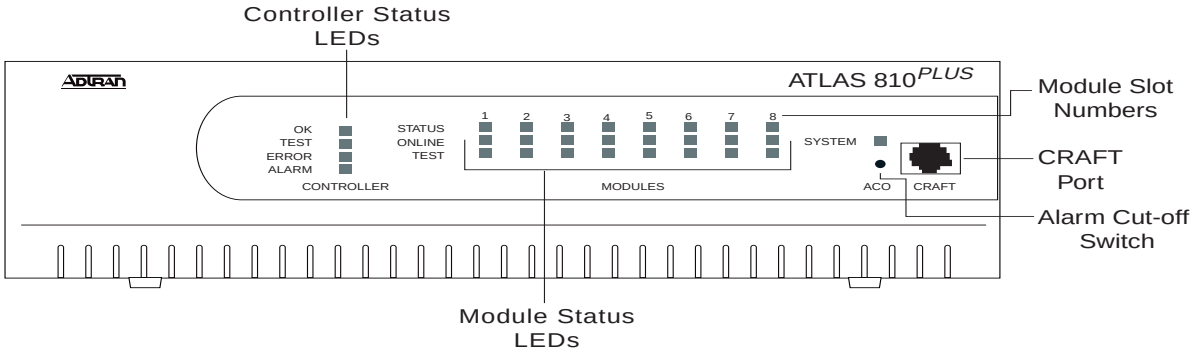


Figure 4-1. ATLAS 810^{PLUS} Front Panel Layout

SYSTEM LED

The System LED indicates the general status of the entire ATLAS 810^{PLUS} (see also *System LED* in Table 4-2 on page 4-3).

ACO SWITCH

The ACO switch deactivates (clears) the Alarm Relay, located on the rear panel of the ATLAS 810^{PLUS}, after an alarm condition has occurred. After the ACO has cleared the Alarm Relay, the same occurrence no longer triggers the Alarm Relay. However, if the alarm condition is corrected and then reoccurs, the Alarm Relay will re-energize (see also *ACO Switch* in Table 4-2 on page 4-3).

CRAFT PORT

Use the CRAFT port to configure the system via an EIA-232 connection. The CRAFT port provides the same functions and operations as the Control In port located on the rear panel of the ATLAS 810^{PLUS}. Table 4-1 gives the CRAFT port pinout (see also *CRAFT Port* on page 4-3 in Table 4-2).

Table 4-1. CRAFT Port Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis
2	RTS	Request to send - flow control
3	RXDATA	Data received by the ATLAS 810^{PLUS}
4	DTR	Data terminal ready
5	TXDATA	Data transmitted by the ATLAS 810^{PLUS}
6	CD	Carrier detect
7	UNUSED	—
8	CTS	Clear to send - flow control

THE FRONT PANEL LEDS

With the ATLAS 810^{PLUS} powered-up, the front panel LED display provides visual information about the status of the ATLAS 810^{PLUS} and any option modules that may be installed. Table 4-2 on page 4-3 provides a brief description of the front panel features, and Table 4-3 on page 4-4 provides detailed information about the LEDs.

Table 4-2. ATLAS 810^{PLUS} Front Panel Description

Feature	Description
Controller Status LEDs	Indicates the status of both network interfaces. (See also Table 4-3 on page 4-4.)
OK	Indicates that both integral network interfaces are operating correctly.
Test	Indicates that one of the network interfaces is in a test mode.
Error	Blinks to indicate the occurrence of error events.
Alarm	Indicates an alarm condition on one of the network interfaces.
Module Slot Numbers	Illuminates to indicate that option modules are installed in the corresponding slots.
Module Status LEDs	Displays, by row, the operational condition (**Status**, **Online**, and **Test**) of each module installed in the option slots. (See also Table 4-3 on page 4-4.)
Status	Displays the operational condition of modules installed in the option slots.
Online	Indicates whether the module is available for use or is currently in use. If the module is manually taken offline, this LED is turned off.
Test	Indicates that one or more ports within a module are in test.
System LED	Indicates the general status of the entire ATLAS 810^{PLUS}. A green light indicates that conditions are normal. A red light indicates a system problem or alarm condition. (See also Table 4-3 on page 4-4.)
ACO Switch	Clears the Alarm Relay connection located on the rear panel of the ATLAS 810^{PLUS}.
CRAFT Port	Allows the ATLAS 810^{PLUS} to connect to a computer or modem using the CRAFT port (an EIA-232 port).

Table 4-3. LED Descriptions

For these LEDs...	This color light...	Indicates that...
System	Green (solid)	No diagnosed system faults were found.
	Green (fast blink)	Flash download is in progress.
	Yellow (solid)	A fault was diagnosed, but the condition no longer exists. The condition will be recorded in the system log.
	Red (solid)	An error condition with either the power supply or the temperature is present.
	Red (fast blink)	A fatal error occurred during flash download.
	Off	Power is not currently supplied to the system.
Controller Status	OK (green)	Both network interfaces are operating normally with error-free operation. If either interface experiences alarms, the **OK** LED remains off.
	Test (yellow)	One of the interfaces is operating in a test mode. This includes a self-test, a test pattern, or a test loopback. When illuminated, this LED also indicates that normal data flow is not occurring in at least one of the module ports.
	Error (flashing red)	Indicates an error such as BPV (bipolar violation), OOF (out of frame), or CRC (cyclic redundancy check).
	Alarm (red)	An alarm condition has been detected. When the alarm condition is no longer valid, the **OK** LED illuminates. To view an alarm condition, select the active alarm menu item or select **Alarm** by pressing **Shift + 8**. If the alarm conditions have been corrected, you can view the alarm which caused the activation of the **Alarm** LED under the **View History** menu.
Module Status	Green (solid)	The module is OK.
	Green (blinking)	The module has been disabled by the user.
	Red (solid)	At least one port on the module has an alarm.
	Red (blinking)	The module is enabled, but is not responding to the system controller.
	Off	No module occupies the slot.
Module Online	Green (solid)	The module is available for use or is currently in use. If the module is manually taken offline, this LED is turned off.
Module Test	Yellow (solid)	One or more ports in a module are in test.

Chapter 5 Navigating the Terminal Menu

TERMINAL MENU WINDOW

The ATLAS 810^{PLUS} uses a multilevel menu structure that contains both menu items and data fields. All menu items and data fields display in the terminal menu window, through which you have complete control of the ATLAS 810^{PLUS} (see Figure 5-1).

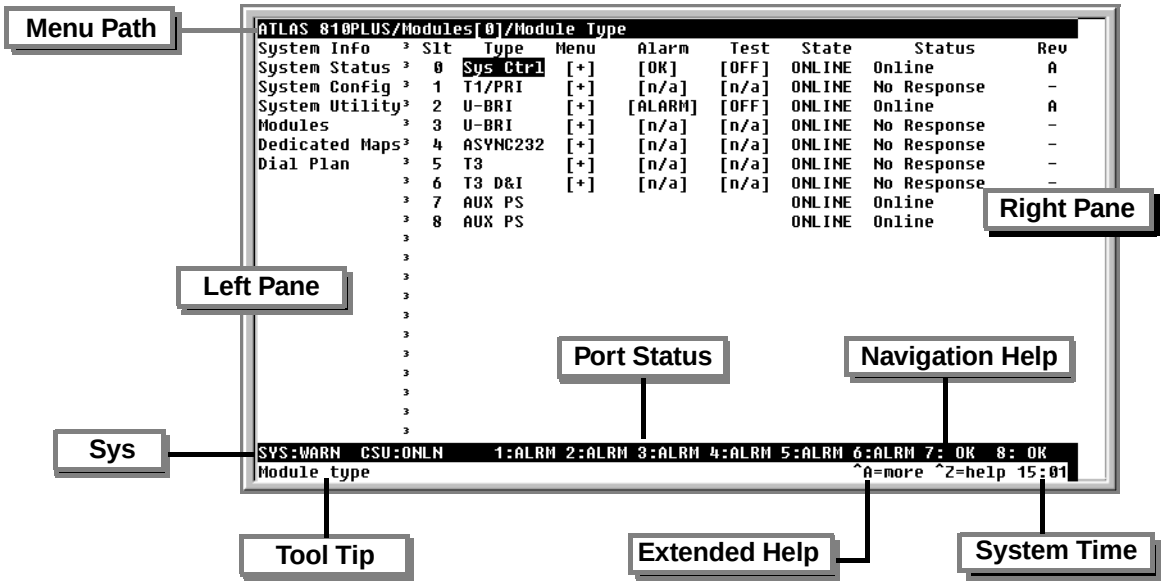


Figure 5-1. Top-level Terminal Menu Window

Menu Path

The first line of the terminal menu window (the menu path) shows the session's current position (path) in the menu structure. For example, Figure 5-1 shows the menu with the cursor on the module **Sys Ctrl**; therefore, the menu path reads **ATLAS 810PLUS/Modules[0]/Module Type.**

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.

Submenus that display horizontally can also be viewed vertically: move your cursor to an index number and press return. Viewing submenus vertically rather than horizontally, allows you to see information at a glance rather than scrolling across the window.

Window Pane Navigation

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

To move...	Press one of these keys...
From left pane to right pane	Tab Enter Left arrow Right arrow
From right pane to left pane	Tab Escape Left arrow Right arrow
Within each pane	Up arrow Down arrow Left arrow Right arrow

Right Window Pane Notation

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

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

Additional Terminal Menu Window Features

The following features are located across the bottom of the window:

Sys	Describes the status of the ATLAS base unit.
Tool Tip	Provides a brief description of the currently selected (highlighted) field.
Port Status	Displays status information, such as OK, WARN (warning), or ALRM (alarm), about ports 1—8.
Extended Help	(**Ctrl-A**) Displays information about selected commands.
Navigation Help	(**Ctrl-Z**) Lists characters used for navigating the terminal menu . See also *Moving through the Menus* on page 5-3
System Time	Displays the current time. See *Current Time/Date (24h)* on page 6-3 for details on editing the time.

NAVIGATING USING THE KEYBOARD KEYS

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

Moving through the Menus

To do this...	Press this key...
Return to the home screen.	H
Jump between two menu items. Press **J** while the cursor is located on a menu item, and you jump back to the main screen. Go to another menu item, press **J**, and you jump back to the screen that was displayed the first time you pressed **J.** Press **J** anytime you want to jump between these items.	J
Select items.	Arrows
Edit a selected menu item.	Enter
Cancel an edit.	Escape
Close pop-up help screens.	Escape

To do this...	Press this key...
Move between the left and right panes.	Tab Arrows
Move to the top of a screen.	A
Move to the bottom of a screen.	Z
Ascend one menu level.	Backspace

Session Management Keystrokes

To do this...	Press this...
Log out of a session.	Ctrl-L
Invalidate the password entry and return to the login screen.	Ctrl-S
Refresh the screen. To save time, only the portion of the screen that has changed is refreshed. This option should only be necessary if the display picks up incorrect characters.	Ctrl-R

Configuration Keystrokes

To do this...	Press this key...
Restore factory default settings. This setting restores the factory defaults based on the location of the cursor. If the cursor is on a module line (in the **Modules** menu), then only the selected module is updated to factory defaults.	F
Copy selected items to the clipboard. The amount of information you can copy depends on the cursor location when you press **C**: If the cursor is over an editable field, only that item is copied. If the cursor is over the index number of a list, then all of the items in the row of the list are copied. For example, if the cursor is over the **Slot #** field in the **Modules** screen, all of the information associated with the slot is copied.	C
Paste the item stored in the clipboard, if the information is compatible. You must confirm all pastes—except those to a single editable field.	P
Increment the value of certain types of fields by one, when you paste information into those fields.	>
Decrement the value of certain types of fields by one, when you paste information into those fields.	<
Insert a new list item. For example, add a new item to the **Dedicated Map** connection list by pressing **I** while the cursor is on an index number.	I
Delete a list item. For example, delete an item from the **Dedicated Map** connection list by pressing **D** while the index number is active (highlighted).	D

Getting Help

The bottom line of the terminal menu window contains context-sensitive help information. When the cursor is positioned over a set of configuration items, a help message (tool tip) displays, when available, providing a description of the set. If more detailed help is available for a particular field, **^A** displays at the bottom of the window. When you press **Ctrl-A,** a pop-up help screen displays additional information about the field.

Press **Ctrl-Z** to activate a help screen that displays the keystrokes for navigating the terminal menu.

Chapter 6

Terminal Menu and System Control

SELECTING THE APPROPRIATE MENU

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

To do this...	Go to this menu...	For more info...
Review and monitor general system information for the ATLAS 810*PLUS*.	**System Info**	See page 6-2.
Review and monitor system status for the ATLAS 810*PLUS*.	**System Status**	See page 6-4.
Set up the operational configuration for the ATLAS 810*PLUS*.	**System Config**	See page 6-7.
Update settings, transfer files, perform system diagnostics, and reboot the ATLAS 810*PLUS*.	**System Utility**	See page 6-16.
Review and configure settings for each installed module, including the ATLAS 810*PLUS* Base Unit.	**Modules**	See page 7-1.
Assign dedicated connections between any two ports in the ATLAS 810*PLUS*.	**Dedicated Maps**	See page 8-1.
Set global ATLAS 810*PLUS* switch parameters or set individual parameters for each port in ATLAS 810*PLUS* that handles a switched call.	**Dial Plan**	See page 9-1.

SECURITY LEVELS

To edit terminal menu items, you must have a password and the appropriate security level. Table 6-1 describes the six security levels. See *Access Passwords* on page 6-13 for additional information on working with passwords.

Table 6-1. Password Security Levels

Security Level	Description
5	Read-only permission for all menu items—**minimum rights.**
4	Read permission for all menu items and permission to use test commands.
3	Access to all commands except passwords, flash download, authentication methods, and interface configurations.
2	Access to all commands except passwords, flash download, and authentication methods.
1	Access to all commands except passwords.
0	Permission to edit every menu item, including creating and editing passwords—**maximum rights.**

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

> MENUS
» Submenus
»» Sub-submenus
Submenu Options

> SYSTEM INFO

The **System Info** menu provides basic information about the unit as well as data fields for editing information. Figure 6-1 displays the submenus that are available when you select this menu item.

```
ATLAS 810PLUS/System Info
System Info    ³ System Name              ATLAS 810PLUS
System Status  ³ System Location          Adtran ATLAS 810 PLUS
System Config  ³ System Contact           ATLAS 810 PLUS
System Utility ³ Firmware Revision        DV206  Rev. DV206 06/09/99 16:40:58
Modules        ³ System Uptime            0 days  20 hours  37 min  49 secs
Dedicated Maps ³ Startup Mode             Warm reboot
Dial Plan      ³ Current Time/Date (24h)  Friday June 11  11:42:15  1999
               ³ Installed Memory         Flash:2097152 bytes  DRAM:16777216 byte
               ³ Serial Number            A854A0005
               ³ Boot ROM Rev             B.04 4/5/99
               ³
               ³
               ³
               ³
               ³
               ³
               ³
               ³
               ³
               ³
SYS:WARN  CSU:ONLN     1:ALRM 2:ALRM 3:ALRM 4:ALRM 5:ALRM 6:ALRM 7: OK  8: OK
System Information menu                                          ^Z=help 11:42
```

Figure 6-1. System Information Menu

» System Name

Security level: 3; Read security: 5

Provides a user-configurable text string for the name of the ATLAS 810^{PLUS}. This name can help you distinguish between different installations. You can enter up to 40 alpha-numeric characters in this field, including spaces and special characters (such as an underbar). This name also displays on the LCD Front Panel.

» System Location

Security level: 3; Read security: 5

Provides a user-configurable text string for the location of the ATLAS 810^{PLUS}. This field is to help you keep track of the actual physical location of the unit. You can enter up to 40 alphanumeric characters in this field, including spaces and special characters (such as an underbar).

» System Contact

Security level: 3; Read security: 5

Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or email address of a person responsible for the ATLAS 810^{PLUS} system. You can enter up to 40 alpha-numeric characters in this field, including spaces and special characters (such as an underbar).

» Firmware Revision

Read security: 5

Displays the current firmware revision level of the controller.

» System Uptime

Read security: 5

Displays the length of time the ATLAS 810^{PLUS} system has been running. Each time you reset the system, this value resets to 0 days, 0 hours, 0 min and 0 secs.

» Startup Mode

Read security: 5

Displays details about the last system startup.

» Current Time/Date (24h)

Security level: 3; Read security: 5

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

» Installed Memory

Read security: 5

Displays the type and amount of memory in use (including Flash memory and DRAM).

» Serial Number

Read security: 5

Displays the serial number for the unit. The serial number of the ATLAS 810^{PLUS} will automatically display in this field.

» Boot ROM Rev

Read security: 5
Displays the boot ROM revision.

> SYSTEM STATUS

The **System Status** menu provides information on the status of the unit. Figure 6-2 shows the submenu functions available in the **System Status** menu.

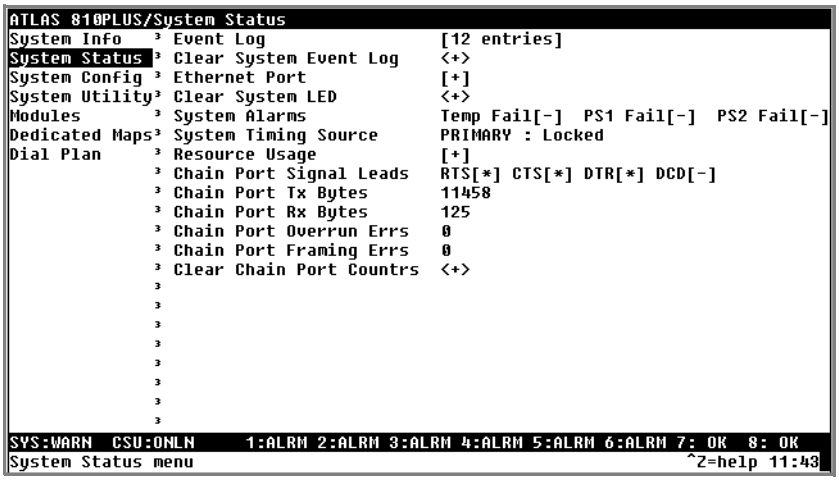


Figure 6-2. System Status Menu

» Event Log

Read security: 5
Displays the last 350 warning or failure messages sent—including the day, date, and priority of the message. The most recent messages display at the top of the list. The following read-only fields are available to review:

»» Time — Displays the date (in mm / dd format) and the time (in hh:mm:ss format) that the event occurred.

»» Cat — Category displays the severity of the event. The possible categories are Critical, Major, Minor, Warning, Normal, and Info. You can specify which types of errors you want the system to log with the System Event Logging option. See *Event Logging* on page 6-12 for details.

»» Src — Displays the type of event.

»» Slot — Displays the slot number in which the event occurred. If this field displays a dash (—), the event occurred in the ATLAS 810^{PLUS} base unit.

»» Port — Displays the port in which the event occurred.

»» Event Description — Displays a description of the event.

» Clear System Event Log

Write security: 3; Read security: 5
Clears the event log. When you select the command, the following prompt displays: **This will clear the entire event log. Confirm (y/n)**. Select **Y** to clear the log or **N** to exit the command.

If you clear the event log, you cannot retrieve the data.

» Ethernet Port

Read security: 5
Displays status information about the Ethernet port. An asterisk (*) indicates activity for the item. The following read-only fields are available to review:

»» I/F Status — Indicates the current status of the 10BaseT port.

»» Tx Frames — Indicates the number of frames transmitted from the 10BaseT port since system startup.

»» Rx Frames — Indicates the number of frames received on the 10BaseT port since system startup.

» Clear System LED

Write security: 3; Read security: 5
Changes the color of the system LED on the front panel from yellow (indicating a previous error) to green (OK). The system LED turns red if the ATLAS 810^{PLUS} detects a major system failure. If the failure condition clears, the LED turns yellow and remains yellow to warn of the past failure.

» System Alarms

Read security: 5
Indicates the status of major system components. An asterisk (*) indicates activity for the items. The following read-only fields display in this field:

»» Temp Fail — The system's internal temperature is outside normal limits.

»» PS1 Fail — The main power supply is not functioning correctly.

»» PS2 Fail — The backup power supply is not functioning correctly.

» System Timing Source

Read security: 5
Indicates which timing source (primary or backup) is currently being used by ATLAS and if ATLAS is locked onto this source. If the display does not indicate locked, the ATLAS 810^{PLUS} does not have a valid source of timing and cannot reliably transfer data. Review the current setting for system timing source in the **System Config** menu. See *Primary Timing Source* on page 6-7 and *Backup Timing Source* on page 6-7 for details.

» Resource Usage — Write security: 4; Read security: 5
Indicates resource use (analog modems; digital modems; voice compression).

»» Data Tables — Tracks resource usage for dynamic resources throughout the system and presents the information in a table format.

- Resource Type — Displays the system resources list.
- Current — Shows the number of resources available (not in use) and the total number of resources. If a resource is taken off line, it is not included in the total.
- Average — Shows the average number of resources available since the statistics were last reset.
- Minimum — Shows the fewest number of resources available since the last reset.
- 0 (zero) available — Provides a count of the number of times the quantity of available resources reached 0.
- Hour Data — Shows availability information by hour for a 24-hour period.
- Reset — Activates the reset of all accumulated availability statistics.

»» Configuration — Write security: 4; Read security: 5
Configures the statistics displayed under data tables.

- Display Formt — Selects the statistics display format—Raw Data or %.
- Reset Mode — Selects the mode for resetting statistics—Manual, Daily, or Weekly.

» Chain Port Signal Leads — Read security: 5
Displays the state of the following options (these fields are read-only). An asterisk (*) indicates activity for the item.

»» RTS — Request to send.

»» CTS — Clear to send.

»» DTR — Data terminal ready.

»» DCD — Data carrier detect.

» Chain Port Tx Bytes — Read security: 5
Displays the number of transmitted data bytes.

» Chain Port Rx Bytes

Read security: 5
Displays the number of received data bytes.

» Chain Port Overrun Errs

Read security: 5
Displays the number of overrun errors.

» Chain Port Framing Errs

Read security: 5
Displays the number of received framing errors.

» Clear Chain Port Countrs

Clears all chain port counters. Press **Y** to activate command.

> SYSTEM CONFIG

The **System Config** menu allows you to set up the ATLAS operational configuration. Figure 6-3 shows the items included in this menu.

```
ATLAS 810PLUS/System Config
System Info    ³ Primary Timing Source   INTERNAL
System Status  ³ Backup Timing Source    INTERNAL
System Config  ³ ADLP Address            9999
System Utility ³ Session Timeout         0
Modules        ³ Max Telnet Sessions     12
Dedicated Maps ³ Ethernet Port           [+]
Dial Plan      ³ Chain Port              [+]
               ³ SNMP                    [+]
               ³ Event Logging           [+]
               ³ Syslog Setup            [+]
               ³ Real Time Clock         [+]
               ³ Access Passwords        [+]
               ³ Licenses                [+]
               ³ BONDING Config          [+]
               ³ Alarm Relay Reset       <+>
               ³ Alarm Relay Threshold   Major
               ³
               ³
               ³
               ³
               ³
SYS:ALRM  CSU:ALRM     1:ALRM 2:ALRM 3:ALRM 4:ONLN 5:ALRM 6:ALRM 7:ALRM 8:ALRM
System Configuration menu                                    ^Z=help 21:15
```

Figure 6-3. System Configuration Menu

» Primary Timing Source

Write security: 3; Read security: 5
Selects the primary timing source. You can select either **INTERNAL** or a port from one of the installed modules.

» Backup Timing Source

Write security: 3; Read security: 5
Selects the secondary timing source. You can select either **INTERNAL** or a port from one of the installed modules. ATLAS 810^{PLUS} uses the backup timing source if the primary timing source goes into alarm. The **Backup Timing Source** should be different from the **Primary Timing Source**.

» ADLP Address

Write security: 2; Read security: 5
Shows the system ADTRAN Data Link Layer Protocol (ADLP) address for connecting remote devices to management software (such as T-Watch PRO). The allowable range is between 2 and 65520. Enter a value not used by any of the TSU units controlled by the management software.

» Session Timeout

Write security: 3; Read security: 5
Defines the number of seconds the terminal session must remain idle before the session times out. You can enter zero to deactivate this option (the session will never time out).

» Max Telnet Sessions

Write security: 3; Read security: 5
Defines the maximum number of Telnet sessions that can be active at the same time. Enter a number between 0 and 100 in this field.

If you enter zero in this field, you will not be able to use Telnet. Only enter zero if you want to completely lock out Telnet access.

» Ethernet Port

Write security: 2; Read security: 5
Provides a way to configure various settings for the Ethernet port. The following options are available for review and editing:

»» Port Name

Defines the name of the Ethernet port. You can leave this field blank.

»» IP Address

Lists the address assigned to the base Ethernet port. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This value is set to 0.0.0.0 by default. The IP address is used for the 10BaseT Ethernet interface. Obtain the correct IP address from your LAN administrator.

»» Default Gateway

Defines or changes the default gateway. Enter the default gateway address by entering a decimal number into the appropriate field and then pressing **Enter** to move to the next field. You will need a default gateway if the LAN contains multiple segments. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This value is set to 0.0.0.0 by default. Contact your LAN administrator for the appropriate address.

»» Subnet Mask

Defines which part of a destination IP address contains the network number. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This value is set to 0.0.0.0 by default. This part of the destination IP address is used along with the ATLAS 810^{PLUS} IP address to determine which nodes must be reached through the default IP gateway.

»» MAC Address

Displays the system Ethernet Media Access Control (MAC) address.

» Chain Port
Write security: 2; Read security: 5
Accepts input for configuring the Chain In port.

»» Port Name
Write security: 2; Read security: 5
Defines the name of the chain port. Type in an alpha-numeric name up to 57 characters long. The name can include spaces and special characters.

»» Port Type
Write security: 2; Read security: 5
Specifies whether you use **Direct** or **Dial** mode.

»» Port Speed
Write security: 2; Read security: 5
Specifies the baud rate of the port. Select either 2400, 9600, 19200, or 38400. If you are using **Dial** for **Port Type**, ensure that the **Port Speed** setting matches the modem baud rate.

»» Modem Initialization String
Write security: 2; Read security: 5
Specifies the initialization string for a modem. Refer to your modem documentation for acceptable initialization strings.

»» Initialize Modem
Write security: 4; Read security: 5
Sends the Modem Initialization string to the modem. When you select this command, the following message displays: **Please verify a modem is connected to the chain port before continuing. Confirm (y/n).** Ensure that a modem is connected before selecting **Y**.

»» Flow Control
Write security: 2; Read security: 5
Sets the flow control for the Chain In port. You may configure the Chain In port flow control for **OFF** or **H/W** (hardware).

» SNMP
Write security: 3; Read security: 5
Provides a way to configure SNMP access for the ATLAS 810^{PLUS}. For detailed information on SNMP, refer to *SNMP Management* on page 11-1. The following options are available for review and editing:

»» SNMP Access
Write security: 3; Read security: 5
Defines whether SNMP access to the ATLAS 810^{PLUS} is enabled or disabled. Select the appropriate option.

»» SNMP Communities
Write security: 3; Read security: 5
Defines SNMP manager(s) characteristics as follows:

IP Address
Specifies the IP address of the network manager.

Privileges
Defines Get (read-only) and Get/Set (read and write) privileges.

Get Name
Defines the community name for Get access. This value must match the Get name defined on the network management station. Public is the default name.

Set Name
Defines the community name for Set access. This value must match either the Get or Set name defined on the network management station. Public is the default name.

»» Trap Transmission — Write security: 3; Read security: 5
Enables and disables SNMP trap transmission.

»» Authen Trap Transmission — Write security: 3; Read security: 5
Enables and disables the authentication failure trap.

»» Traps Destination — Write security: 3; Read security: 5
Defines the destination for SNMP traps as follows:

- IP Address — Identifies the IP address to which the network manager sends traps.
- Community — Defines the community name for trap destinations. This name must match the community name defined at the network management station.
- Trap Filtering — Sets the minimum severity level required for a system event to generate an SNMP trap.

  If a trap event occurs and if the trap's severity level is equal to or more severe than the trap type's current threshold setting, that event is sent as an SNMP trap. (Refer to the ATLAS 810^{PLUS} MIB for a listing of all traps and their severity levels.) You can set the following threshold levels for the available selections: disabled, critical, major, minor, warning, normal, and info.
- Station Type — Trap packets destined for the T-Watch GUI-based management station require ".ADLP ADDRESS" to be appended to the Community Name. Defining the Station Type to "T-Watch Mgmt" will automatically update this field within the SNMP trap packet before sending it to the management station. Defining the Station Type to "Normal" will deliver the SNMP trap packet with the Community Name unchanged.

»» DS1 Current Perf TD — Defines performance threshold values for DS1 Line and Path statistics recorded in a 15-minute interval. If a statistic value exceeds its threshold value, then the corresponding Alert Trap will be sent if the alert event is armed and Alert Traps are enabled. These thresholds apply to all DS1 interfaces in the system.

- Current ES Thrsh — The DS1 performance monitor Threshold Value for the Current 15 minute Errored Seconds (ES) parameter. The default value is 65 for an approximate BER level of 10E-5.
- Current SES Thrsh — The DS1 performance monitor Threshold Value for the Current 15 minute Severely Errored Seconds (SES) parameter. The default value is 10 for an approximate BER level of 10E-5.
- Current SEFS Thrsh — The DS1 performance monitor Threshold Value for the Current 15 minute Severely Errored Framing Seconds (SEFS) parameter. The default value is 2 for an approximate BER level of 10E-5.
- Current UAS Thrsh — The DS1 performance monitor Threshold Value for the Current 15 minute Unavailable Seconds (UAS) parameter. The default value is 10 for an approximate BER level of 10E-5.

Current CSS Thrsh	The DS1 performance monitor Threshold Value for the Current 15 minute Controlled Slip Seconds (SES) parameter. The default value is 1 for an approximate BER level of 10E-5.
Current PCV Thrsh (D4)	The DS1 performance monitor Threshold Value for the Current 15 minute Path Code Violation (PCV) parameter, when the Line Type is Super Frame (AT&T D4 format) DS1. The default value is 72 Framing errors for an approximate BER level of 10E-5.
Current PCV Thrsh (ESF)	The DS1 performance monitor Threshold Value for the Current 15 minute Path Code Violations (PCV) parameter, when the Line Type is Extended Super Frame (ESF) DS1. The default value is 13,296 CRC errors for an approximate BER level of 10E-5.
Current LES Thrsh	The DS1 performance monitor Threshold Value for the Current 15 minute Line Errored Seconds (LES) parameter. The default value is 65 for an approximate BER level of 10E-5.
Current LCV Thrsh	The DS1 performance monitor Threshold Value for the Current 15 minute Line Code Violations (LCV) parameter. The default value is 13,340 for an approximate BER level of 10E-5.
»» DS1 Total Current Perf Threshold	Defines performance threshold values for DS1 Line and Path statistics. If a statistic value exceeds its threshold value, then the corresponding Alert Trap will be sent if the alert event is armed and Alert Taps are enabled. These threshold apply to all DS1 interfaces in the system.
Total ES Thrsh	The DS1 performance monitor Threshold Value for the Total Errored Seconds (ES) parameter. The default value is 648 for an approximate BER level of 10E-5.
Total SES Thrsh	The DS1 performance monitor Threshold Value for the Total Severely Errored Seconds (SES) parameter. The default value is 100 for an approximate BER level of 10E-5.
Total SEFS Thrsh	The DS1 performance monitor Threshold Value for the Total Severely Errored Framing Seconds (SEFS) parameter. The default value is 17 for an approximate BER level of 10E-5.
Total UAS Thrsh	The DS1 performance monitor Threshold Value for the Total Unavailable Seconds (UAS) parameter. The default value is 10 for an approximate BER level of 10E-5.
Total CSS Thrsh	The DS1 performance monitor Threshold Value for the Total Controlled Slip Seconds (SES) parameter. The default value is 4 for an approximate BER level of 10E-5.
Total PCV Thrsh (D4)	The DS1 performance monitor Threshold Value for the Total Path Code Violations (PCV) parameter, when the Line Type is Super Frame (AT&T D4 format) DS1. The default value is 691 Framing Errors for an approximate BER level of 10E-5.
Total PCV Thrsh (ESF)	The DS1 performance monitor Threshold Value for the Total Path Code Violations (PCV) parameter, when the Line Type is Extended Super Frame

(ESF) DS1. The default value is 132,960 CRC errors for an approximate BER level of 10E-5.

Total LES Thrsh — The DS1 performance monitor Threshold Value for the Total Line Errored Seconds (LES) parameter. The default value is 648 for an approximate BER level of 10E-5.

Total LCV Thrsh — The DS1 performance monitor Threshold Value for the Current 15 minute Line Code Violations (LCV) parameter. The default value is 133,400 for an approximate BER level of 10E-5.

» Event Logging — Write security: 3; Read security: 5
Sets the system event severity level threshold for each of the ATLAS 810^{PLUS} system event types. Whenever a system event occurs, that event is logged if the event's severity level is equal to or more severe than the event type's current threshold setting. See *System Event Logging* on page A-1 for detailed information on the system events.

» Syslog Setup — Write security: 3; Read security: 5
Configures the ATLAS Syslog client for use with a Syslog server (supplied on ADTRAN / Utility disk or available on most UNIX platforms).

»» Transmission — Enables or disables the transmission of log events to the external Syslog server.

»» Host IP Address — Lists the IP address of the external server that is running the Syslog host daemon.

»» Host Facility — Specifies the facility destination of log events. Facilities are located on the host and are managed by the Syslog host daemon running on either a UNIX machine or a PC.

» Real Time Clock — Write security: 3; Read security: 5
Provides access to the following two options that you can review and edit:

»» Current Time/Date — Displays the current date and time, including seconds. To edit this field, enter the time in 24-hour format (such as 23:00:00 for 11:00 pm), and enter the date in mm-dd-yyyy format (for example, 09-23-1998).

»» Auto Daylight Savings — When enabled, automatically updates the time and date when Daylight Savings Time starts and, also, when Standard Time starts.

» Access Passwords Write security: 0; Read security: 5
Provides a way to edit passwords and, also, to add new users and passwords. All menu items are protected by passwords of varying security levels. By assigning different passwords to different security levels, the ATLAS system administrator can control which users can 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.

Each of the six password security levels is described in Table 6-1 on page 6-2.

Passwords are case-sensitive.

Instructions for Adding/Deleting Passwords	
To add a new password...	Select the first column **(0)** and press **I**
To delete a password...	select the first column **(0)** and press **D**.

If you lose or forget the ATLAS 810^{PLUS} system administrator password, contact ADTRAN technical support (see inside back cover) for help in resetting the password.

»» Label Write security: 0; Read security: 5
Defines a user name.

»» Password Write security: 0; Read security: 5
Allows you to change the password (the default password is **password**). The current password displays as a series of asterisks (********).

Passwords are case-sensitive.

Instructions for Changing Passwords	
Step	**Action**
1	Select the **Password** field—a new **Password** field displays.
2	Type the new password in the **Enter** field.
3	Type the new password again in the **Confirm** field.

The password can contain up to 12 alphanumeric characters. You can also use spaces and special characters in the password.

»» Access Rights — Write security: 0; Read security: 5
Defines the password level for the corresponding label. You can select from six different password levels (see also Table 6-1 on page 6-2).

»» Active — Write security: 0; Read security: 5
Displays the number of users for each label that are currently logged into the system.

» Licenses — Menus to enable optional ATLAS feature upgrades (Frame Relay, etc.).

»» Feature — Names the ATLAS feature upgrade.

»» License Key — Displays the license key of the feature upgrade.

»» Serial Number — Displays the serial number of the feature upgrade.

»» Lic cnt — Displays the number of instances of the feature that the license provides. This field may not be applicable for a given feature—if it is not, this field is blank.

»» Status — Reflects the status, Permanent or Temporary, of the feature upgrade license key.

» BONDING Config

»» TXINIT Timer (sec) — This option specifies the length of time the originating endpoint attempts to detect the BONDING negotiation pattern from the answering endpoint before deciding the BONDING call has failed.

»» TXFA Timer (sec) — This option specifies the length of time both endpoints attempt to detect the BONDING frame pattern when a call is connected before deciding the BONDING call has failed. When interoperating with other manufacturers' BONDING equipment, it may be necessary to change this time so that it matches TXADD01.

»» TXADD01Timer (sec) — This option specifies the length of time both endpoints wait for the additional calls to be connected at the end of negotiation before deciding the BONDING call has failed. The factory default setting is sufficient for most calls to connect, although when dialing overseas, it may be necessary to lengthen this timer to allow for slower call routing.

»» TXDEQ Timer (sec) — This option specifies the length of time both endpoints attempt to equalize the network delay between the bearer channels before deciding the BONDING call has failed.

»» TANULL Timer (sec) — This option specifies the length of time the answering endpoint attempts to detect the BONDING negotiation pattern from the originating endpoint before aborting the clear channel mode. It may be necessary to shorten this time if the DTE equipment using the BONDING module also has timer constraints for completing non-BONDING parameter negotiation.

»» TCID Timer (sec) — This option specifies the length of time both endpoints attempt to negotiate an agreeable value for bearer channels and channel capacities before deciding the BONDING call has failed.

»» Call Stagger — This option specifies the amount of delay placed between calls. Options include No Stagger, 100 ms, 200 ms, 500 ms, 1 sec, and 2 sec.

» Alarm Relay Reset

Clears the Alarm Relay located on the rear panel of the ATLAS 810^{PLUS}.

» Alarm Relay Threshold

Logs Event Thresholds necessary to set Alarm Relay. These thresholds include Critical, Major, Minor, Warning, and Normal.

> SYSTEM UTILITY

Use the **System Utility** menu to view and set the system parameters shown in Figure 6-4.

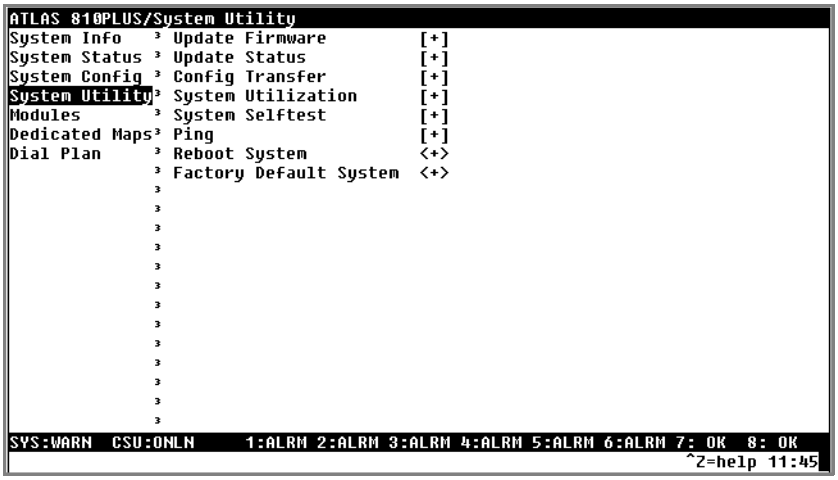


Figure 6-4. System Utility Menu

» Update Firmware

Write security: 1; Read security: 5

Updates firmware when ATLAS 810^{PLUS} enhancements are released. Two transfer methods are available for use in updating any modules that contain Flash memory—including the ATLAS system controller.

The first transfer method uses the ATLAS serial Chain In port of the system controller and XMODEM protocol. For detailed information on how to update firmware using this method, see *XMODEM Firmware Updates* on page 10-1.

The second transfer method uses the ATLAS built-in Ethernet port of the system controller and TFTP (Trivial File Transfer Protocol). For detailed information on how to update firmware using this method, see *TFTP Firmware Updates* on page 10-4.

> **NOTE** *The available update options vary depending on whether you select* **Slot 0**, **Slots 1** *through* **8**, *or* **All Modules of a Type**.

»» Module Slot

Write security: 1; Read security: 5

Displays the slot you selected for firmware updating. When this option first appears, **None Selected** displays. When you move the cursor to this field and press **Enter**, a dialog box opens, allowing you to select **Slot 0** through **Slot 8** or **All Modules of a Type.** (**All Modules of a Type** is useful if several identical modules are installed in the ATLAS 810^{PLUS}).

»» Module Type

Write security: 1; Read security: 5
Reflects the module type selected in **Module Slot**. This is normally a read-only field; however, if you selected **All Modules of a Type**, you must select a particular module type to update all modules of that type. The selections only include upgradable modules.

»» Transfer Method

Write security: 1; Read security: 5
Lists the two transfer methods for updating firmware: XMODEM and TFTP, after selecting a module slot. XMODEM transfers files by connecting to a communications program that supports XMODEM uploads to the terminal interface. TFTP transfers files by specifying an appropriate server address and filename:

TFTP Server IP Address

Write security: 1; Read security: 5
Configures the IP address of the TFTP Server on which the update file resides. ATLAS uses this field to locate the network server on which the update file resides.

TFTP Server Filename

Write security: 1; Read security: 5
Identifies the name of the update file to retrieve from the TFTP Server. Enter the full path name and filename for the file.

»» Restart Schedule

Write security: 1; Read security: 5
Indicates when to restart the updated module to invoke the new code, after selecting a module slot. The two options include **Restart Immediately After Update** and **Restart at Specified Date and Time**:

Restart Immediately After Update

Automatically restarts the module immediately after the update is complete.

Restart at Specified Date and Time

Lets you specify a date and time to automatically restart the updated module. (When you select this option, a new field called **Restart Date and Time** displays below the current field.)

Restart Date and Time

Write security: 1; Read security: 5
Defines the date and time to restart the system.

- Enter the time using a 24-hour format (i.e., 23:00:00 for 11:00 pm).
- Enter the date in mm-dd-yyyy format (i.e., 10-30-1998).

Restart at Specified Date and Time *is only available for the System Controller— not for modules residing in expansion slots, since they are unable to maintain normal operation during the update process.*

»» Current Update Status

Read security: 5
Indicates progress or problems encountered during the current update process. The field displays **Idle** if no update is in progress or when the update is successfully completed. At the end of a successful update, the contents of this field are copied into **Previous Update Status**.

If you are updating several modules at the same time (if **Module Slot** is set to **All Modules of a Type**), this option displays **[+]**, indicating this field contains submenu items. The following submenus display:

Slt — Indicates the slot number.

Type — Defines the type of module for each slot.

Current Status — Indicates the status of the current update.

Previous Status — Indicates the status of the previous update.

Previous Time — Indicates the time of the previous update.

During the TFTP upload process, various status messages are provided in **Current Update Status** (see Table 10-1 on page 10-5).

»» Previous Update Status

Read security: 5
Displays the status of the previous update, after selecting a module slot. If a firmware update has not been attempted for a particular slot, this field reads **Has not been attempted.** Following a successful update, the field reads **Module Update Complete.** If an update was unsuccessful, the appropriate error message displays.

»» Begin Firmware Update

Write security: 1; Read security: 5
Begins updating the firmware for the selected modules. To start this action, enter **Y** to begin or enter **N** to cancel. You can also cancel the operation after the update has begun. For XMODEM updates, cancel the process via the terminal emulation software (consult your documentation for information on how to do this). For TFTP updates, you can cancel the process by selecting **Cancel Update** from this field.

» Update Status

Read security: 5
Displays the status of the current firmware update. These fields are identical to those defined in *Current Update Status* on page 6-18.

» Config Transfer

Write security: 3; Read security: 5
Used only with TFTP transfers. Sends a file containing the ATLAS 810^{PLUS} configuration to a file on a TFTP Server using the TFTP protocol through the 10BaseT Ethernet port. **Config Transfer** also lets you save the ATLAS 810^{PLUS} configuration as a backup file, so you can use the same configuration with multiple ATLAS 810^{PLUS} units. In addition, **Config Transfer** can retrieve a configuration file from a TFTP Server.

To support these transfers, ADTRAN delivers a TFTP program with ATLAS 810^{PLUS} called *TFTP Server*. You can configure any PC running Microsoft Windows with this software, and store a configuration file. See *TFTP Server* on page 12-10 for details on how to use *TFTP Server*.

Before using **Config Transfer**, *the ATLAS 810^{PLUS} should have a valid IP address, subnet mask, and default gateway (if required), and should be connected to an Ethernet network.*

Only one configuration transfer session (upload or download) can be active at a time. The TCP / IP parameters are not saved or overwritten as part of an ATLAS 810^{PLUS} unit's transferred configuration; this way, identical configurations can be sent to multiple units.

»» Transfer Method
Write security: 3; Read security: 5
Displays the method used to transfer the configuration file to or from a server. Currently, you must use TFTP.

»» TFTP Server IP Address
Write security: 3; Read security: 5
Specifies the IP address of the TFTP Server. Get this number from your system administrator.

»» TFTP Server Filename
Write security: 3; Read security: 5
Defines the name of the configuration file that you transfer to or retrieve from the TFTP Server. The default name is **atlas.cfg**, but you can edit this name.

»» Current Transfer Status
Read security: 5
Indicates the current status of the update.

»» Previous Transfer Status
Read security: 5
Indicates the status of the previous update.

»» Load and Use Config
Write security: 3; Read security: 5
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 **Load and Use Config**, *the ATLAS 810^{PLUS} retrieves the configuration file, reboots, then restarts using the new configuration.*

»» Save Config Remotely

Write security: 3; Read security: 5
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 Utilization

Write security: 0; Read security: 0
Displays statistics related to the ATLAS internal operating system. Please check with ADTRAN Technical Support before attempting to use this menu.

» System Selftest

Write security: 3; Read security: 5
Initiates a system self-test. The self-test consists of memory tests and data integrity tests for each installed module.

Self-tests disrupt data flow.

»» Selftest Run

Write security: 3; Read security: 5
Runs system-wide selftest, Memory, Flash, Bootrom, and Port Tests. These tests are disruptive to all data traffic; therefore, do not run these tests on a unit unless data interruptions are acceptable. To confirm self-test activation, press **Y**; to cancel the self-test press **N**.

»» Current Test Status

Security level: 3; Read security 5
Indicates a system self-test. The self-test consists of memory tests and data integrity tests for each installed module.

»» Current Slot/Port

Displays slot and port of the subsystem currently being tested.

»» View Selftest Log

Read security: 5

Displays time-stamped log of the tests conducted and the Pass / Fail results. Self-tests verify data integrity and processor control to each port. Each port is looped back and a data pattern is sent and tested.

The result of the self-test on each installed port is listed with Pass / Fail results. A typical test log is shown in Figure 6-5 on page 6-21. The log includes the following additional fields.:

Idx	Index number of the log.
Time	Time and date of the log entry.
Sl	ATLAS slot number.
Pt	ATLAS port number.
Event	Event description.
Result	Shows Pass / Fail results.

The tests associated with the system controller include the following:

This event...	Logs this result...
Flash	Flash memory checksum verified.
BootRom	Boot ROM checksum verified.
DSP RAM	Memory associated with the DTMF DSP.
RTC RAM	Memory associated with the real time clock.
TDM RAM	Memory associated with mapping TDM bandwidth.
DRAM	Dynamic RAM used for program execution.

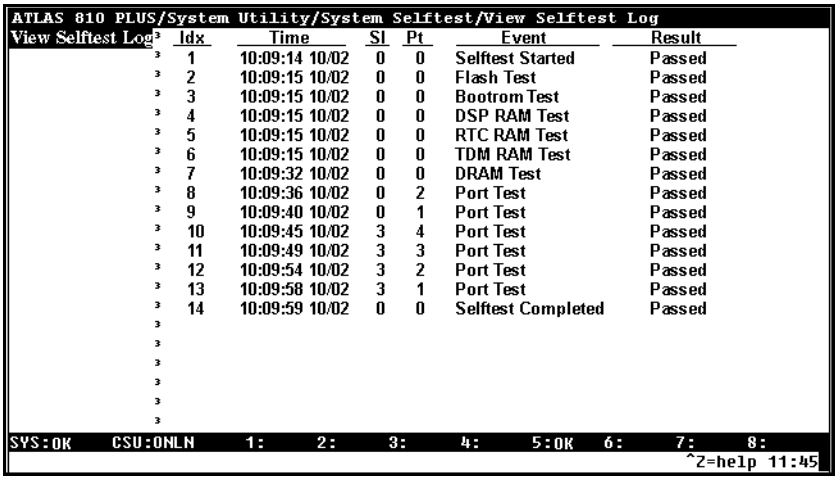


Figure 6-5. View Self-test Log

»» Clear Self-test Log
Write security: 3; Read security: 5
Clears the self-test log.

» Ping
Write security: 5; Read security: 5
Allows you to send pings (ICMP requests) to devices accessible via the network.

Only one ping session can be active at a time.

»» IP Address
Write security: 5; Read security: 5
Specifies the IP address to ping.

»» Count
Write security: 5; Read security: 5
Specifies the number of pings to send. The default number of tries is 4, and the maximum value is 99.

»» Size
Write security: 5; Read security: 5
Specifies the size in bytes of the data portion of the ping request. The default value is 64 bytes, and the maximum size is 1024 bytes.

»» Timeout
Write security: 5; Read security: 5
Specifies the time in milliseconds to wait for the ping reply before timing out. The default timeout is three seconds, and the maximum timeout value is ten seconds.

»» Round trip min
Read security: 5
Displays the minimum round trip time of the ping request / reply of the current set of pings.

»» Round trip avg
Read security: 5
Displays the average round trip time of the ping request / reply of the current set of pings.

»» Round trip max
Read security: 5
Displays the maximum round trip time of the ping request / reply of the current set of pings.

»» Tx Stats
Read security: 5
Displays the number of ping requests transmitted (**n txed**), the number of ping replies received (**n rxed**) and the number of ping requests that were lost (**n lost**).

»» Reset Stats
Write security: 5; Read security: 5
Resets all ping statistics to zero. If the ping client is active, this menu will stop it.

»» Start/Stop

Write security: 5; Read security: 5
If the ping client is currently idle, this menu sends pings to the specified address. If the ping client is active, the menu stops sending pings.

» Reboot System

Write security: 2; Read security: 5
Reboots the ATLAS 810^{PLUS}. When you select this command, the following message displays: ****WARNING ** This will reboot the entire system!** Press **y** to reboot the system, or **n** to exit the command.

» Factory Default System

Write security: 0; Read security: 0
Resets the entire system to the factory default settings. To reset the system, press **y**; to cancel this command, press **n**.

Chapter 7 Modules Terminal Menu

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

> MENUS
» Submenus
»» Sub-submenus
Submenu Options

> MODULES

Write security:3; Read security:5
The **Modules** menu provides options that allow you to configure and control the installed option modules as well as the controller T1/PRI ports. Figure 7-1 shows the **Modules** menu.

```
ATLAS 810PLUS/Modules
System Info    ³ Slt   Type    Menu    Alarm    Test   State     Status       Rev
System Status  ³  0  Sys Ctrl  [+]     [OK]     [OFF]  ONLINE  Online          A
System Config  ³  1  T1/PRI    [+]     [n/a]    [n/a]  ONLINE  No Response     -
System Utility ³  2  HDLC-128  [+]      n/a      n/a   ONLINE  No Response     -
Modules        ³  3  U-BRI     [+]     [n/a]    [n/a]  ONLINE  No Response     -
Dedicated Maps ³  4  ASYNC232  [+]     [n/a]    [n/a]  ONLINE  No Response     -
Dial Plan      ³  5  T3        [+]     [n/a]    [n/a]  ONLINE  No Response     -
               ³  6  T3 D&I     [+]     [n/a]    [n/a]  ONLINE  No Response     -
               ³  7  AUX PS                              ONLINE  Online          -
               ³  8  AUX PS                              ONLINE  Online          -
               ³
               ³
               ³
               ³
               ³
               ³
               ³
               ³
               ³
               ³
               ³
SYS:WARN  CSU:ONLN     1:ALRM 2:ALRM 3:ALRM 4:ALRM 5:ALRM 6:ALRM 7: OK  8: OK
Access module menus                                              ^Z=help 11:45
```

Figure 7-1. Modules Menu

The controller board (slot 0) has two T1/PRI interface ports. This section only describes the module options available for the T1/PRI interface ports. Individual module choices are described in the applicable module manuals. The ATLAS system controller automatically detects the presence of modules when they are installed in the system. To view the menus for the installed modules via the terminal menu, use the **arrow keys** to scroll to the appropriate menu and press **Enter.** You can then access the module choices.

» Slt

Write security:3; Read security:5

Identifies the slot number. Slot 0 refers to the ATLAS 810^{PLUS} Base Unit.

» Type

Write security:3; Read security:5

Displays the type of module actually installed in the slot or the type of module you plan to install in the slot. The ATLAS 810^{PLUS} automatically detects the type of module installed in each slot, and the **Type** field automatically defaults to the installed module type. You can also use this field to pre-configure a unit before actually installing modules by specifying the module that you want to install in each slot.

To use this option, navigate to the field you want to edit and press **Enter**. For empty slots, a list of all the available module types displays. Select the one you want and it displays in the **Type** field. If this field is already configured with a module, you can only set this field to **Empty**.

If you install a module in a slot, then want to install a different type of module in the slot, you must set this field to **Empty** *before selecting another module type.*

If a module is installed, the module type automatically shows the name of the installed module, and it cannot be set to any other option.

» Menu

Displays additional status and configuration menus for the selected module. To access the submenus for this item, use the **arrow keys** to scroll to the **Menu** column for the module you want to edit, and press **Enter**. For detailed information on each submenu item, see *Modules Menu (Quad T1/PRI)* on page 7-4.

» Alarm

Read security:5

Displays whether there is an alarm condition on the ATLAS 810^{PLUS} Base Unit. Press **Enter** to access the **Alarm** menu.

» Test

Read security:5

Displays whether the ATLAS 810^{PLUS} is executing a test. To initiate a test, choose the **Menu** submenu on this screen. Then, select the **Test** option to access the screen that allows you to set up and initiate tests. See *Test* on page 7-2 for details. Press **Enter** to access the **Test** menu.

» State

Read security:5

Displays whether the module is online of offline. Even though a module is physically installed, it must be marked **Online** for it to be considered an available resource. This parameter allows an installed module to be marked **Offline**, which may be useful in system troubleshooting. If you choose **Offline**, the module will not be in alarm condition, but will display **Offline**.

Once a module is installed, the state must be set to Online in order for the ATLAS to utilize the module for any data bandwidth.

» Status

Read security:5

Displays status information on the ATLAS 810^{PLUS} T1/PRI ports and other installed modules as follows:

Online	The module is enabled and is responding to the system controller's status polls. This is the normal response of the system.
No Response	The module is enabled but is not responding to the system controller's status polls. This response indicates a problem in the system or that the module is not installed.
Empty	The system controller has not detected the presence of a module in the system, nor has a module been manually enabled for this option slot.
Offline	The module is installed but has been taken Offline by a user. The module is still responding to controller polls.
Offline/No Response:	The module is installed but has been taken Offline by a user. The module is not responding to polls.
Not Supported	The module is not supported by the current system configuration.

» Rev

Read security:5

Displays the hardware revision of the ATLAS 810^{PLUS}.

Modules Menu (Quad T1/PRI)

This section provides detailed information on the **Modules** / **Menu** submenus. **Menu** provides access to commands that allow you to review the status of various options, change the configuration for general parameters, and initiate tests. This section *only* describes the menu options for the Quad T1/PRI controller port (the ATLAS 810^{PLUS} Base Unit). For details on menu options for individual modules, refer to the appropriate module manuals.

»» Controller Info — Read security:5
Displays general information about the ATLAS 810^{PLUS} Base Unit and Quad T1/PRI ports as follows:

- Part Num — Displays the part number of the ATLAS 810^{PLUS}.
- PLL Status — (Phase Lock Loop) Indicates whether the clock is locked to its specific source.

»» Alarm Status — Read security:5
Displays any active alarms as follows:

- Prt — Port number displayed.
- Alarms — Displays alarm type. Table 7-1 describes each alarm type.

Table 7-1. Alarm Types

LOS	(Loss of Signal) No signal detected on port interface.
RED	(Red Alarm) Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF).
YELLOW	(Yellow Alarm) Remote alarm indicator (RAI) being received on port.
BLUE	(Blue Alarm) Receiving unframed all ones from the port alarm indicator signal (AIS).
DS0 ALARM	HDLC framing is operational on PRI D channel. This indication only applies when operating in PRI mode.
RX LEVEL	(Receive Level) Indicates the strength of the signal received on the port.

»» DS0 Status

Read security:5
Indicates usage on a DS0 basis for each port as follows.

*	Inactive
A	Active call on this DS0
D	Active D channel DS0
M	Maintenance DS0
N	Dedicated DS0
O	Off hook detected
R	Ringing detected

»» DS0 Alarms

Indicates DS0 alarm as follows:

-	No alarm DS0
D	D channel alarm (ISDN)
F	Frame alarm (Packet)
T	TBOP alarm (Packet)

»» Sig Status

Read security:5
Indicates signaling of all 24 DS0s. The A/B bits for Rx and Tx DS0s are shown for each port.

»» Performance: Curr

Write security:4; Read security:5
The performance fields – either current, 15 minute total, or 24 hour total – provide status on key performance measures as specified in ANSI T1.403 and AT&T TR54016 for each of the four T1/PRI ports as follows:

Prt	Displays the port number.
CLR	Clears information for the selected port. Press **Enter** when the cursor is over this field to clear the data.
ES	Errored Seconds. An ES is a second with one or more error events *or* one or more Out Of Frame events *or* one or more Controlled Slips.
BES	Bursty Errored Seconds. A BES is a second with more than one, but less than 320 error events.
SES	Severely Errored Seconds. An SES is a second with 320 or more error events *or* one or more Out Of Frame events.
SEFS	Severely Errored Frame Seconds.
LOFC	Loss of Frame Count.
CSS	Controlled Slip Seconds.
UAS	Unavailable Seconds.

LCV	Line Code Violations.
PCV	Path Code Violations.
LES	Line Errored Seconds.
»» Performance: 15 Min	Write security:3; Read security:5 In the Performance 15 min. menu, the performance data for the previous 15 minute window is stored. Refer to *Performance: Curr* on page 7-5 for a detailed description.
»» Performance: 24 Hr.	Write security:3; Read security:5 In the Performance 24 hr. menu, the performance data for the previous 24 hour window is stored. Refer to *Performance: Curr* on page 7-5 for a detailed description.
»» Configuration	All of these configurable parameters depend on whether the port is connected to a Primary Rate ISDN circuit or a Channelized T1 circuit—dedicated or switched.
Prt	Read security:5 Identifies the port number.
Port Name	Write security:3; Read security:5 Accepts any alphanumeric name up to 16 characters long to uniquely identify each port.
Frame	Write security:2; Read security:5 Matches the frame format of the circuit to which it is connected (available from the network supplier).
Code	Write security:2; Read security:5 Matches the line code of the circuit to which it is connected (available from the network supplier).
Tx Yellow	Write security:3; Read security:5 (Auto Tx Yellow Alarm) Enables and disables the transmitting of yellow alarms.
Tx PRMs	Write security:3; Read security:5 (Transmit PRMs) Enables and disables the sending of PRM data on the facility data link (FDL). The PRM data continues to be collected even if Tx PRM is disabled (possible only with ESF format).
LBO	Write security:2; Read security:5 (Line Build Out) Depends on whether the circuit is provisioned for DS1 by the telephone company.
LB Accept	Write security:3; Read security:5 (Loopback Accept) Sets unit to accept or reject the in-band loop up and loop down codes as defined in ANSI T1.403. This is a line loopback.

»» Test — Initiates different types of tests and displays test results.

These **Test** *commands temporarily disrupt service.*

Prt — Identifies the port number.

Loc LB — Read security:5
(Local Loopback) Causes loopback on near-end port.

Line	Metallic loopback
Payld	Payload loopback framing and clocking are regenerated.

Remote LB — Write security:4; Read security:5
(Remote Loopback) Sends a loopback code to a remote CSU.

ANSI FDL Line	Requires ESF mode.
ANSI FDL Pyld	Requires ESF mode.
AT1 Inband l	

Pattern — Write security:4; Read security:5
Specifies the test pattern to be transmitted out the port.

ALL ONES	Framed ones
ALL ZEROS	Framed zeros
QRSS	2 20-1 pseudorandom pattern with suppression of excess zeros

QRSS/RLB Results — Read security:5
(Remote Test Pattern Results) Suppresses excess zeros—indication of sync and errors of received data pattern.

Clr — Write security:4; Read security:5
(Test Pattern Results Clear) Clears current error counters on test pattern results menu.

Inj — Write security:3; Read security:5
(Test Pattern Error Inject) Injects errors into transmitted test pattern.

Chapter 8

Dedicated Maps Terminal Menu

OVERVIEW

The **Dedicated Maps** menu assigns dedicated connections between any two ports in the ATLAS 810^{PLUS} Base Unit. This chapter describes the **Dedicated Maps** menu items (see Figure 8-1). In addition, step-by-step instructions are provided for setting up a sample dedicated map (see *Creating A Dedicated Map* on page 8-6).

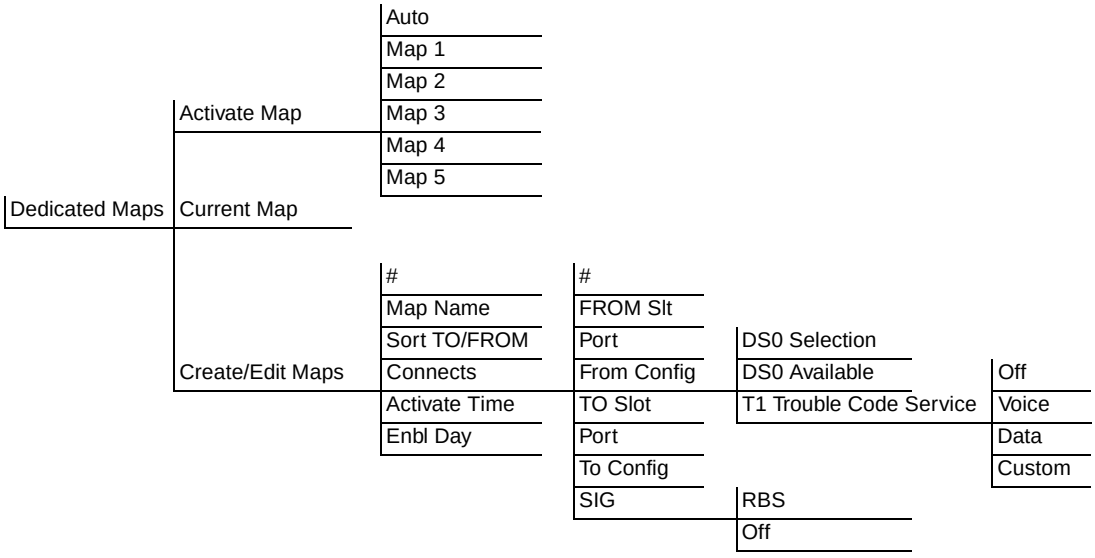


Figure 8-1. Dedicated Maps Menu Tree

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

> **MENUS**
» Submenus
»» Sub-submenus

> ACTIVATE MAP

Write security:3; Read security:5
Activates a dedicated map—automatically or manually. You can have up to five different dedicated maps, each with an optionally specified name.

» Auto

Automatically activates a particular dedicated map at the time and day specified in **Activate Time** (see *Activate Time* on page 8-5).

» Maps 1—5

Lets you manually activate a specific dedicated map.

Instructions for Manually Activating a Dedicated Map	
Step	**Action**
1	Move the arrow keys to highlight the **Activate Map** field and press **Enter**.
2	Move the arrow key to highlight the map of choice from the pop-up menu list and press **Enter**.

> CURRENT MAP

Read security:5
Displays the name of the currently active dedicated map (read only).

> CREATE / EDIT MAPS

Creates new maps and defines settings, as well as edits existing maps. To add a new map, position the cursor in the index column and press **I**. ATLAS automatically names the maps in the sequence in which they are created. You can change the names with **Map Name**.

»

Index number of the available maps.

» Map Name

Write security:3; Read security:5
Displays the name of the dedicated map. The name can contain up to 57 alphanumeric characters, including spaces and special characters. To edit the name, press **Enter** and type in the new name.

» Sort TO/FROM

Write security:3; Read security:5
Specifies sort order based on the end points set in **Connects/From Config** and **Connects/To Config**. You can also turn **Off** this option. This sort feature is helpful when you are attempting to find a particular connection in a large connection list.

» Connects

Enters the dedicated map connections. Press **Enter** to activate the submenus.

Some of the options available in this submenu change depending on the type of modules selected in the FROM or TO fields.

»» #

(Index Number) Displays the number of the dedicated map connection. If you press **I** in this field, ATLAS 810^{PLUS} adds another dedicated map connection, numbered consecutively.

»» FROM Slt

Write security:3; Read security:5
(From Slot) Specifies the slot to use for the **FROM** connection. When you select this option, a list of all of the slots and the modules installed in the slots displays. Pick the appropriate slot and press **Enter**.

»» Port

Write security:3; Read security:5
Specifies the port to use for the **FROM** connection. When you select this option, a list of ports and module types appears. Pick the appropriate port and module type, and press **Enter**.

»» From Config

Write security:3; Read security:5
Specifies the configuration for the **FROM** connection. The selections displayed in this field are based on the type of module selected in the **FROM Slt** option. You must input the following information—based on the module type.

DS0 Selection

Write security:3; Read security:5
Defines DS0s for a T1 port. Use this field to define which DS0s will be used for this connection. You can enter the DS0s in several ways. For example, to enter DS0s one through five, enter **1-5**. For DS0s one and five, enter **1,5**.

DS0 Available

Read security:5
Indicates which DS0s of the T1 are assigned. DS0 assignment is based on the following items:

digits 0—9	This DS0 is available. The digit that displays in this field represents the last digit of the DS0 number.
*	This port is requesting this DS0 for this connection, but the DS0 is not yet activated.
!	This DS0 is used by this port in this connection and is activated.
s	This DS0 is used in the switched Dial Plan.
S	This DS0 is used in the switched Dial Plan and conflicts with this connection.
n	This DS0 is already used in this dedicated map.
N	This DS0 is already used in this dedicated map and conflicts with this connection.

Data Rate

Write security:3; Read security:5
Defines the data rate per DS0. If **FROM Slt** is an Nx port, the data rate per DS0 must be set. You can choose from 64 kbps or 56 kbps.

Trunk Conditioning

Write security: 3; Read security: 5
Sets known values in the signaling bits and the data field for outgoing DS0s which are cross-connected to a T1 port experiencing alarms. The trunk conditioning process consists of a 2.5-second transmission (indicating call termination), followed by a continuous transmission signaling the final condition as chosen by the user.

> **NOTE** *Trunk conditioning only applies to RBS T1s in the dedicated map.*

Fault Signaling

Defines to ATLAS the type of signaling being used on the trunk: E&M, LS / GS Network or User, SW56, or Custom.

> **NOTE** *Fault signaling is only visible when RBS is turned on.*

Fault State — Defines the final fault signaling state:

- Idle — Used for one-way trunks; that is, for outgoing *or* incoming calls only—not both.
- Seized — Used for two-way trunks. Prevents the PBX from attempting to use a failed trunk for an outgoing call.

Custom — Permits users to define the fault signaling to use in the form of A / B set to 1 / 0.

> **NOTE** *See also the trunk conditioning example on page 8-5.*

»» TO Slot

Write security: 3; Read security: 5
Specifies the slot to use for the second end of a connection. Select this option, and a list of all of the slots and the modules installed in the slots displays. Pick the appropriate slot.

»» Port

Write security: 3; Read security: 5
Selects the port used for the second connection. When you select this option, a list of all the slots and available modules displays. Select the appropriate slot.

»» To Config

Write security: 3; Read security: 5
Specifies the configuration for the **To** connection. The selections that display in this field are based on the type of module selected in the **TO Slot** option. You must input the following information (based on the type). The same options for setting DS0s are available for this command as with the **FROM Config** option.

»» SIG

Write security: 3; Read security: 5
(Signaling) Defines whether the connection has active RBS. Where RBS is not an option, the ATLAS 810^{PLUS} automatically assigns the correct setting. For example, a T1-to-Nx connection is set to **Off**.

RBS	Preserves the signaling bits between the connections.
Off	Ignores signaling bits.

» Activate Time

Write security: 3; Read security: 5
Sets the time when the map becomes active if you have selected **Auto** in the **Activate Map** field (see *Activate Map* on page 8-2). Enter this time in hh:mm:ss 24-hour format.

» Enbl Day

Write security: 3; Read security: 5
Specifies which days of the week the map is active.

Example 1 Setting Trunk Conditioning

The trunk conditioning process sets known values in the signaling bits and the data bits for outgoing DS0s which are cross-connected to a T1 port experiencing alarms. The trunk conditioning process consists of a 2.5-sec transmission (indicating call termination), followed by a continuous transmission (signaling the final condition as chosen by the User).

Use the trunk conditioning menu items **Fault Signaling** (to set the state of the signaling bits) and **Fault Data Code** (to set the state of the data bits) for this process. You can set trunk conditioning for each end of each T1-to-T1 connection in a dedicated map. To simplify this procedure, use the copy command (press **C**). Connections to the Network and connections to User equipment (PBX) contain different signaling bit states.

For this example, assume voice traffic is received on T1-A, and T1-B is groomed onto T1-C to the PBX (see Figure 8-2). If T1-A fails, the DS0s which were cross-connected to T1-C will receive trunk conditioning.

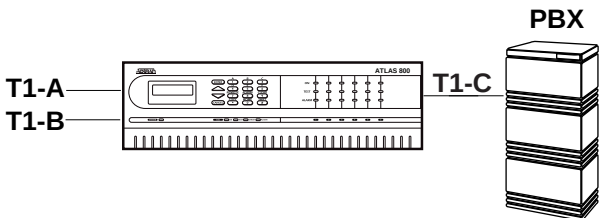


Figure 8-2. Trunk Conditioning

Example 2 Creating A Dedicated Map

A dedicated map defines connections for dedicated bandwidth between ports, and grooms and cross-connects bandwidth between T1 ports. Any ATLAS port supporting dedicated bandwidth can be mapped to any other port supporting dedicated bandwidth (see the example in Figure 8-3).

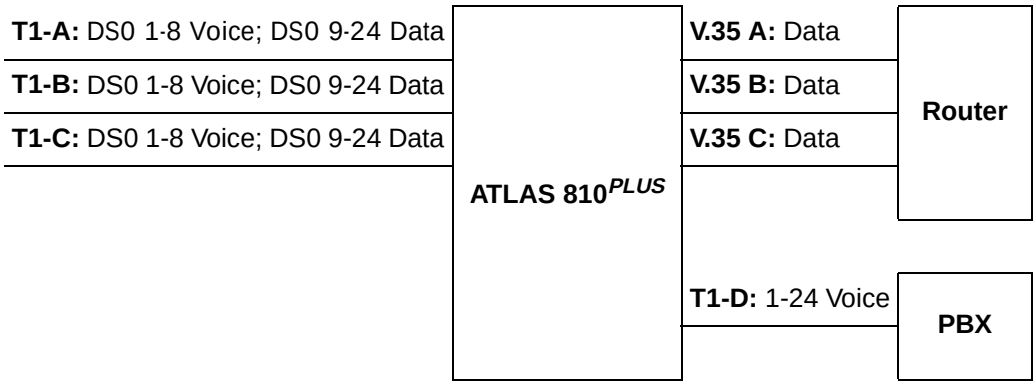


Figure 8-3. Dedicated Map Overview Example

The example shown in Figure 8-3 contains three T1s (T1-A, T1-B, T1-C) supporting dedicated bandwidth from three remote sites. Each T1 includes DS0s for data and voice. At the central site (ATLAS), each incoming DS0 carrying data is mapped to a separate V.35 port and connected to the router. DS0s carrying voice are collected together (groomed) and sent to the PBX over a single T1 (T1-D).

Designing the Dedicated Map for Example 2

In designing a dedicated map, you must first determine what connections to make and which ports to involve. (For T1 ports, you must also decide which DS0s to use). Then, you must configure the ports. Finally, you must define the appropriate connections. The remainder of this chapter provides step-

by-step procedures for creating a sample dedicated map based on the connections and ports given in Table 8-1.

Table 8-1. Connections and Ports

Name	ATLAS 810*PLUS* Port	DS0s	Name	ATLAS 810*PLUS* Port	DS0s
T1: Data A	Controller T1 Slot 0 Port 1	9-24 RBS Off	V.35 - A	Quad V.35 Slot 2/Port 1	N/A
T1: Data B	Controller T1 Slot 0/Port 2	9-24 RBS Off	V.35 - B	Quad V.35 Slot 2/Port 2	N/A
T1: Data C	Quad T1/PRI Slot 1/Port 1	9-24 RBS Off	V.35 - C	Quad V.35 Slot 2/Port 3	N/A
T1: Voice A	Controller T1 Slot 0/Port 1	1-8 RBS On	T1-D	Quad T1/PRI DSX Slot 1/Port 2	1-8 RBS On
T1: Voice B	Controller T1 Slot 0/Port 2	1-8 RBS On	T1-D	Quad T1/PRI DSX Slot 1/Port 2	9-16 RBS On
T1: Voice C	Quad T1/PRI Slot 1/Port 1	1-8 RBS On	T1-D	Quad/PRI DSX Slot 1/Port 2	17-24 RBS On

Configuring the Ports for Example 2

Begin by navigating to **Terminal Menu/Modules**. From this menu, configure the various ports to match the framing parameters of the T1 line provided by the telco.

Instructions for Configuring the Ports	
Step	**Action**
1	Select **Slt / 0** (system controller T1/PRI port).
2	Set the line framing parameters by selecting **Menu / Configuration / Frame / ESF**.
3	Copy this configuration information for use with additional ports. (Navigate to **Prt** and press **C**.)
4	Navigate to the port index number of the second port (**Prt**) and press **P** to paste the configuration information. Press **Y** to confirm paste.
5	Repeat Step 4 for the first port of the T1/PRI card located in Slot 1.
6	Navigate to the V.35 port **Configuration** submenu and repeat Step 2 for the first port, followed by a copy-and-paste to the second and third ports (see Figure 8-4).

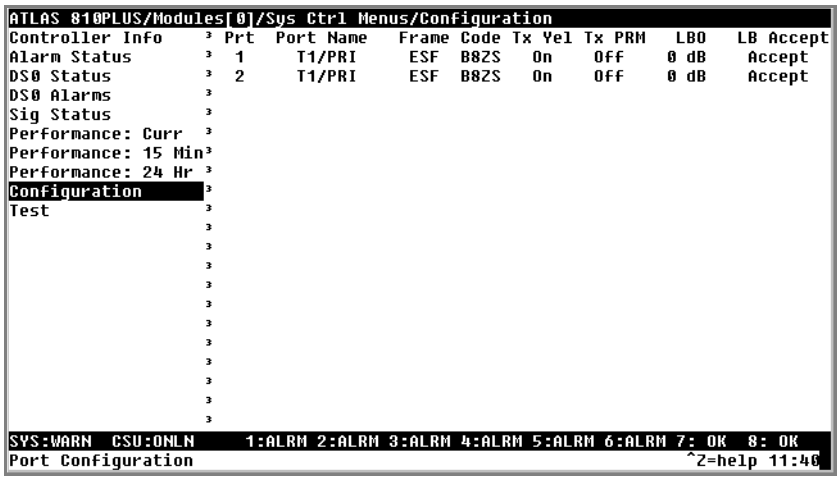


Figure 8-4. Slot 0 Module Configuration Menu

Defining the Connections for Example 2

Begin by navigating to **Dedicated Maps/Create/Edit Maps** and naming your map. Navigate to **Dedicated Maps/Connects**. The **Connects** sub-menu defines the connections necessary to route the required bandwidth. Refer to Table 8-1 on page 8-7 to define each of the necessary connections. For this procedure, first define the data connections, and then define the voice connections. The following Step / Action tables guide you through this process. (Figure 8-5 shows the completed map.)

Instructions for Defining Data Connections	
Step	**Action**
1	For Data A, select and define **FROM Slot** (i.e., **0 Sys Ctrl**).
2	Select and define "from" **Port** (i.e., port **1** for T1: Data A).
3	Select and define **From Config** DS0s (i.e., **DS0=9-24**).
4	Select and define **TO Slot** and “to” **Port** in the same way (i.e., **2 V.35Nx4** and **1** where 2 = Slot 2 and 1 = Port 1.)
5	From **To Config**, set **V.35** to operate at **56k/64k** per DS0.
6	Repeat for the remaining data connections (i.e., Data B and Data C) as follows:
6a	Insert new connection lines by positioning the cursor over the index # of the first connection and pressing **I**.
6b	Copy the first connection by positioning the cursor on the index # and pressing **C**.

Instructions for Defining Data Connections (Continued)	
Step	**Action**
6c	Paste this information onto a new connection line by positioning the cursor over the index numbers of the new connections, and pressing **P**.
7	Modify these connection lines to complete the connections for data.

Instructions for Defining Voice Connections	
Step	**Action**
1	Select the **FROM Slot** and **Port** for the first voice connection (i.e., Slot 0/Port 1 for T1-A Voice).
2	Select the voice DS0s; i.e., 1 through 8 for Voice A.
3	Select the **TO Slot** and **Port** (PBX Connection); i.e., Quad T1/PRI in Slot 1/Port 2.
4	From **Configuration**, set the starting DS0 that these voice DS0s will appear in; i.e., 1 for Voice A; 9 for Voice B; 17 for Voice C. (This action sets the DACSing between the T1s.)
5	Set **RBS** to **On** for the voice connections.
6	(Optional) From **Configuration**, set the trunk conditioning (Signaling and Data code) for T1 failure.
7	Repeat for the remaining voice connections.

A connection is not actually "made" (connected) until the cursor leaves the connection. The cursor leaves the connection when you press ESC to move the cursor to the index # or when you move the cursor onto another connection line.

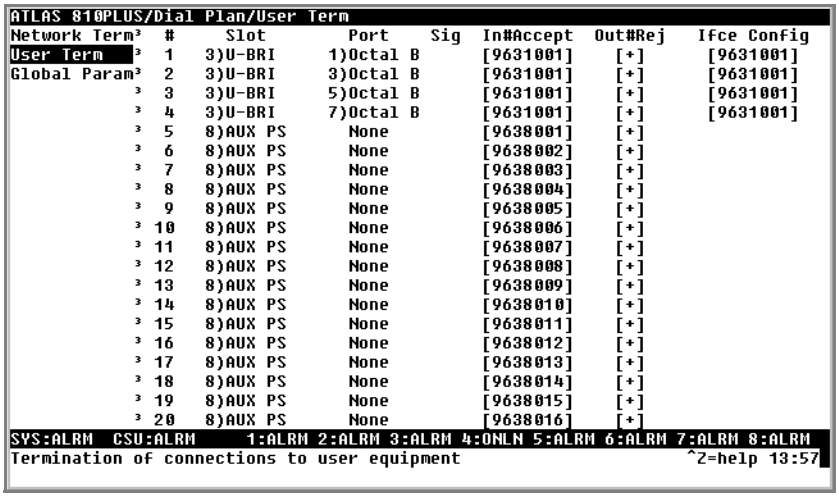


Figure 8-5. Completed Dedicated Map

Chapter 9 Dial Plan Terminal Menu

OVERVIEW

The **Dial Plan** submenus (see Figure 9-1) set global ATLAS switch parameters as well as individual parameters for each ATLAS port handling a switched call. The individual ports are separated into two port types: network and user. Network ports terminate a connection from the Network. User ports terminate incoming calls and, in turn may be connected to user equipment. *Network Term* on page 9-3 and *User Term* on page 9-5 provide clarification for these two port types. (See also Figure 9-2 for the complete menu structure.)

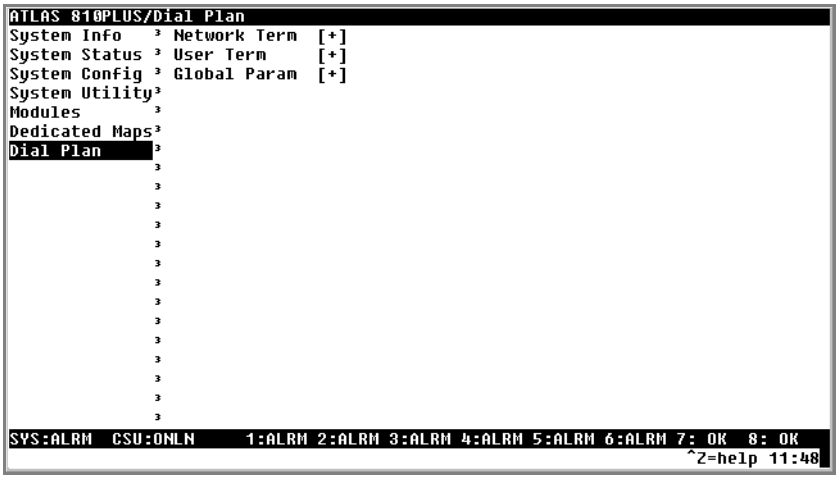


Figure 9-1. Dial Plan Menu

NOTE

In the menus described in the following sections, **Incoming Calls** *refer to calls coming to ATLAS from the Network (PSTN) and* **Outgoing Calls** *refer to calls directed toward the Network (PSTN).*

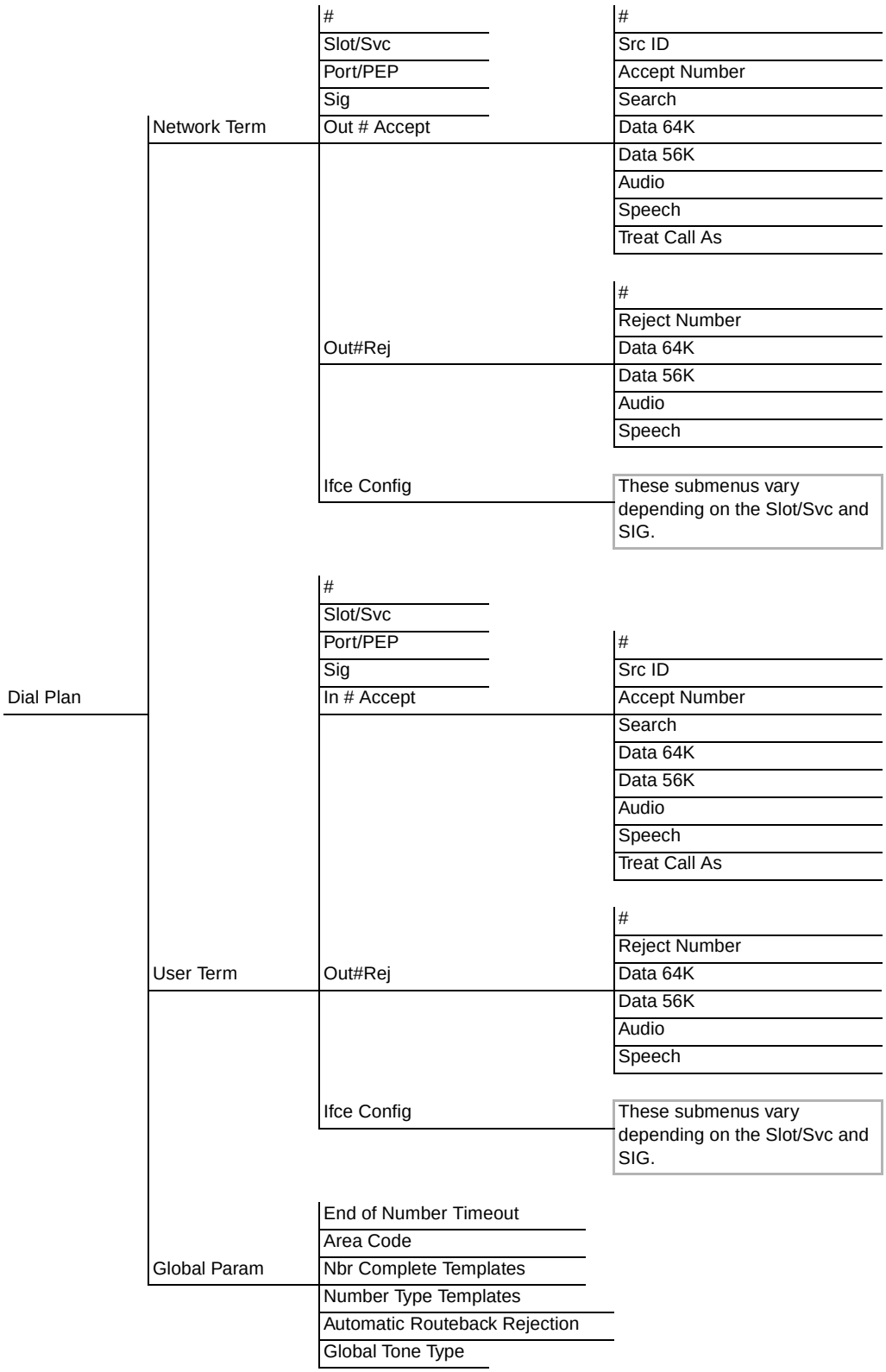


Figure 9-2. Dial Plan Menu Tree

> NETWORK TERM

This menu allows the user to define option parameters for ports which terminate a connection from the Network (PSTN).

> **NOTE** *In applications where two ATLAS units are used in a point-to-point configuration, a port in the ATLAS at one end would act as the Network (User termination), while the ATLAS at the opposite end would be terminating a "Network" connection.*

» Slot/Svc

Write security: 3; Read security: 5
Selects the ATLAS slot that terminates a Network connection.

» Port/PEP

Write security: 3; Read security: 5
Selects the ATLAS port that terminates a Network connection.

> **NOTE** *There may be more than one "endpoint" associated with a particular port. If a T1 is connected to the PSTN, some DS0s may be used for long distance, while others are used for local calls. These would constitute two "endpoints" (trunks) over a single physical port.*

» Sig

Write security: 3; Read security: 5
Defines the type of signaling being used for this connection (endpoint). Select **RBS** for a T1 using Robbed Bit Signaling, **PRI** for a Primary Rate ISDN interface, and **NFAS** for a Primary Rate ISDN interface using Non-Facility Associated Signaling. This selection is only necessary if a T1/PRI is selected as the Slot/Port type.

» Out#Accept

Write security: 3; Read security: 5
Defines the parameters for the outgoing calls that ATLAS sends to the Network.

»» Src ID

Write Security: 3 Read Security: 5
Identifies the call source ID from which this endpoint accepts calls. This field simplifies the creation of a Dial Plan in applications where the criterion for switching calls to a certain endpoint is a function of which endpoint originated the call. Source ID may be entered with the usual wild card entries (except $).

X = any digit 0—9
[1,3,5] = any of these digits

Default value = 0. The default ID for all source endpoints is 0 and all accept #'s is 0. This results in all calls being routed based on the dialed number.

»» Accept Number

Designates which numbers this endpoint passes on toward the Network (PSTN). The accept list may consist of multiple entries. The numbers are defined using the following "wild cards":

X = Any single digit
N = Any single digit 2—9
$ = Any number of digits of any value
9 = This specific number
[1,2,3...] = A single digit in this group

For example, 1-800-$ only permits toll free long distance calls to 1-800. If this were used, then a second accept # would need to be specified (NXX-XXXX) permitting local numbers to be dialed.

Any specific entry takes precedence over a wild card. For example, if endpoint "A" was designated as $ while endpoint "B" accepted 963-800X, then an incoming call to 963-800X would only be accepted by endpoint "B."

»» Search

Write Security: 3 Read Security: 5
Instructs ATLAS in which order to search for an accept number match. Normally, all searches are set to primary. The secondary search selection forces ATLAS to only accept a call at this endpoint if all primary endpoints are unavailable.

Primary Search

All long distance calls should go out a PRI directly to an IXC (MCI, ATT, etc.), and local calls should go out a T1 to the LEC. It may be desirable to place long distance calls on the local exchange if all of the IXC trunks are unavailable (busy or in alarm). In this case, the primary accept number for the local exchange would be N$, and the secondary accept would be 1$.

Secondary Search

The same accept rules apply for all secondary number searches as for primary searches.

»» Data 64K, Data 56K, Audio, Speech

Reflects the bearer capability the Network has provisioned for this line. If the ISDN lines were purchased with different services provisioned, then ATLAS would send the call out of the port which supports the type of service the call requires.

For example, the Network termination is on a pair of BRIs (with the same phone number) with one provisioned for data and the other for voice. By enabling data in one and not the other, ATLAS ensures that calls bearing data will be sent out the right BRI interface.

»» Treat Call As

Allows the incoming call t be treated as the selected call type, regardless of the actual incoming call type. The default selection **As Received** effectively disables the feature by using the actual call type.

» Out#Rej

Write security: 3; Read security: 5
Defines the parameters for the outgoing calls that ATLAS will not send to the Network.

»» Reject Number

Identifies which numbers this endpoint will not pass on toward the Network (PSTN). The reject list may consist of multiple entries. The reject list may be used to more easily specify the call filtering desired. The "wild cards" are identical as in **Outgoing Call Accept**.

The Reject list takes precedence over the Accept list. For example, 1-900-$ rejects all 1-900 long distance calls, and 1-$ rejects all long distance calls.

»» Data 64K, Data 56K, Audio, and Speech

Rejects outgoing calls based on call type. For example, setting the reject number to $, Digital 56/64 to enabled, and Audio and Speech to disabled, rejects all digital calls while not rejecting analog calls.

This list may remain blank if the Accept list meets desired filtering.

» Ifce Config

Sets configuration parameters for the endpoint. These parameters vary by the type of port selected. For detailed information on the interface configuration, refer to *Interface Configurations* on page 9-10.

> USER TERM

This menu allows you to define option parameters for ports which terminate a connection from user equipment. In this case, ATLAS 810^{PLUS} is acting as the Network.

In applications where two ATLAS units are used in a point-to-point configuration, a port in the ATLAS at one end acts as the Network (set up as a User termination), while the ATLAS at the opposite end terminates a Network connection.

» Slot/Svc, Port/PEP

Write security: 3; Read security: 5
Selects the ATLAS slot and port that terminate a User connection. (The user selects from a list of option modules/ports.)

More than one endpoint may be associated with a particular port. If a T1 port is connected to a channel bank with analog voice cards, each DS0 or a group of DS0s may have a different phone number. These numbers constitute multiple endpoints over a single physical port.

» Sig

Write security: 3; Read security: 5
(User Selection - RBS; PRI) Defines the type of signaling being used for this connection (endpoint). Select **RBS** for a T1 using Robbed Bit Signaling, **NFAS** for a Primary Rate ISDN interface using Non-Facility Associated Signaling, and **PRI** for a Primary Rate ISDN interface. This selection is only necessary if a T1 / PRI is selected as the Slot / Port type.

» In#Accept

Write security: 3; Read security: 5
Defines the parameters for incoming calls that ATLAS 810^{PLUS} accepts from the Network.

»» Src ID

Write Security: 3 Read Security: 5
(Source ID) Identifies the ID of the call sources from which this endpoint accepts calls. This field simplifies the creation of a Dial Plan in applications where the criterion for switching calls to a certain endpoint is a function of which endpoint originated the call. Source ID may be entered with the usual wild card entries (except $).

X = any digit 0—9
[1,3,5] = any of these digits

Default value = 0. The default ID for all Source endpoints and all accept numbers is 0. This results in all calls being routed based on the dialed number.

»» Accept Number

Write security: 3; Read security: 5
Designates which numbers this endpoint will accept (terminate) from the Network (PSTN). The accept list may consist of multiple entries. The numbers are defined using the following wild cards:

X = Any single digit
N = Any single digit 2—9
$ = Any number of digits of any value
9 = This specific number
[1,2,3...] = A single digit in this group

For example, 963-8000 would be a specific incoming number that would be accepted by this endpoint. If this endpoint consisted of a T1 with multiple DS0s, a “hunt” group for 963-8000 would be formed. The entry **$** would accept any call.

Any specific entry will take precedence over a wild card. For example, if endpoint “A” was designated as $ while endpoint “B” accepted 963-800X, then an incoming call to 963-800X would only be accepted by endpoint “B.”

»» Search

Write Security: 3; Read Security: 5
Defines to ATLAS the order in which to search for an accept number.

Primary Search

The Search parameter instructs ATLAS which order to search for an accept number match. Normally all searches are set to primary. The secondary search selection would be used to force ATLAS to only accept a call at this endpoint if all primary endpoints were unavailable.

For example, all long distance calls should go out a PRI directly to an IXC (MCI, ATT, etc.), and local calls should go out a T1 to the LEC. It may be desirable to place long distance calls on the local exchange if all of the IXC trunks are unavailable (busy or in alarm). In this case, the primary accept number for the local exchange would be N$, and the secondary accept would be 1$.

Secondary Search

The same accept rules apply for all secondary number searches as for primary searches.

»» Data 64K, Data 56K, Audio, Speech

Write security: 3; Read security: 5
Reflects the attached user equipment (typically a TA) bearer capability. If the attached TA can only handle digital calls, then a voice call sent to this endpoint would be rejected.

»» Treat Call As

Allows the incoming call t be treated as the selected call type, regardless of the actual incoming call type. The default selection **As Received** effectively disables the feature by using the actual call type.

» Out#Rej

Write security: 3; Read security: 5
Defines the parameters for outgoing calls that ATLAS 810^{PLUS} will not send to the Network.

»» Reject Number

Designates which numbers this particular endpoint will not pass on toward the Network (PSTN). Use when the outgoing call filter is different for different users. The wild cards are identical to the **Outgoing Call Accept** wild cards. If desired, each User termination port can be set to reject different numbers.

[0,1]-$ rejects all long distance calls, but only for this User termination. If permitted in the Network termination endpoint, this user could not dial long distance numbers while other users could.

»» Data 56K, Data 64K, Audio, Speech

Rejects outgoing calls based on call type. For example, setting the reject number to $, Digital 56/64 to enabled, and Audio and Speech to disabled, rejects all digital calls while not rejecting analog calls.

This list may remain blank if the Accept List meets desired filtering. The Call Reject list takes precedence over the Call Accept list.

» Ifce Config

Sets configuration parameters for the endpoint. These parameters vary by the type of port selected. For detailed information on the interface configuration, see *Interface Configurations* on page 9-10.

> GLOBAL PARAM

Sets ATLAS options which apply to all switched operations, both incoming and outgoing calls.

» End of Number Timeout

Write security: 3; Read security: 5
Sets the length of time ATLAS waits before assuming the outgoing dialed number is complete. The default value is six seconds. This timeout will only be invoked if the dialed number does not match one of the patterns set in the Number Complete Template menu (see *Nbr Complete Templates* below).

» Area Code

Write security: 3; Read security: 5
The local area code. Use for sending caller ID to the Network.

» Nbr Complete Templates

Write security: 1; Read security: 5
Sets completed number patterns for outgoing calls so that ATLAS recognizes when the phone number is complete. For example, a local number will be 7 digits long while a long distance (1+ #) will be 11 digits long. The ATLAS defaults cover almost any installation, and these templates should not require any additional user input except for unusual circumstances. The template allows the use of the following wild card inputs to define numbers:

X = Any single digit
N = Any single digit 2—9
911 = This specific number
[1,2,3...] = A single digit in this group

» Number Type Templates

Write security: 1; Read security: 5
Sets call type patterns. ISDN interfaces require that a number type be sent over the D channel when a call is sent or received. A normal RBS trunk does not send a type designator, but uses prefixes instead. For example, “1 +” prefix is a national long distance call type while a “011 +” prefix is an international long distance call type. These templates form a table to permit ATLAS to translate the RBS prefix into a call type for ISDN and vice-versa.

»» # — Denotes an Entry Number (MAX 50). Press **INS/DEL** to insert / delete any entry.

»» Pattern — Modifies an entry when you press **Enter** (MAX 40).

For example, 1+(NXX) NXX - XXXX would be a pattern for a normal long distance call. Note that the symbols ( ), +, - and space are not required and are only used to improve readability.

The ATLAS default templates should cover all applications and should not need to be added to by the user except for very rare circumstances.

» Automatic Routeback Rejection

Write security: 1; Read security: 5
When enabled, **Automatic Routeback Rejection** prevents calls which enter through Network termination interfaces from being forwarded out another network interface. Such an event could happen if an incoming call specifies a number that has no endpoint configured to accept it and another network interface has a call acceptance entry which could accept it (such as $). Without automatic rejection, such a call would be forwarded back to the Network. The Network would in turn resend the call to the unit until all incoming resources are consumed.

»» # — Denotes an Entry Number (MAX 50). Press **INS/DEL** to insert / delete any entry.

»» Prefix — Sets the prefix for the number type. Only digits 0 and 1 are allowed (MAX 6).

»» Pattern — Modifies an entry when you press **Enter** (MAX 40).

»» Number Typ — Lists valid selections when you press **Enter**.

Use extreme caution when disabling **Automatic Routeback Rejection**.

» Global Tone Type

Specifies the dialing digit tone encoding to be used throughout the entire system.

INTERFACE CONFIGURATIONS

This section describes Dial Plan **Network Termination** and **User Termination** configuration settings for the following modules.

Quad T1/PRI Module (Network Termination/PRI)

When you are working in the **Network Termination** section of the **Dial Plan**, **Slot** is defined as a T1/PRI module, and **Sig** is set to PRI, the following configuration options are available:

»» Switch Type
Write security: 2; Read security: 5
Defines the type of PRI switch that ATLAS is connected to. If connected to another ATLAS, both need to be set to the same type. The available options include Lucent 5E, Northern DMS 100, National ISDN, and AT&T 4ESS.

»» First DS0
Write Security: 3 Read Security: 5
Defines the first active DS0 for a fractional PRI.

»» Number of DS0s
Write Security: 3 Read Security: 5
Defines the number of DS0s used for calls on this PRI. DS0 24 is assumed to be used by the PRI for the D channel.

»» Outgoing Number Conversion

Write Security: 3 Read Security: 5
Defines the rules for converting as-dialed numbers into ISDN number type and plan.

As dialed	Send digits provided as unknown number type.
ISDN - National pref	Convert to ISDN type, using the 10-digit national form if possible.
ISDN - Subscriber pref	Convert to ISDN type, using the 7-digit subscriber form if possible.
ISDN - National DMS Reserved pref	Send digits provided as National Number Type, DMS Reserved Numbering Plan.

When a 4ESS is configured, many installations will require the national form where possible; this may also be the preferred form in 10-digit calling areas.

»» Strip MSD

Write Security: 3 Read Security: 5
Strips a selected quantity of the Most Significant Digits (MSD) of a dialed number prior to being forwarded out of the port. For example, a Network port set to accept all calls beginning with 9 (9$) and **Strip MSD** set to 1, sends all digits toward the Network except the leading 9.

Strip MSD *does not affect the* **Call Accept** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as Accept criteria.*

»» Netwrk Spec. Fac.-Voice

Write Security: 3 Read Security: 5
(Network Specific Facility - Voice) Defines specific facility IEs to send to the Network. Use this option if the customer has subscribed to a network specific facility service such as AT&T Megacom service. The facility request sent can be different for voice calls versus data calls. A setting of **Normal** indicates no special facilities have been subscribed.

»» Netwrk Spec.-Fac. Data

Write Security: 3 Read Security: 5
(Network Specific Facility - Data) Defines specific facility IEs to send to the Network. Use this option if the customer has subscribed to a network specific facility service such as AT&T Megacom service. The facility request sent can be different for voice calls versus data calls. A setting of **Normal** indicates no special facilities have been subscribed.

»» Called Digits Transferred

Write security: 2; Read security: 5
Defines the number of digits to expect (choose from **None, Three, Four,** and **All**). The default is All and would almost always be correct. If less than All digits are sent, then the prefix is defined below. Use this option for PRI switches that only send a portion of the called number (like DID).

»» Outgoing Caller ID — Write Security: 3 Read Security: 5
Inserts a called ID based on the following selections:

Send as provided — ATLAS forwards whatever ID it receives (including None).

Substitute if not present — ATLAS inserts a User-defined ID value if no value is received.

ID Presentation — Sends to the Network control information for the presentation of Caller ID (Presentation Allowed; Presentation Restricted; Number Not Available).

ID Number — Value for Caller ID to be sent to the Network (i.e., 256 963 8020).

Substitute always — ATLAS always inserts the User-defined ID in place of the value received.

ID Presentation — Same as above.

ID Number — Same as above.

»» Source ID — Simplifies the creation of a **Dial Plan** in applications where the criterion for switching calls to a certain endpoint is a function of which endpoint originated the call.

- Default value = 0. The default ID for all endpoints is 0 and for all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple endpoints can have the same **Source ID**.
- When creating the **Call Accept** list, specify a **Source ID**(s) as well as a dialed number or range of dialed numbers to accept.

Say, for example, an application requires that all calls originating from Port 1 of the Quad T1 / PRI module in Slot 1 be switched to Port 4 of that same module. Assign a unique **Source ID** (e.g., 7) to Port 1 of the module, and then configure Port 4 to only accept calls from that unique **Source ID** (7).

»» Swap ANI/DNIS — Swaps the ANI and DNIS numbers received from the Network. ANI (Automatic Number Identification) is the billing number of the calling party, and DNIS (Dialed Number Identification Service) is the called party number.

This swap causes the ATLAS switchboard to use ANI to route the call. The accept number in the Dial Plan must use the ANI number, not the DNIS number.

Quad T1/PRI Module (Network Termination/NFAS)

When you are working in the **Network Termination** section of the **Dial Plan** menu, **Slot** is defined as a T1 / PRI module, and **Sig** is set to NFAS, the fol-

lowing configuration menu is available (in addition to the standard Network Termination / PRI configuration menus and options):

» Secondary Interfaces
Write security: 3; Read security: 5
Defines the additional PRI interfaces controlled by the D-channel on this endpoint.

» Slot, Port
Write security: 3; Read security: 5
Defines the slot and port in which the additional interface terminates.

» Interface Number
Write security: 3; Read security: 5
Defines the interface number (assigned by the network provider) that uniquely identifies each additional interface.

Quad T1/PRI Module (Network Termination/RBS)

When you are working in the **Network Termination** section of the **Dial Plan** menu, **Slot** is defined as a T1 / PRI module, and **Sig** is set to RBS, the following interface configuration options are available:

»» First DS0
Write security: 2; Read security: 5
Defines to ATLAS the DS0s which will be used for this endpoint. These are the DS0s which ATLAS will use to send and receive calls to and from the Network (PSTN). Outgoing calls which will be allowed or restricted over these DS0s are set by the **Outgoing Call Accept** and **Reject Numbers** discussed earlier.

»» Number of DS0s
Write security: 3; Read security: 5
Specifies the number of DS0s already defined for this endpoint. This field is read-only.

»» DS0s Available

Read security: 5
Indicates which DS0s of the T1 have been defined in this switched endpoint (indicated by "**!** "), in another switched endpoint (indicated by "s"), or in a dedicated map (indicated by "n"). The following symbols may display in this field:

digits 0—9	This DS0 is available. The digit that displays in this field represents the last digit of the DS0 number.
*	This port is requesting this DS0 for this connection, but the DS0 is not yet activated.
!	This DS0 is used by this port in this connection and is activated.
s	This DS0 is used in the switched Dial Plan.
S	This DS0 is used in the switched Dial Plan and conflicts with this connection.
n	This DS0 is already used in this dedicated map.
N	This DS0 is already used in this dedicated map and conflicts with this connection.

»» Trunk Type (Voice/ SW56)

Write security: 3; Read security: 5
Use if the incoming service on this trunk is Switched 56 digital instead of standard voice.

»» Signaling Method

Write security: 3; Read security: 5
Defines to ATLAS the type of signaling to be used across this trunk. The signaling selected needs to match the signaling being provided by the Network (PSTN). The available options include E&M Immediate, E&M Wink, Loop Start, and Ground Start.

»» Direct Inward Dialing

Write security: 3; Read security: 5
Defines to ATLAS whether DID is being used by the Network. If DID is Enabled, then the following information must be defined:

DID Digits Transferred

Write security: 3; Read security: 5
Defines the number of digits sent to ATLAS from the Network if DID is used.

DID Prefix

Write security: 3; Read security: 5
Defines to ATLAS the prefix digits which are not received as a part of the DID number. ATLAS uses the combination of prefix and DID number to determine the User endpoint that should receive the incoming call. This option only displays if Direct Inward Dialing (DID) is set to Enabled. If DID is Disabled, then you must define the trunk number.

»» Trunk Number

Write security: 3; Read security: 5
Defines to ATLAS the number to use to determine which user endpoint should receive the incoming call, when the Network connection does not provide DID digits. This field only displays when Direct Inward Dialing is set to Disabled. For example, if a certain incoming DS0 (trunk) is meant to connect to an endpoint with the accept number of 963-8615, the trunk number would be set to 963-8615.

The trunk number must be specific (i.e., no wild cards).

»» Strip MSD

Write Security: 3 Read Security: 5
Strips a selected quantity of the Most Significant Digits (MSD) of a dialed number prior to being forwarded out of the port. For example, a Network port set to accept all calls beginning with 9 (9$), and with **Strip MSD** set to 1, would send all digits toward the Network except the leading 9.

Strip MSD *does not affect the* **Call Accept** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criteria.*

»» Source ID

Simplifies the creation of a **Dial Plan** in applications where the criterion for switching calls to a certain endpoint is a function of which endpoint originated the call.

- Default value = 0. The default ID for all endpoints is 0 and all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple endpoints can have the same **Source ID**.
- When creating the **Call Accept** list, specify a **Source ID(**s) as well as a dialed number or range of dialed numbers to accept.

For example, an application requires that all calls originating from Port 1 of the Quad T1/PRI module in Slot 1 be switched to Port 4 of that same module. Assign a unique **Source ID** (e.g., 7) to Port 1 of the module, and then configure Port 4 to only accept calls from that unique **Source ID** (7).

Quad T1/PRI Module (User Termination/PRI)

When you are working in the **User Termination** section of the **Dial Plan** menu, **Slot** is defined as a T1/PRI module, and **Sig** is set to PRI, the following configuration options are available:

»» Switch Type
Write security: 3; Read security: 5
Defines the type of PRI switch that ATLAS is going to emulate. If connected to another ATLAS, both need to be set to the same type. Options include Lucent 5E, Northern DMS100, National ISDN, and AT&T 4ESS.

»» First DS0
Write Security: 3 Read Security: 5
Defines to ATLAS the first active DS0.

»» Number of DS0s
Write Security: 3 Read Security: 5
Defines the number of DS0s used for calls on this PRI. DS0 24 is assumed to be used by the PRI for the D channel.

» Strip MSD
Write Security: 3 Read Security: 5
Allows a selected quantity of the Most Significant Digits (MSD) of a dialed number to be stripped prior to being forwarded out of the port. For example, a Network port could be set to accept all calls beginning with 9 (9$), and then with **Strip MSD** set to 1, all digits would be sent toward the Network except the leading 9.

The Strip MSD parameter does not affect the Call Accept criteria. All of the digits (including the MSDs that are subsequently stripped) are used as Accept criteria.

» Network Specific Facility Voice
Write Security: 3 Read Security: 5
Defines the specific facility IEs to send to the Network. Use this option if the customer has subscribed to a network specific facility service such as AT&T Megacom service. The facility request sent can be different for voice calls versus data calls. A setting of **Normal** indicates no special facilities have been subscribed.

» Network Specific Facility Data
Write Security: 3 Read Security: 5
Defines the specific facility IEs to send to the Network. Use this option if the customer has subscribed to a network specific facility service such as AT&T Megacom service. The facility request sent can be different for voice calls versus data calls. A setting of **Normal** indicates no special facilities have been subscribed.

»» Called Digits Transferred
Write security: 3; Read security: 5
Defines to ATLAS the number of called-number digits to forward. When attached to a PBX, the PBX may be provisioned to expect to receive fewer than all of the called digits of the incoming call. This would normally be set to **All**.

»» Outgoing Caller ID

Write Security: 3 Read Security: 5
Allows the user to insert a called ID to outgoing calls (coming in from attached User equipment). If set to **Send as Provided**, then ATLAS will forward whatever ID it receives (including none). If set to **Substitute if not present**, then ATLAS inserts a User-defined ID value if no value is received. If set to **Substitute Always**, then ATLAS always inserts the User-defined ID in place of the value received.

» ID Presentation

Defines control information for the presentation of **Caller ID** (**Presentation Allowed; Presentation Restricted; Number Not Available**).

» ID Number

Value for **Caller ID** to be sent to the Network (i.e., 256 963 8020).

» Source ID

Simplifies the creation of a **Dial Plan** in applications where the criterion for switching calls to a certain endpoint is a function of which endpoint originated the call.

- Default value = 0. The default ID for all endpoints is 0 and all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple endpoints can have the same **Source ID**.
- When creating the Call Accept list, specify a **Source ID**(s) as well as a dialed number or range of dialed numbers to accept.

For example, an application requires that all calls originating from Port 1 of the Quad T1/PRI module in Slot 1 be switched to Port 4 of that same module. Assign a unique **Source ID** (e.g., 7) to Port 1 of the module, and then configure Port 4 to only accept calls from that unique **Source ID** (7).

»» Swap ANI/DNIS

Swaps the ANI and DNIS numbers prior to being forwarded to the attached user equipment. ANI (Automatic Number Identification) is the billing number of the calling party, and DNIS (Dialed Number Identification Service) is the called party number.

This swap occurs after the ATLAS switchboard has routed the call. The accept number in the Dial Plan must use the number in the DNIS position prior to swapping.

Quad T1/PRI Module (User Termination/NFAS)

When you are working in the **User Termination** section of the **Dial Plan** menu, **Slot** is defined as a T1/PRI module, and **Sig** is set to NFAS, the following configuration menu is available (in addition to the standard User Termination/PRI configuration menus and options):

» Secondary Interfaces

Write security: 3; Read security: 5
Defines the additional PRI interfaces controlled by the D-channel on this endpoint.

» Slot, Port

Write security: 3; Read security: 5
Defines the slot and port in which the additional interface terminates.

» Interface Number Write security: 3; Read security: 5
Defines the interface number that uniquely identifies each additional interface.

Quad T1/PRI Module (User Termination/RBS)

When you are working in the **User Termination** section of the **Dial Plan** menu, **Slot** is defined as a T1/PRI module, and **Sig** is set to RBS, the following configuration options are available:

»» First DS0/Number of DS0s — Write security: 3; Read security: 5
Defines to ATLAS the DS0s which will be used for this endpoint. These are the DS0s which will be used by ATLAS to send and receive calls to and from User equipment (PBX). The incoming calls which will be accepted and the outgoing calls which will be restricted over these DS0s are set by the Incoming Call Accept and Outgoing Call Reject Numbers discussed earlier.

»» DS0s Available — Read security: 5
Indicates which DS0s of the T1 have been defined in this switched endpoint (indicated by "**!** "), in another switched endpoint (indicated by "s"), or in a dedicated map (indicated by "n").

»» Signaling Method — Write security: 3; Read security: 5
Defines to ATLAS the type of signaling to be used across this trunk. The signaling selected needs to match that being used by the user equipment (PBX). The available options include E&M Immediate, E&M Wink, Loop Start, and Ground Start.

ATLAS converts signaling types between Network and User terminations.

»» Direct Inward Dialing — Write security: 3; Read security: 5
Defines to ATLAS whether DID is being used by the Network. This option only displays if Direct Inward Dialing (DID) is set to Enabled. If DID is Enabled, then the following information must be defined:

DID Digits Transferred — Write security: 3; Read security: 5
Defines the number of digits sent to ATLAS from the Network if DID is used.

DID Prefix

Write security: 3; Read security: 5
Defines to ATLAS the prefix digits which are not received as a part of the DID number. ATLAS uses the combination of prefix and DID number to determine the User endpoint that should receive the incoming call.

If DID is Disabled, then you must define the trunk number.

» Caller ID Number

Write security: 3; Read security: 5
Defines the number for ATLAS to use to provide Caller ID to the Network for outgoing calls sent through this endpoint. This option only displays if **Direct Inward Dialing** is set to **Disabled**. This item is optional.

The Caller ID number must be specific (i.e., no "wild cards").

»» Strip MSD

Write Security: 3; Read Security: 5
Allows a selected quantity of the Most Significant Digits (MSD) of a dialed number to be stripped prior to being forwarded out of the port. For example, a User port could be set to accept all calls beginning with 8 (8$), and then with Strip MSD set to 1, all digits would be sent toward the network except the leading 8.

The Strip MSD parameter does not affect the Call Accept criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criteria.

»» Source ID

Write security: 3; Read security: 5
Simplifies the creation of a Dial Plan in applications where the criterion for switching calls to a certain endpoint is a function of which endpoint originated the call.

- Default value = 0. The default ID for all endpoints is 0 and all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple endpoints can have the same **Source ID.**
- When creating the **Call Accept** list, specify a **Source ID**(s) as well as a dialed number or range of dialed numbers to accept.

For example, an application requires that all calls that originate from Port 1 of the Quad T1 / PRI module in Slot 1 be switched to Port 4 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 4 to only accept calls from that unique Source ID (7).

Quad Nx56/64 Module (User Termination)

The Quad Nx56/64 can only serve as a User termination endpoint.

When you are working in the **User Termination** section of the **Dial Plan** menu, and **Slot** is defined as a QuadNx56/64 module, the following interface configuration options are available:

»» Ports Available — Indicates which of the four ports of the Quad Nx56/64 module have already been defined either in another switched endpoint (indicated by "s") or in a dedicated map (indicated by "n"). This field is read-only.

»» Number of Ports — Defines to ATLAS how many of the ports could be used to answer calls to the number(s) defined in the Accept Call list. You can enter numbers 1 through 4. The ports are contiguous beginning with the port number select and the number of ports.

For example, if the port selected (as a part of Slot/Port selection) is 2, and the number of ports selected here was 2, then ports 2 and 3 would be enabled to receive calls to the numbers listed under the Incoming Call Accept list.

Octal BRI Module (Network Termination)

The Octal BRI with a "U" interface can interface directly to the Network (PSTN). When you are working in the **Network Termination** section of the **Dial Plan** menu and **Slot** is defined as a UBRI-8 option module, the following interface configuration options are available:

»» Switch Type — Write security: 2; Read security: 5
Defines the type of ISDN switch that ATLAS is connected to. If connected to another ATLAS, both need to be set to the same type. The available options are Lucent 5E, Northern DMS 100, and National ISDN.

»» SPID List — Write security: 2; Read security: 5
In order to properly operate with a network (PSTN) ISDN switch, the BRI interface must have SPID (Service Profile Identifier) and phone number(s) that match the SPID(s) and phone number(s) which have been programmed into the ISDN switch for this line. Each BRI may have one or more phone numbers and SPIDs. The **SPID Number** list submenu defines to ATLAS these parameters.

Phone Number — The phone number(s) assigned to this BRI phone line.

SPID Number — This entry must match the SPID number(s) which have been set in the Network's ISDN switch (or in the PBX) for this BRI line. A SPID must be entered for each phone number.

Calls	The number of calls (1 or 2) which can be received or sent on this number / SPID.
D64, D56, Audio, Speech	These options reflect what the Network has provisioned for this SPID. If the BRI was purchased with different services provisioned for the SPIDs, then the call must match the services supported.

Octal BRI Module (User Termination)

The Octal BRI with a "U" interface acts as the Network while interfacing to user equipment (terminal adapters). When you are working in the **User Termination** section of the **Dial Plan** menu and **Slot** is defined as a UBRI-8 module, the following interface configuration options are available:

»» Switch Type	Write security: 2; Read security: 5 Defines the type of ISDN switch that ATLAS will simulate. If connected to another ATLAS, both need to be set to the same type. The available options include Lucent 5E, Northern DMS 100, and National ISDN.
»» SPID List	Write security: 2; Read security: 5 ATLAS, acting as the Network, must use a SPID and a phone number in order to satisfy the ISDN connection protocol expected by the User's Terminal Adapter (TA).
Phone Number	The phone number(s) assigned to this BRI phone line.
SPID Number	Defines the SPID number(s) which will be used for this BRI line. Although the value of the SPID is not significant, a SPID must be entered for each phone number. For convenience, the SPID can be set to be the same as the phone number.
Calls	For User terminations, the number of calls is fixed at 2.
D64, D56, Audio, Speech	Reflects what the Network has provisioned for this SPID. If the BRI was purchased with different services provisioned for the SPIDs, then the call must match the services supported.

ATLAS 810^{PLUS} does not support autoSPID detection software which some terminal adapters offer.

CREATING DIAL PLANS—EXAMPLES

The ATLAS **Dial Plan** acts as the numbering plan for switched connections. This menu defines to ATLAS the phone numbers and features associated with dual-tone-multifrequency (DTMF) dialing, Primary Rate ISDN (PRI), and Basic Rate ISDN (BRI). To operate as a switch, ATLAS must be able to terminate Network connections (*Network terminations*) and emulate the network onto other termination equipment (*User terminations*).

Understanding Dial Plan Configurations

Understanding Dial Plan configurations results in the successful creation of a switched connection. This understanding includes determining which of the connections are acting as Network terminations and which are acting as User terminations. Use Examples 1 and 2 to help clarify the definitions for these two types of terminations.

Example 1 PSTN Connection Dial Plan Configuration

In this example, access to the PSTN is provided by a single PRI line. Therefore, this line is configured as a Network termination. The remaining circuits, which feed various types of switched equipment, are configured as User termination because ATLAS is emulating the network on those connections (see Figure 9-3).

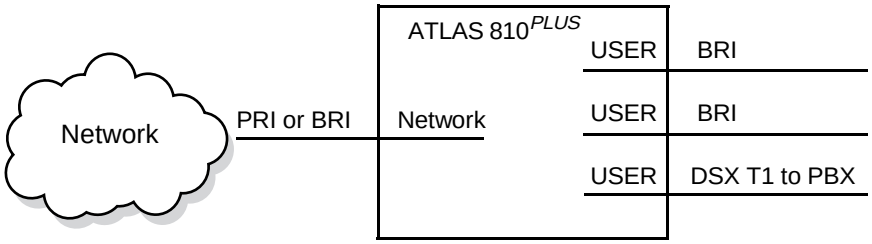


Figure 9-3. PSTN Connection

Example 2 Point-to-Point Connection Dial Plan Configuration

In this example, ATLAS A operates as the network while ATLAS B *terminates* the network. That is, ATLAS A emulates the network and its PRI interface acts as the User termination. The PRI interface of ATLAS B acts as the Network termination (see Figure 9-4).

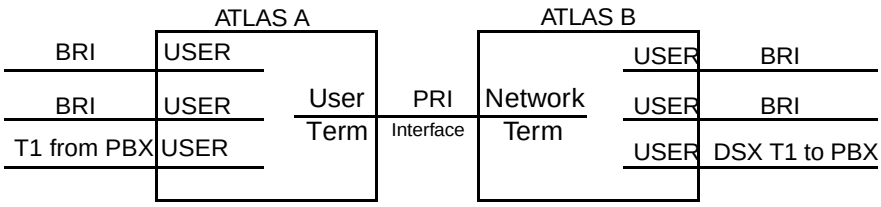


Figure 9-4. Point-to-Point

Example 3 Remote Access and Video Conferencing Dial Plan

A corporate office has T1 RBS service for voice but wants to add a PRI for video conferencing and remote access. The office would like to use the PRI for all functions, but it still wants to use the incoming BRI to supply added bandwidth. The office wants to provide BRI lines to the video equipment, provide a PRI to the remote access server (RAS), and send a T1 RBS to the PBX (see Figure 9-5).

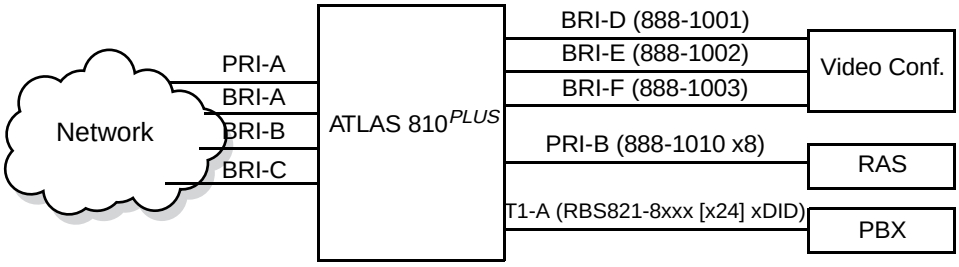


Figure 9-5. Remote Access and Video Conferencing Setup

For this example, the User termination BRI lines (D, E, F) each have a specific phone number. The PRI serving the RAS has an 8-number hunt group, and the T1 to the PBX uses DID. Assume that all calls originating from the PBX to 1-900 numbers are restricted. Also, assume that the Network termination BRI lines (A, B, C) only allow outgoing calls to other local corporate offices for video conferencing. The numbers fall in the range of 888-0100 to 888-0120.

The following Step / Action Tables and numbered tables provide information on setting up Example 3.

Instructions for Configuring the Ports for Example 3	
Step	**Action**
1	Prior to setting up the Dial Plan, you must configure the Controller T1/PRI interfaces.
2	This configuration action only brings up the T1 transport; set the BRI configuration (SPID and phone number) as part of the Dial Plan.

Instructions for Setting Up the Dial Plan for Example 3	
Step	**Action**
1	Determine the network and the attached equipment (video equipment and PBX) provisioning (see Table 9-1).
2	From **Dial Plan**, select **Global Parameter**, and enter the local area code (needed for Caller ID operation).
3	Determine which ports are Network terminations and which are User terminations.
4	Define the phone number acceptance and rejection criteria for each termination.

Example 3 includes one PRI port terminating the network (PRI-A) and three BRIs (BRI A, B, and C)—see Table 9-2.

User terminations include one PRI, one RBS T1, and three BRIs (see Table 9-3).

Table 9-1. Network and Attached Equipment Provisioning

Network PRI	**Type of provided PRI switch** National ISDN DMS 100 custom 4ESS custom 5ESS custom DID- number of digits
	Type of provided BRI switch National ISDN DMS 100 custom 5ESS custom SPID(s) and phone number(s) provisioned for the BRI line
User Equipment	**PRI** Switch type the user equipment expects to interface to (ATLAS supports 4ESS custom and 5ESS custom).
	DID Number of digits.
	BRI Switch type the user equipment expects to interface to (ATLAS supports National ISDN, 5ESS custom, and DMS 100 custom). SPID and phone numbers provisioned in equipment.
	T1 RBS DID enabled on PBX/number of digits; Signaling (E&M/ Loop Start/Ground Start).

Table 9-2. Network Terminations

NAME	PORT	OUTGOING ACCEPT #	OUTGOING REJECT #	OTHER
PRI-A	Controller T1 Slot 0, Port 1	$ - This port will forward any call to the network.	Blank - No called number will be rejected.	**PRI Type:** National ISDN
BRI-A BRI-B BRI-C	Octal BRI Slot 1, Port 1,2,3	1)888-01[0,1]X Allows calls to 888-0100 to 888-0119 2)888-0120	Blank - No called number will be rejected.	**BRI Type:** National ISDN SPID #s **PHONE #s:** 888-1001, 1002,1003, & 888-1010 (All)

Table 9-3. User Terminations

NAME	PORT	INCOMING ACCEPT #	OUTGOING REJECT #	OTHER
BRI-D BRI-E BRI-F	Octal BRI Slot 1, Ports 4-5,6	888-1001 (D); 888-1002 (E); 888-1003 (F)	Blank - No called number will be rejected.	**BRI type**: 5ESS SPID # to match Video Equipment provisioning. **Phone #s:** 888-1001 (D); 888-1002 (E); 888-1003 (F) Phone numbers must match phone numbers provisioned in video equipment.
PRI-B	Controller T1 Slot 0, Port 2	888-1010 This forms a hunt group.	Blank - No called number will be rejected.	**PRI type**: 5ESS Must match RAS equipment. DID=none
T1-A	Slot 2, Port 1	821-8XXX This accepts all calls beginning with 821-8.	1-900-$ This rejects all calls beginning with 1-900.	**RBS** 1st DS0=1; #DS0 = 24 Signalling = E&M wink DID = Enable/# of digits = 4

To implement the Dial Plan for Example 3, navigate to **Dial Plan/Global Param** and set the global parameters for PRI A, B, and C. Then, navigate to **User Term** and set the connections for PRI D, E, and F. The following Step / Action tables provide step-by-step instructions for completing these procedures.

Setting PRI A Global Param	
Step	**Action**
1	Navigate to **Dial Plan** (in the terminal menu).
2	Enter the area code by selecting **Global Param**/**Area Code** and pressing **Enter**. Input the area code, and press **Enter** again.
3	Define the interface type as PRI by selecting Network Term and entering the following settings: **Slot = 0, Port = 1, Sig = PRI**.
4	Tell ATLAS to forward any call to the network by selecting Out#Accept and entering **$** in the number field. Leave all other selections set to default (Enabled).
5	Ensure **Out#Reject** contains no entry.
6	Set the PRI switch type to **National ISDN** (from **Ifce Config**).

Setting PRI A Global Param (Continued)	
Step	**Action**
7	Back out of the connection to the index number column by pressing **ESC** on the keyboard.
8	Insert three more connections into the list for the BRI lines by typing the letter **I** three times.
9	Enter **Out#Accept** and **Out#Reject** numbers for Slot 1/ Port 1. The **Out#Accept** numbers have two entries: Entry 1) 888-01[0,1]X Entry 2) 888-0120 } Allows all numbers 888-0100 to 888-0120
10	Set the BRI switch type (from **Ifce Config**) used by the network to **National ISDN**. From **SPID**, enter the SPID numbers and phone numbers which match the network provisioning for this BRI line.
11	Press **ESC** to return to the index column, #.

Setting PRI B Global Param	
Step	**Action**
1	While on the entry for BRI A, type **C** to copy the entire BRI A entry.
2	Move to the next connection list entry and type **P** to paste all of the BRI data.
3	Move to each field and modify as appropriate for BRI B.

Setting PRI C Global Param	
Step	**Action**
1	While on the entry for BRI B, type **C** to copy the entire BRI B entry.
2	Move to the next connection list entry and type **P** to paste all of the BRI data.
3	Move to each field and modify as appropriate for BRI C.

After completing the network entries, the Network connection map appears as shown in Figure 9-6.

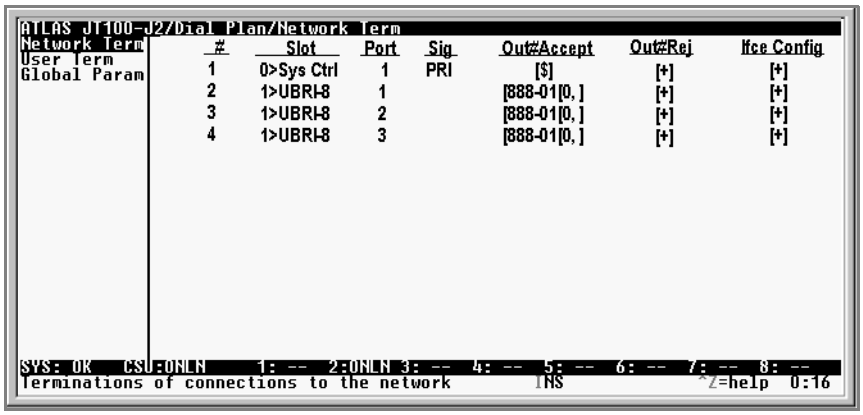


Figure 9-6. Completed Network Map

Setting User Term Connections	
Step	**Action**
1	Navigate to **User Term.**
2	Enter connections for BRI D,E, and F in the same manner as BRI A, B, and C: use the copy (**C**) and paste (**P**) commands to enter the appropriate **Out#Accept** and **Out#Reject** numbers.
3	Ensure that the **SPID** and **Phone** entries under **Ifce Config** match the SPID and phone numbers of the attached equipment.
4	Enter the connection for T1-A: select **RBS** under **Sig,** and enter 1-900-$ under **Out#Reject**.
5	Set **Trunk Type** (under **Ifce Config**) to **Analog**.
6	Set **Signaling Method** to **E&M Wink**.
7	Set **DID** (under **Ifce Config**) to enabled.
8	Set the **DID Digits Transferred** to **4**.

When you complete the **User Term** Dial Plan, it appears as shown in Figure 9-7.

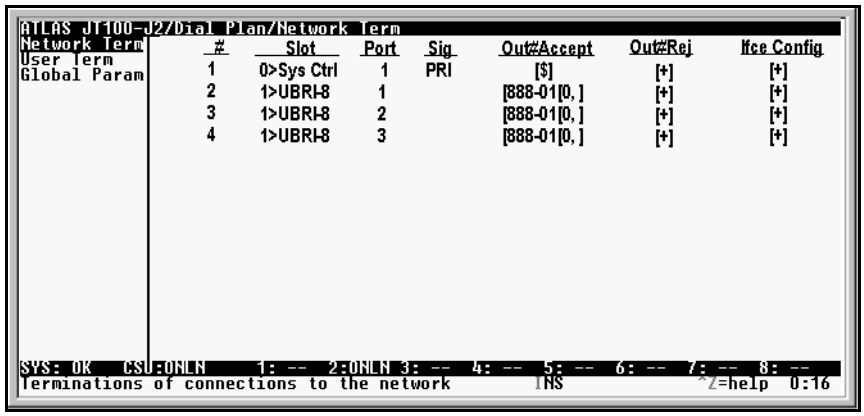


Figure 9-7. Completed User Map

A connection is not actually made *(available) until you press* **Esc** *to move the cursor to the index number or move the cursor onto another connection line.*

Chapter 10 Updating Firmware

OVERVIEW

To provide feature enhancements in the future, ATLAS 810^{PLUS} supports firmware updating by field personnel. Two transfer methods are available for use in updating any modules that contain Flash memory, including the ATLAS 810^{PLUS} system controller. The first transfer method is via the ATLAS 810^{PLUS} Chain In port using XMODEM protocol. The second transfer method is via the ATLAS built-in Ethernet port using TFTP (Trivial File Transfer Protocol). To simplify the update procedure, a common menu interface is available for updating any upgradable module within the ATLAS 810^{PLUS} (see also *Update Firmware* on page 6-16). The following sections describe the procedure for updating using either transfer method.

Please consult the appropriate ATLAS 810^{PLUS} module manual to determine if the module supports Flash upgrading.

Users must use the supplied connector when using VT-100 or when doing any asynchronous Flash activity.

XMODEM FIRMWARE UPDATES

The ATLAS 810^{PLUS} supports firmware updating to any upgradable module using XMODEM transfer protocol via the base unit's Chain In port. XMODEM is found in most PC communications software packages. To configure the Chain In port's data rate and other communication parameters, consult *Control/Chain In Port* on page 2-4 and *Control/Chain Out Port* on page 2-5.

Ensure the communications software package being used has flow control turned off.

Updating Firmware using XMODEM

Before beginning this procedure,

- you must have a level 2 password for updating any module within ATLAS 810^{PLUS}. Please consult the ATLAS 810^{PLUS} administrator if you do not know the password.
- you must obtain the appropriate update file for the particular module from ADTRAN Technical Support at (888) 4ADTRAN (423-8726).
- you may want to review *Update Firmware* on page 6-16.

Instructions for Updating Firmware Using XMODEM	
Step	**Action**
1	Using a VT-100 terminal emulation communication software package which contains XMODEM protocol support, **log in** to ATLAS 810^{PLUS}.
2	Select **System Utility** / **Update Firmware** (see Figure 10-1).
3	Move the cursor to **Module Slot**, and press **Enter**. Select the appropriate module slot to update. To update multiple modules of the same type, select **All Modules of a Type** from **Module Slot**. (Only upgradable modules are displayed as choices for **Module Type** when updating **All Modules of a Type** in the ATLAS.)
4	Select **XMODEM** for **Transfer Method**.
5	From **Restart Schedule**, select the time for the module to perform a restart after completing the update process (see *Restart Schedule* on page 6-17).
6	View **Current Update Status** to verify the progress of the current firmware update or any errors encountered during the download process (see *Current Update Status* on page 6-18).
7	Select **Begin Firmware Update** to start the update process. Enter **Y** to confirm the transfer and to set up the module to receive the XMODEM upload. *When ATLAS is ready to receive the XMODEM upload, the menu screen will clear and display* **Awaiting XMODEM Upload…… <CTRL-X> to Cancel**. *If this does not appear, please review the steps above for possible configuration errors.*

Instructions for Updating Firmware Using XMODEM *(Continued)*	
Step	**Action**
8	From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. (If necessary, refer to your 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.) *Because XMODEM data is being transferred in-band through the menu interface, the VT-100 menus of ATLAS will be inoperable from the Chain In port. 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	To update additional modules, begin at step 3 and repeat this process.

When the update process has successfully completed, **Idle** displays in the **Current Update Status** field and **Module Update Complete** displays in the **Previous Update Status** field. Either the module restarts immediately and resumes operation, or it restarts at the specified time and day of the week—depending on your selection.

If an error occurred during the update process, **Previous Update Status** displays an appropriate error message.

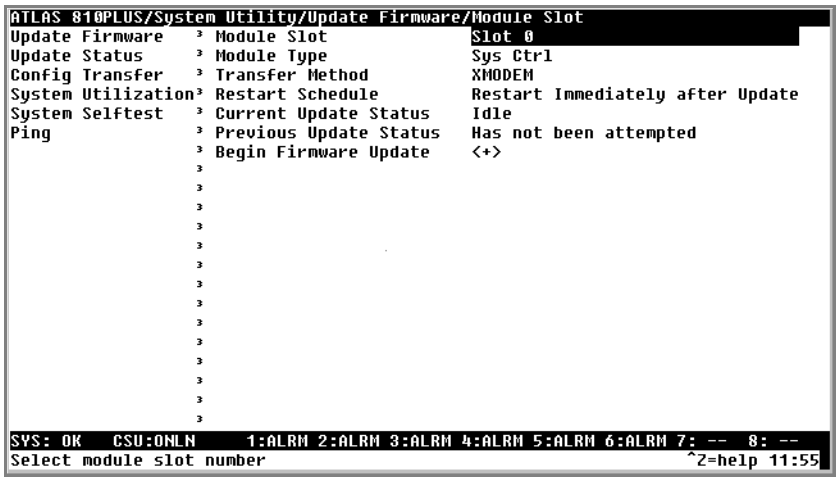


Figure 10-1. Update Firmware Menu Interface

TFTP FIRMWARE UPDATES

ATLAS 810^{PLUS} supports firmware updates to any module via the 10BaseT Ethernet port using TFTP from a network server. The network server must be capable of supporting TFTP Server requests from the TFTP client within ATLAS 810^{PLUS}.

Updating Firmware using TFTP

Before beginning this procedure,

- you must have a level 2 password to perform updates of any modules within ATLAS. Please consult the ATLAS administrator if this password is not known.
- you must obtain the appropriate update file for the particular module from ADTRAN Technical Support at (888) 4ADTRAN (423-8726).
- you must copy the update file provided by ADTRAN to a network server that supports TFTP Server requests. Record both the IP address of the server and the full path location of the update file to be downloaded.

Instructions for Updating Firmware Using TFTP

Step	Action
1	Using a Telnet program, **log in** to ATLAS.
2	Select **System Utility / Update Firmware** (see Figure 10-2 on page 10-6).
3	Move the cursor to **Module Slot**, and press **Enter**. Select the appropriate module slot to update. To update multiple modules of the same type, select **All Modules of a Type** from **Module Slot**. (Only upgradable modules are displayed as choices for **Module Type** when updating All Modules of a Type in the ATLAS.)
4	Select **TFTP** for the **Transfer Method**.
5	Enter into **TFTP Server IP Address**, the IP address of the network server that was recorded earlier.
6	Enter into **TFTP Server Filename**, the full path name and filename of the update file that was recorded earlier.
7	From **Restart Schedule**, select the time for the module to perform a restart after completing the update process (see *Restart Schedule* on page 6-17).
8	View **Current Update Status** to verify the progress of the current firmware update or any errors encountered during the download process (see *Current Update Status* on page 6-18).

Instructions for Updating Firmware Using TFTP *(Continued)*	
Step	**Action**
9	Select **Begin Firmware Update** to start the update process. Enter **Y** to confirm the transfer and to set up the module to receive the TFTP upload.
10	To update additional modules, begin at step 3 and repeat this process.

During the TFTP upload process, various status messages display in **Current Update Status** *to indicate progress. Table 10-1 describes these messages.*

When the update process has successfully completed, **Idle** displays in **Current Update Status**, and **Module Update Complete** displays in **Previous Update Status**. Either the module restarts immediately and resumes operation, or it restarts at the specified time and day of the week—depending on your selection.

If an error occurred during the update process, **Previous Update Status** displays the appropriate error message. In this case, return to step 3 and attempt the update process again. If the same error occurs, contact ADTRAN Technical Support.

Table 10-1. TFTP Upload Messages

Message	Meaning
Contacting Server	Indicates communication with the TFTP Network Server is trying to be established with the specified server address in the TFTP Server IP Address field.
Beginning TFTP Transfer	Indicates communication with the TFTP Network Server has been established and the update file is being transferred between ATLAS and the TFTP Network Server.
Completed	Indicates the ATLAS product successfully received the update file.
Error: File Not Found	Indicates the TFTP Network Server was unable to locate the specified file name or path in the TFTP Server Filename field.
Error: Access Violation	Indicates the TFTP Network Server denied ATLAS access to the given update file name and path. Please verify appropriate user rights are selected for the specified path.
Error: Illegal Operation	An unknown operation was detected by ATLAS when transferring the update file from the TFTP Network Server.
Error: User Aborted	Indicates the user selected Cancel Update to abort reception of the update file from the TFTP Network Server.

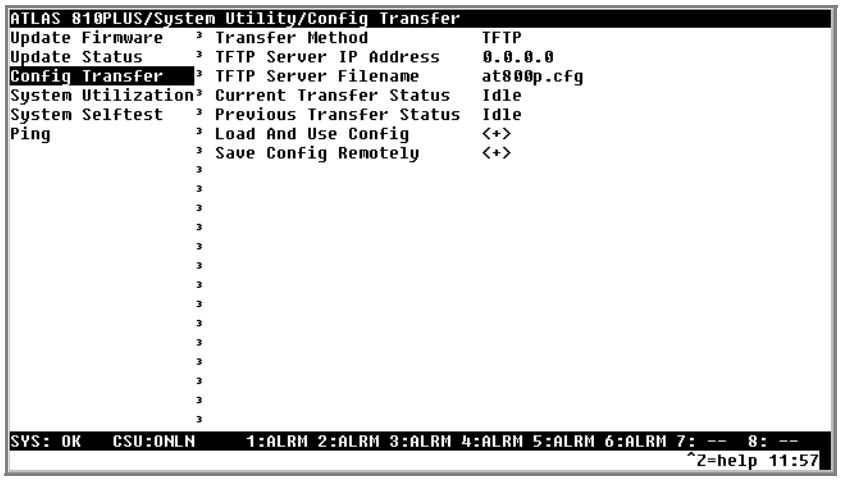


Figure 10-2. Update Firmware Menu Interface

Chapter 11 SNMP Management

SNMP

As local area network (LAN) environments became standardized over the past ten years, multivendor equipment grew with competition. It became necessary to manage various vendor equipment from a single control console. Thus, Simple Network Management Protocol (SNMP) emerged as the standard for managing commercial TCP/IP networks. The term SNMP broadly refers to the message protocols used to exchange information between the network management station and the managed devices, as well as to the structure of network management databases.

Basic Components

SNMP has three basic components: network manager, agent, and management information base (MIB).

Network Manager

The network manager is a control program that collects, controls, and presents data pertinent to the operation of the network devices. It resides on a network management station.

Agent

The agent is a control program that responds to queries and commands from the network manager and returns requested information or invokes configuration changes initiated by the manager. It resides in **each** network device.

MIB

The MIB is an index to the organized data stored within a network device. The MIB defines the operating parameters that can be controlled or monitored. When the MIB requests the network manager to retrieve or modify a particular piece of information about a network device, the network manager transmits that request to the network device. The **agent** in that device interprets the incoming request, performs the requested task, and sends its response to the network manager. The network manager collects all of the data from the various network devices and presents it in a consistent form.

SNMP TRAPS

An SNMP trap is a message sent by a network device, such as the ATLAS 810^{PLUS}, to report an operational anomaly or alarm condition.

Trap Destination List

A trap destination list contains information about sites designated to receive SNMP traps. You can configure this list via a Telnet session or the VT-100 terminal menu. The ATLAS 810^{PLUS} supports up to four trap destination lists. By default, the destination list is empty.

Configuring a Trap Destination List via Terminal Menu

To configure the trap destination list, from the terminal menu select **System Config / SNMP / Traps Destination**. Then enter your information, similar to that shown in Table 11-1. (See also, *Traps Destination* on page 6-10.)

Table 11-1. Trap Destination List

IP Address		Community	Trap Filtering
0	0.0.0.0	public	[+]
1	0.0.0.0	public	[+]
2	0.0.0.0	public	[+]
3	0.0.0.0	public	[+]

IP Address is the address of the network management station to which ATLAS 810^{PLUS} sends the trap. *Community* is the trap community-name used for the selected network device. *Trap Filtering* is a record allowing you to assign thresholds to each category of the ATLAS 810^{PLUS} events.

Filtering (Disabling) Traps

You can disable trap generating events in three ways:

1. Disable **Trap Transmission.** From the terminal menu, select **SNMP** and set **Trap Transmission** to **DISABLED**.

OR

2. Define trap thresholds to disable specific trap events. Refer to the ATLAS MIB in *System Event Logging* on page A-1 for a description of each trap event supported by the ATLAS.

   For example, consider the **coldStart** trap, a system controller event. If you defined for destination 0 a trap filtering threshold of **Warning** for the system controller, the **coldStart** trap would not generate to that destination because the **coldStart** trap severity level is defined as **Normal**. (Recall that each trap event has a severity level: **Disabled, Informational, Normal, Warning, Minor, Major,** and **Critical**.)

OR

3. Control certain traps through SNMP of specific MIB variables. These variables are outlined in the remainder of this chapter.

Standard Traps

Table 11-2 describes the standard traps supported by ATLAS.

Table 11-2. Standard Traps

Index	Trap Name	Severity	Description
0	coldStart	Normal	ATLAS is such that its configuration may be altered; this trap is generated on power up.
1	warmStart	Normal	ATLAS is reinitializing without altering its configuration.
2	linkDown	Warning	One of the ATLAS communication links has failed.
3	linkUp	Normal	One of the ATLAS communication links has come up.
4	authenticationFailure	Informational	ATLAS has received a protocol message that has failed authentication.

RFC1213, or MIB II, defines the object type *snmpEnabledAuthenTraps*. If you set this value to *2*, the generation of the *authenticationFailure* trap is disabled. This trap is enabled by setting *snmpEnableAuthenTraps* to *1*. One possible reason for an authentication failure would be an invalid community name in the received protocol message.

DS1 Traps

ATLAS supports RFC1406, the DS1 standard MIB, as well as the ADTRAN DS1 MIB, an extension to RFC1406. The ADTRAN DS1 group lets you send traps for DS1 Alarm Failures and Performance Threshold Crossing Alerts. The DS1 Alarm Table, defined in the ADTRAN DS1 extension MIB, contains entries that enable the status bits to send an Alarm Trap message. Each Alarm Table row entry corresponds to a DS1 interface managed by the device. The DS1 Alert Table, also defined in the ADTRAN DS1 MIB, contains similar entries for controlling the Alert Traps.

DS1 Alarm Traps

DS1 line status is reported in the bit-encoded *dsx1LineStatus* object variable. Each trap represents a bit value = 1 change in *dsx1LineStatus*. Table 11-3 describes the DS1 alarm traps supported by ATLAS 810^{PLUS}.

Table 11-3. DS1 SNMP Traps

Alarm	Severity	Description
adATLAS800NoAlarm	Warning	No alarms are present.
adATLAS800RxYellow	Minor	The Far End is experiencing Red Alarm (a.k.a. Yellow Alarm).
adATLAS800TxYellow	Warning	The Near End is sending Loss Frame Indication (a.k.a. Yellow Alarm).
adATLAS800RxAIS	Minor	The Far End is sending Alarm Indication Signal (a.k.a. Blue Alarm).
adATLAS800TxAIS	Warning	The Near End is sending Alarm Indication Signal (a.k.a. Blue Alarm).
adATLAS800RedAlarm	Major	The Near End is experiencing Loss of Frame (a.k.a. Red Alarm).
adATLAS800LOS	Major	The Near End is experiencing Loss of Signal.

When enabled, ATLAS 810^{PLUS} sends alarm traps to the each member of the trap destination list upon detecting status bit changes in *dsx1LineStatus*. Each status change sets an event bit = 1 in the *adDS1LineEvent* variable in the DS1 alarm table. If you have previously set the corresponding *enable bit = 1* in the *adDS1LineArm* variable and *adDS1AlarmEnable = On*, then ATLAS 810^{PLUS} sends an alarm trap message. A single alarm trap message may report multiple event changes. ATLAS 810^{PLUS} clears the event bits after sending the trap message or sending the response to a *Get* request for the *adDS1LineEvent* variable.

DS1 Alert Traps

RFC1406 also defines a series of *Current* and *Total Alert* threshold values. You can enable ATLAS 810^{PLUS} to send an alert trap message to each mem-

ber of the trap destination list when accumulated error statistics exceed these threshold values. Table 11-4 describes the alert traps supported by ATLAS 810^{PLUS} for events that have occurred in the last 15-minute interval.

Table 11-4. DS1 Current Alert SNMP Traps

Current Alert	Severity	Description
adATLAS800CurrentES	Warning	The current interval errored second threshold has been exceeded.
adATLAS800CurrentSES	Warning	The current interval severely errored second threshold has been exceeded.
adATLAS800CurrentSEFS	Warning	The current interval severely errored framing second threshold has been exceeded.
adATLAS800CurrentUAS	Major	The current interval is unavailable.
adATLAS800CurrentCSS	Warning	The current interval path code violations have been exceeded.
adATLAS800CurrentLES	Warning	The current interval line errored second threshold has been exceeded.
adATLAS800CurrentCV	Warning	The current interval line code violation threshold has been exceeded.

When one of the *Current Alert* thresholds is exceeded, the corresponding event bit is set to 1 in the *adDS1CurrentAlert* variable in the DS1 alert table. When enabled, ATLAS 810^{PLUS} sends alert traps to each member of the trap destination list upon detecting status bit changes in *adDS1CurrentAlert*. If you have previously set the corresponding enable bit = 1 in the *adDS1CurrentArm* variable and *adDS1AlertEnable* = *On*, then ATLAS 810^{PLUS} sends an alert trap message. A single alert trap message may report multiple event changes. ATLAS 810^{PLUS} clears the event bits after sending the trap message or sending the response to a *Get* request for the *adDS1CurrentAlert* variable. ATLAS 810^{PLUS} clears the *Current Alert* values at the beginning of a new 15-minute interval. *Total Alert* values are cleared at the beginning of a new 24-hour interval.

Table 11-5 shows the *Total Alert Traps*, which describe events that have occurred in the last 24-hour interval.

Table 11-5. Total Alert Traps

Total Alert	Severity	Description
adATLAS800TotalES	Warning	The total interval errored second threshold has been exceeded.
adATLAS800TotalSES	Warning	The total interval severely errored second threshold has been exceeded.
adATLAS800TotalSEFS	Warning	The total interval severely errored framing second threshold has been exceeded.
adATLAS800TotalUAS	Major	The total interval unavailable second threshold has been exceeded.
adATLAS800TotalCSS	Warning	The total interval controlled slip second threshold has been exceeded.
adATLAS800TotalPCV	Warning	The total interval path code violations has been exceeded.
adATLAS800TotalLES	Warning	The total interval line errored second threshold has been exceeded.
adATLAS800TotalLCV	Warning	The total interval line code violation threshold has been exceeded.

When one of the *Total Alert* thresholds is exceeded, the corresponding event bit is set to 1 in the *adDS1TotalAlert* variable in the DS1 alert table. When enabled, ATLAS 810^{PLUS} sends alert traps to each member of the trap destination list upon detecting status bit changes in *adDS1TotalAlert*. If you have previously set the corresponding enable bit = 1 in the *adDS1TotalArm* variable and *adDS1AlertEnable = On*, then ATLAS 810^{PLUS} sends an alarm trap message. A single alert trap message may report multiple event changes. ATLAS 810^{PLUS} clears the event bits after sending the trap message or sending the response to a *Get* request for the *adDS1TotalAlert* variable.

Current Alert and Total Alert described above are *Near End* events. ATLAS 810^{PLUS} also supports Current Alert and Total Alert for the *Far End*. Far End alert traps are generated upon status bit changes in *adDS1FarCurrentAlert* for Current Alerts and *adDS1FarTotalAlert* for Total Alerts. Current and Total Far End Alerts can be disabled by setting the corresponding enable bit = 0 in the *adDS1FarCurrentArm* and *adDS1FarTotalArm* variables, respectively. Far End alert traps can also be disabled by setting *adDS1AlertEnable = Off*.

Chapter 12 ADTRAN Utilities

OVERVIEW

ADTRAN delivers several PC software utilities along with the ATLAS 810^{PLUS}. These utilities are located on the three diskettes that came with your shipment. They also include MIB files (located in the MIB directory).

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

The utilities make interfacing with the terminal menu and transferring configuration files to and from TFTP Servers easier. The utilities all run on Microsoft Windows 3.1 or higher. The following sections describe the Syslog, Telnet, VT-100, and TFTP Server utilities.

SYSLOG HOST DAEMON

The SysLog Host Daemon allows remote monitoring, collecting, and logging of ATLAS 810^{PLUS} events in realtime. This information can be useful during installation setups and/or troubleshooting.

To use this utility, you must configure the remote ATLAS 810^{PLUS} (using a Telnet or VT-100 connection) with destination IP address of the PC to which you want to transmit SysLog messages; i.e., the IP address of the PC running the SysLog host utility.

SysLog GUI

Figure 12-1 on page 12-2 shows the SysLog Host GUI. The conventional Menu Bar is described below beginning on page 12-3 (see also Figure 12-2). Other features are described here.

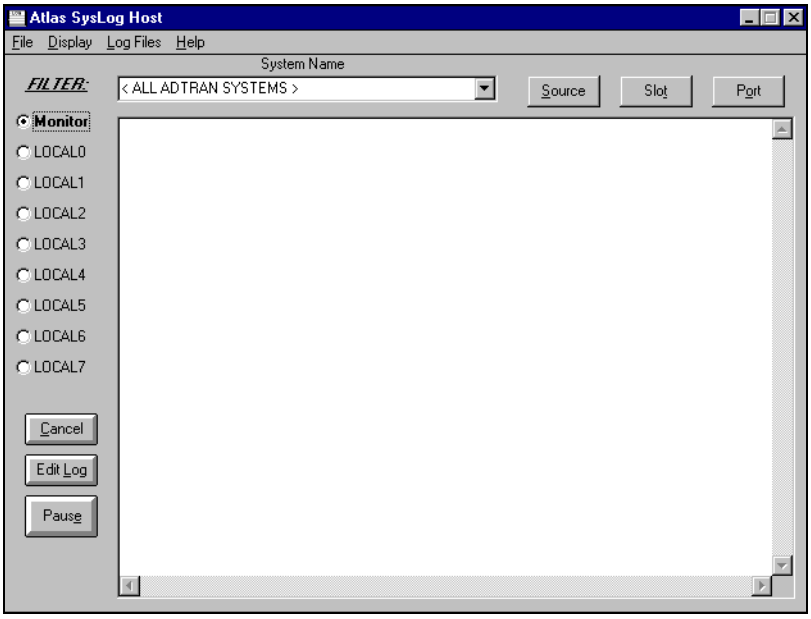
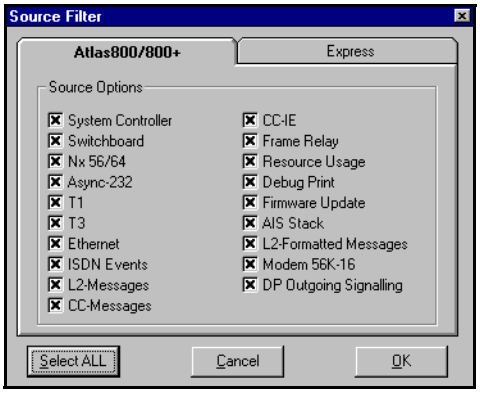


Figure 12-1. ATLAS SysLog Host GUI

Monitor

The **Monitor** feature allows all SysLog messages to be pre-filtered 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.

System Name	Select from pull-down menu.
Source	Provides various filter options for the ATLAS.
Slot	Select applicable slots (0—8).
Port	Select applicable port range.



Menu Bar

The SysLog Menu Bar provides common functions. The Menu Tree shown in Figure 12-2 shows the structure.

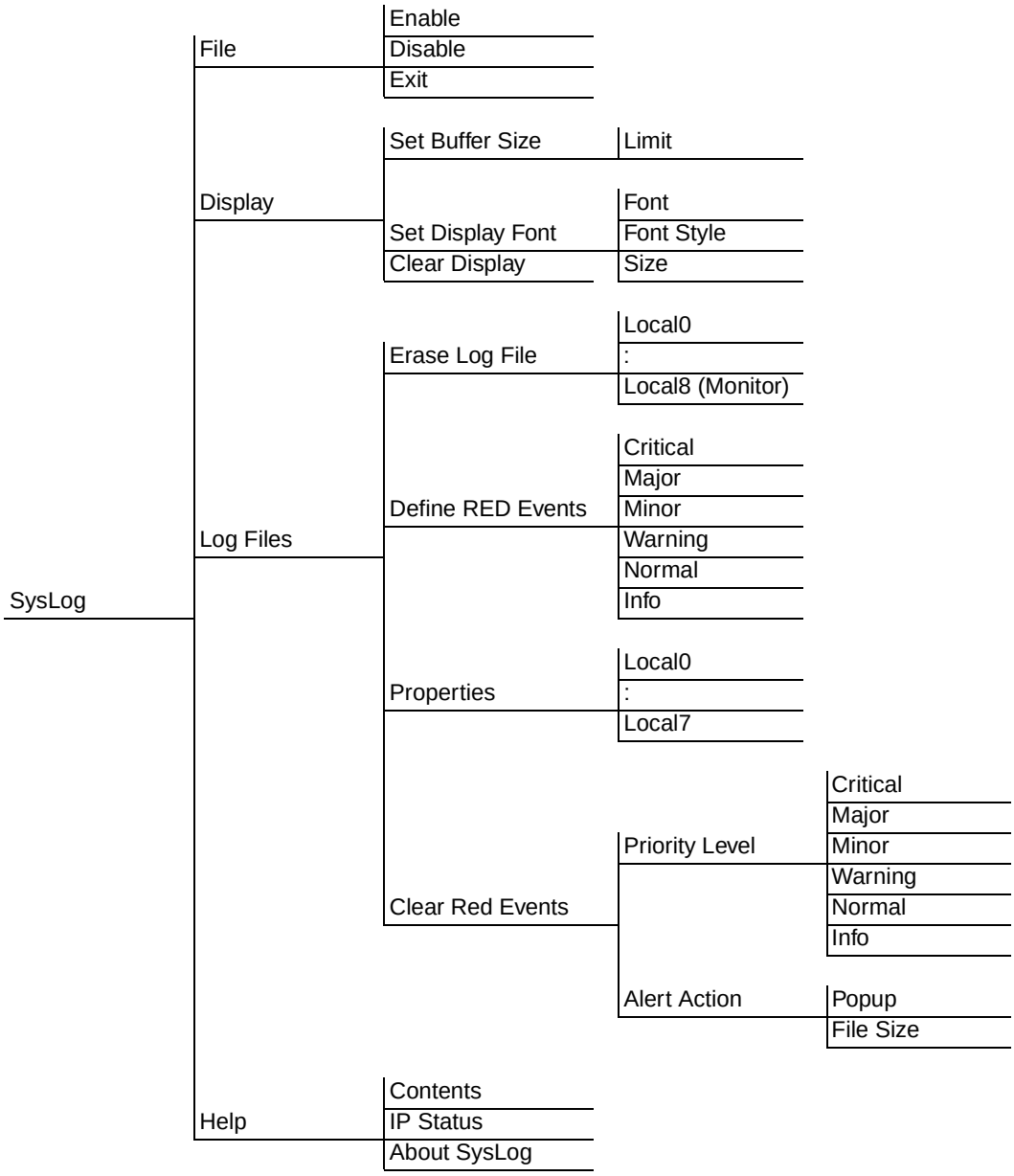


Figure 12-2. SysLog Menu Tree for the Menu Bar

> FILE

Enables, disables, and exits the SysLog Host program.

> DISPLAY

Sets the buffer size and display font. Also, clears the display.

> LOG FILES

Erases log files, defines Red events, sets priorities and action to be taken when an event occurs, and clears Red events. (See *Define RED Events* on page 12-4.)

» Erase Log Files

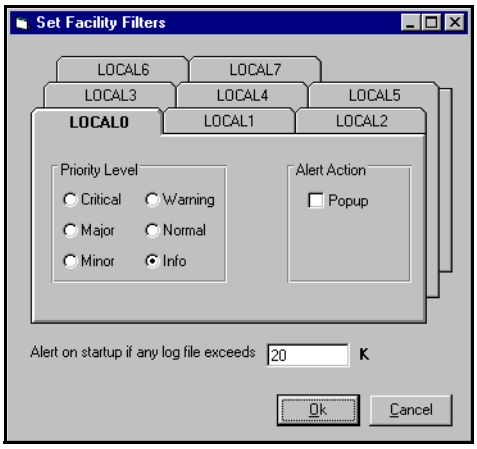
The SysLog utility, by default, stores all messages of a certain priority in a specified local log file or facility. These files are named LOCAL0.txt, LOCAL1.txt, LOCAL2.TXT, and so on. To erase the file, click on this menu.

» Define RED Events

The red events feature allows the user to predefine a message priority condition so that if the condition occurs, the file is highlighted in red. In the figure shown here, any LOCAL0 through LOCAL7 facility becomes highlighted in red if a **Critical**, **Major** or **Minor** message is received. This feature allows a user to quickly locate problem units during troubleshooting.

» Properties

When you click on **Properties**, the **Set Facility Filters** dialog box opens, allowing you to specify what types of messages will be logged to an ASCII text file. In the example shown in here, all SysLog event messages of **Normal** and above (i.e., **Critical, Major, Minor** and **Warning**) will be logged. **Info** (debug) messages will be blocked. In this example, if the log file exceeds 20K, SysLog alerts the user on startup to this fact. Also, from this box, you can set the alert action.



» Clear Red Events

Click this item to clear all predefined red events.

> HELP

Opens the help files, reports on the IP status, and provides information on SysLog version number.

TELNET UTILITY

The Telnet utility delivered with the ATLAS 810^{PLUS} provides enhancements to standard Telnet programs that make it easier to work with ATLAS 810^{PLUS} options.

Access the Telnet program remotely through the 10BaseT Ethernet port. For a detailed description of how to work with the Telnet program, refer to *Navigating the Terminal Menu* on page 5-1, and for a detailed description of the Telnet interface, see Figure 5-1 on page 5-1. If you need help setting up the

ATLAS 810^{PLUS} for a Telnet session, refer to *Using The Terminal Menu* on page 3-1.

The Telnet menus include **Session**, **Edit**, **Options**, **Capture**, and **Help** (see the menu tree in Figure 12-3).

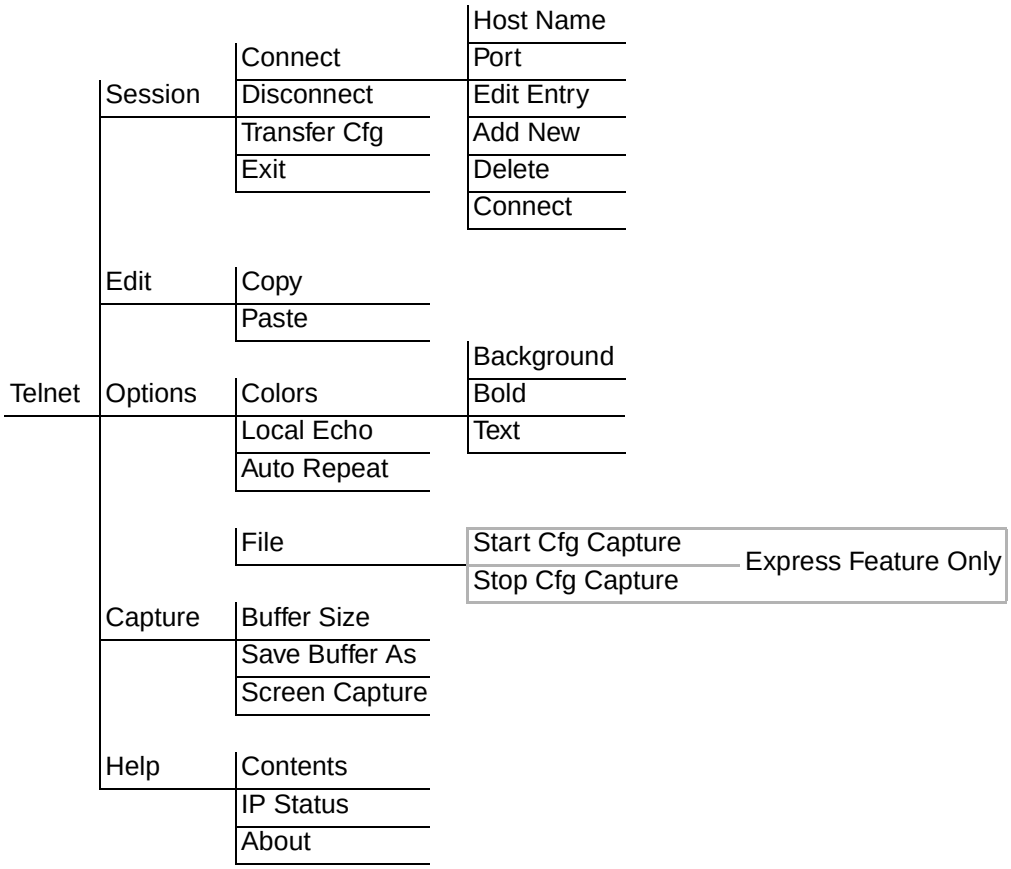
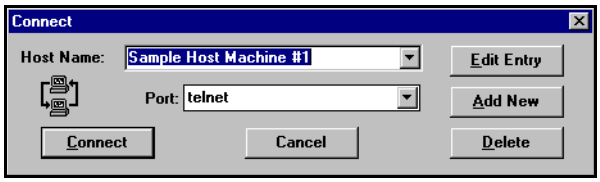


Figure 12-3. Telnet Menu Tree

> SESSION MENU

Click on **Session** to open the Telnet session.

» Connect



Opens dialog box for setting **Host Name** and **Port** parameters for a Telnet session. Also lets you **Edit Entry**, **Add New** entry, and **Delete** stored entries. When the parameters are set, click **Connect** to make the connection. Click **Cancel** to end the session.

»» Host Name

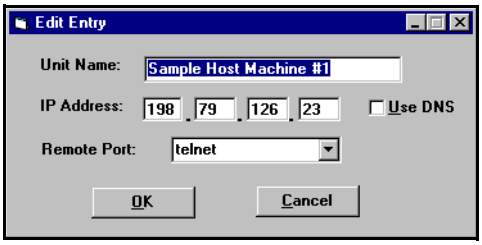
Accepts and stores host names. You may either enter a name, an IP address, or a domain name directly from this field. Click on the drop-down arrow to display a complete list of previously stored host names.

»» Port

Provides several port options. You may enter port numbers directly into this field to connect to non-standard ports or select the drop-down combo-box to display the following options:

Telnet	Establishes a Telnet session
Echo	Provides a loopback for troubleshooting
Discard	Bit bucket; discards data
Daytime	Returns the time
Chargen	Displays as a unique character stream; used for self-tests

»» Edit Entry



Changes either the unit name or the IP address of each host. Press either **Tab, Return,** or a **period (.)** after each number in the IP address to move to the next field. If you press **Return** or **(.)** while the cursor is located in each IP field, that field entry is deleted.

»» Add New

Prompts you for the same information as the **Edit Entry** dialog box for new host. When enabled, the **Use DNS** (Domain Name Server) feature allows users to request **Domain Look Up** via a DNS server on the network, rather than specifying an IP address. The name then appears in the **Host Name** field.

»» Delete

Removes a host name from the list; simply select the host name you want to remove, and, at the prompt, click **Delete**.

»» Connect

Establishes the Telnet session.

» Disconnect

Terminates the Telnet session.

To re-establish the session, select **Connect** from **Session Menu** or press **Enter** three times. This action restores the previous connection.

» Transfer Cfg This feature is used with Express products primarily for sending configuration files to the unit.

» Exit Ends the Telnet session and closes the Telnet screen.

> EDIT MENU

Provides **Copy** and **Paste** commands.

> OPTIONS MENU

Provides viewing alternatives for the terminal screen.

» Colors Three options change the color of the background window (**BackGround**), bold highlights (**Bold**), and text (**Text**).

» Local Echo Echoes each character that you enter.

» AutoRepeat Repeats characters you select from the keyboard, if you hold down the key.

> CAPTURE MENU

Provides options for capturing screen images.

» File Sends screen options data to a file in the format options listed below:

»» Start Cfg Capture Used with the Express product line to start sending the scrolling screen capture to a file storage location.

»» Stop Cfg Capture Used with the Express 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 ATLAS.) This number represents the number of lines to capture in the memory buffer.

» Save Buffer As Save screen capture to a file.

» Screen Capture Copies the text on the current Telnet screen to the clipboard. You can open any word processor and paste the clipboard contents into the program. This option is helpful when debugging.

> HELP MENU

Provides on-line help for using the ADTRAN Utilities.

» Contents Opens the on-line help.

» IP Status Displays the local port address and the status of the connection.

» About Displays version and owner information.

VT-100 UTILITY

Use the VT-100 to configure an ATLAS 810^{PLUS} which is directly connected to a PC. The VT-100 display is almost identical to the Telnet display.

For a detailed description of how to work with the Telnet program, refer to *Navigating the Terminal Menu* on page 5-1, and for a detailed description of the VT-100 interface, see *VT-100 Utility* on page 12-8. If you need help setting up the ATLAS 810^{PLUS} for a VT-100 session, refer to *Using VT-100 Terminal Emulation* on page 3-1.

VT-100 menus include **Session**, **Edit**, **Port**, **Options**, **Capture**, and **Help** (see the menu tree in Figure 12-4).

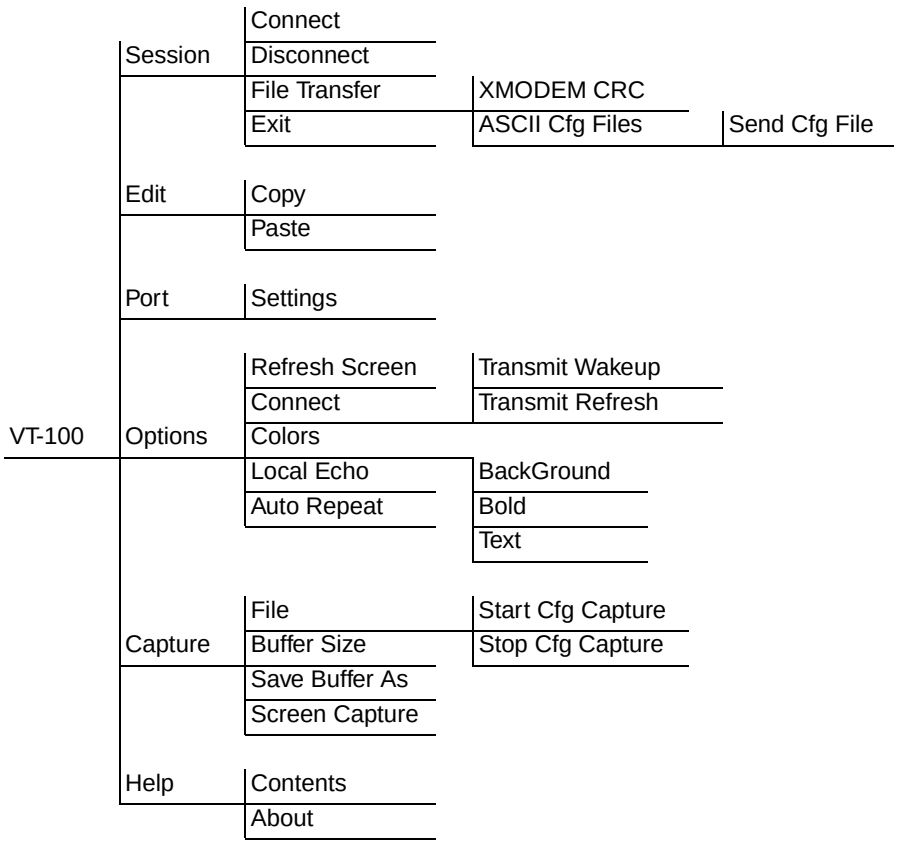


Figure 12-4. VT-100 Menu Tree

> SESSION MENU

Opens VT-100 terminal emulation session.

» Connect

Opens a specified serial port for a VT-100 session.

» Disconnect

Closes a specified serial port at the end of a VT-100 session.

» File Transfer

Uploads and downloads files to and from an ATLAS.

»» XMODEM CRC Selects the XMODEM file transfer protocol.

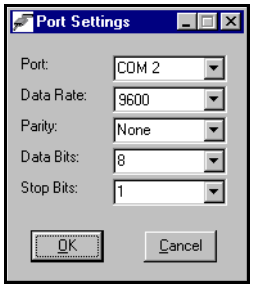
»» ASCII Cfg Files Selects ASCII transfer mode. Primarily useful for configuration transfers for the Express products.

> EDIT MENU

Identical to the Telnet **Edit Menu** (see *Edit Menu* on page 12-7).

> 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 ATLAS Control Port online in terminal mode.

»» Transmit Refresh Provides a control sequence to automatically refresh the screen when connecting. (This is the default setting for the ATLAS.)

» Colors Identical to Telnet **Colors Menu** (see *Colors* on page 12-7).

» 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 12-7).

> HELP MENU

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

» Contents Opens on-line help.

» About Displays version and owner information.

TFTP SERVER

The TFTP Server utility transfers ATLAS 810^{PLUS} configuration files to and from a TFTP Server. You can install this program on a PC running any version of Microsoft Windows. The configuration of an ATLAS 810^{PLUS} can be saved offline as a backup file. The saved file may also be used to send the same configuration to multiple ATLAS 810^{PLUS} units. Transfer configuration files using the TFTP protocol (a TCP / IP user protocol) via the 10BaseT Ethernet port. The ATLAS 810^{PLUS} must have a valid IP address, subnet mask, and default gateway (if required), and be connected to an Ethernet network before proceeding. Figure 12-6 shows the TFTP Server interface.

NOTE

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

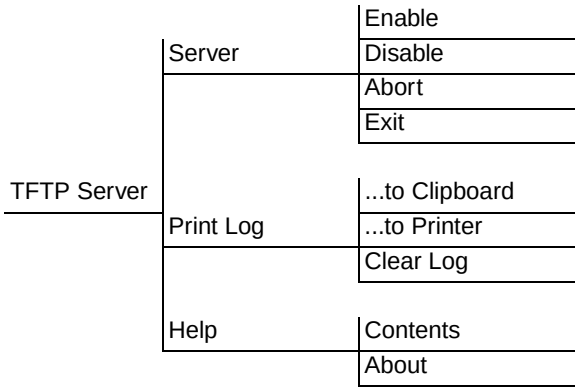


Figure 12-5. TFTP Server Interface Menu Tree

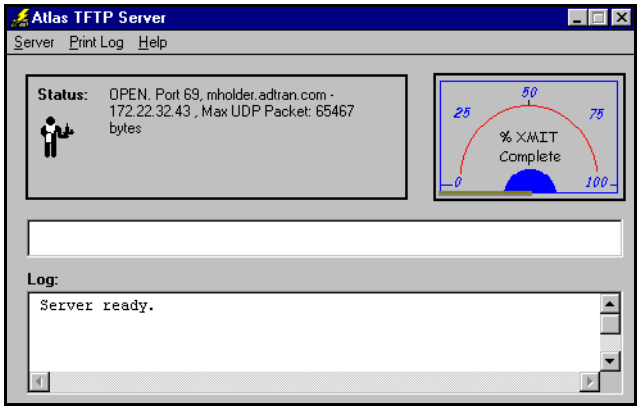


Figure 12-6. TFTP Server Interface

Only one configuration transfer session (upload or download) may be active at a time. The TCP/IP parameters are not saved or overwritten as part of an ATLAS 810*PLUS* unit's transferred configuration to allow sending identical configurations to multiple units. When you start this program, a port is automatically opened.

> SERVER MENU Provides enable, disable, abort, and exit options.

» Enable Enables the TFTP Server. The IP address displays in the Status field and Server Ready displays in the Log field.

» Disable Disables the TFTP Server. When you select this option, the message PORT CLOSED displays in the Status field and Port Closed displays in the Log field.

» Abort Terminates a transfer that is in progress.

» Exit Terminates active transfers and closes the TFTP window.

> PRINT LOG Provides print options.

» ...to Clipboard Copies the information in the Log field to the clipboard. You can then open any word processor and paste the information into the program for review.

» ...to Printer Sends the information in the Log field to the default printer.

» Clear Log Deletes the information stored in the Log field.

> HELP Provides on-line help and version information.

» Contents Opens on-line help.

» About Displays version and owner information.

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.

METER FIELD

The **XMIT** meter provides a visual record of the transfer process.

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, from the **Print Log** menu, select **Clear Log**. Save this information to a file before deleting it with the **...to Clipboard** command.

Saving the Current Configuration to a TFTP Server

Before trying to save a configuration, ensure that the TFTP Server is running. If you are using the ADTRAN TFTP Server program, the server automatically enables when you start the program. Also, please note the following:

- A level 3 or better password is required for a configuration download—the same level required to modify most configuration parameters. Please consult the ATLAS administrator if level 3 access is not available.
- Some TFTP Servers constrain filename formats. For example, a TFTP Server running on a PC under any platform may only permit 8.3 format filenames (8 characters, period, and three extension characters).

To save the current configuration, follow these steps:

Step	Action
1	Use Telnet and **log in** to the ATLAS 810*PLUS* for which you want to save the configuration file.
2	Select the **System Utility** menu, then the **Config Transfer** menu.
3	Set the TFTP Server IP Address to the IP address of the machine running the TFTP Server program. (If you are using the ADTRAN TFTP Server, the IP address displays in the Status field.)
4	Change the TFTP Server filename to a unique filename for saving the configuration file to the remote server. (Enter the complete directory path to the file.)
5	Move to the **Save Config Remotely** button and press **Enter**. Press **Y** to confirm the transfer request.

Successful Transfer

The **Previous Transfer Status** field indicates success or failure of the transfer. If successful, the field reads **TFTP Download Complete**, and the **Current Transfer Status** field displays **Idle**. The file is now present on the TFTP Server. (For the ADTRAN TFTP Server, it is stored in the installation directory or the directory you specified.)

> **WARNING**
>
> *TFTP is **not** secure. No passwords are required for client access. Anyone can access files through the IP port on the server machine if they know the target file's name. For security purposes, close this utility as soon as you have finished using it.*

Unsuccessful Transfer

There are various reasons why a configuration download may fail. For example, the server may not allow the specific filename to be created or overwritten, the specified directory path may not be valid, or there may not be sufficient disk space on the remote server for the new file (although configuration files are not normally large). A specific error message displays when the transfer is unsuccessful.

Also, a TFTP Server may not be available at the configured IP address. If the TFTP Server cannot be contacted, the download attempt will timeout in approximately 20 seconds. Remember to direct transferred files to the Application directory.

Retrieving the Configuration from a TFTP Server

Before trying to retrieve the configuration, ensure that a TFTP Server is running on a remote machine. If you are running the ADTRAN TFTP Server program, the server is automatically enabled when you start the program.

Also, a level 3 or better password is required for performing a configuration upload. Please consult the ATLAS administrator if level 3 access is not available.

Instructions for Retrieving a Configuration from TFTP Server	
Step	**Action**
1	Use Telnet to **log in** to the ATLAS 810^{PLUS} to which you want to upload a configuration file.
2	Select the **System Utility** menu, then the **Config Transfer** menu.
3	Set the TFTP Server IP Address to the IP address of the machine running the TFTP Server program. (If you are using the ADTRAN TFTP Server, the IP address displays in the Status field.)
4	Change the TFTP Server filename to the filename of a previously saved configuration you wish to load. (Enter the complete directory path to the file.)
5	Move to the **Load And Use Config** button and press **Enter** to proceed with the transfer. Respond with **Y** to confirm the transfer request.

WARNING *The ATLAS 810^{PLUS} reboots immediately after a configuration successfully loads. No additional confirmation is requested, and any online sessions are terminated.*

The **Current Transfer Status** field indicates the transfer progress. If the upload succeeds, the unit automatically reboots and runs using the new configuration. If the upload fails, an error message displays in the **Previous Transfer Status** field. If the TFTP Server cannot be contacted, the transfer attempt times out in approximately 20 seconds.

Appendix A System Event Logging

This appendix describes the entries that may be logged by the system event log. Of particular importance is the log event's Category – this is the minimum severity level that must be set in order that the event be logged.

Use caution when changing Categories from their default levels. If too many sources have their Category values set too low, the number of messages being logged in a given period can be very large. If too many messages are being logged too rapidly, system performance can be adversely affected.

Most of the events discussed in the following tables are used primarily during troubleshooting and should be turned off in normal operation:

Table A-1. System Event

Event	Category	Console Log String
ATLAS configuration file loaded into the system and activated	Critical	System Configuration Uploaded
Console login failure[a]	Minor	Login Failure
Internal system temperature has returned to normal	Critical	Internal Temperature Warning Cleared
Internal system temperature is too high	Critical	Internal Temperature Warning
Module found	Info	Module Found
Module removed or not responding	Warning	Module Not Responding
Primary power supply is present but is not operating properly	Critical	Main Power Supply Failure
SNMP authentication failure[b]	Info	SNMP Authentication Failure
System cold start[c]	Normal	Cold
The backup power supply is operating properly or has been removed	Critical	Backup Power Supply Failure Cleared
The backup power supply is present but is not operating properly	Critical	Backup Power Supply Failure
The primary power supply is operating properly or has been removed	Critical	Main Power Supply Failure Cleared

a. Three consecutive login attempts were attempted and failed.

b. Generated if the ATLAS receives an SNMP request from an SNMP manager defined in the ATLAS SNMP communities list but with a community name that does not match the community name defined in the SNMP communities list.

c. Generated five seconds after the completion of system initialization.

Table A-2. Switchboard Events

Event	Category	Console Log String
Call rejected[a]	Warning	<number> rejected: No such number
Call rejected[b]	Normal	<number> rejected: Outgoing reject list
Call rejected[c]	Normal	<number> rejected: Busy
Call successfully routed	Normal	<number> accepted: <slot> <port>

a. No such number in dial plan.

b. Number is on outgoing reject list.

c. All endpoints busy.

Table A-3. Nx 56/64 Events

Event	Category	Console Log String
511 Test Pattern Activated	Warning	Nx 56/64 511 Test Pattern Active
511 Test Pattern Deactivated	Warning	Nx 56/64 511 Test Pattern Cleared
Bilateral Loopback Activated	Warning	Nx 56/64 Bilateral Loopback Active
Bilateral Loopback Deactivated	Warning	Nx 56/64 Bilateral Loopback Cleared
Clock Slip Alarm Active	Major	Nx 56/64 Clock Slip Alarm Active
Clock Slip Alarm Cleared	Major	Nx 56/64 Clock Slip Alarm Cleared
CTS Asserted	Information	Nx 56/64 CTS Asserted
CTS Dropped	Information	Nx 56/64 CTS Dropped
DCD Asserted	Information	Nx 56/64 DCD Asserted
DCD Dropped	Information	Nx 56/64 DCD Dropped
DTR Asserted	Information	Nx 56/64 DTR Asserted
DTR Dropped	Information	Nx 56/64 DTR Dropped
Excessive Zeros condition cleared	Warning	Nx 56/64 Excessive Zeros Alarm Cleared
Excessive Zeros from DTE	Warning	Nx 56/64 Excessive Zeros Alarm
External Clock Alarm	Major	Nx 56/64 External Clock Alarm Active
External Clock Alarm Cleared	Major	Nx 56/64 External Clock Alarm Cleared
Pll Alarm Active	Major	Nx 56/64 PLL Alarm Active
Pll Alarm Cleared	Major	Nx 56/64 PLL Alarm Cleared
RTS Asserted	Information	Nx 56/64 RTS Asserted
RTS Dropped	Information	Nx 56/64 RTS Dropped

Table A-4. Time Events

Event	Category	Console Log String
Blue Alarm Cleared	Major	T1 Blue Alarm Cleared
Blue Alarm Set	Major	T1 Blue Alarm Active
Current T1 Controlled Slip Seconds Threshold Exceeded	Warning	T1 Curr CSS Thrs Exceeded
Current T1 Errored Seconds Threshold Exceeded	Warning	T1 Curr ES Thrs Exceeded
Current T1 Line Code Violations Threshold Exceeded	Warning	T1 Curr LCV Thrs Exceeded
Current T1 Line Errored Seconds Threshold Exceeded	Warning	T1 Curr LES Thrs Exceeded
Current T1 Path Code Violations Threshold Exceeded	Warning	T1 Curr PCV Thrs Exceeded
Current T1 Severely Errored Framing Seconds Threshold Exceeded	Warning	T1 Curr SEFS Thrs Exceeded
Current T1 Severely Errored Seconds Threshold Exceeded	Warning	T1 Curr SES Thrs Exceeded
Current T1 Unavailable Seconds Threshold Exceeded	Warning	T1 Curr UAS Thrs Exceeded
D Channel Alarm Cleared	Major	T1 D Channel Alarm Cleared
D Channel Alarm Set	Major	T1 D Channel Alarm Active
Line Loopback Active	Warning	T1 Line Loopback Active
Loopback Cleared	Warning	T1 Loopback Cleared
LOS Alarm Cleared	Major	T1 LOS Cleared
LOS Alarm Set	Major	T1 LOS Active
Payload Loopback Active	Warning	T1 Payload Loopback Active
Red Alarm Cleared	Major	T1 Red Alarm Cleared
Red Alarm Set	Major	T1 Red Alarm Active
Total T1 Controlled Slip Seconds Threshold Exceeded	Warning	T1 Total CSS Thrs Exceeded
Total T1 Errored Seconds Threshold Exceeded	Warning	T1 Tot ES Thrs Exceeded
Total T1 Line Code Violations Threshold Exceeded	Warning	T1 Total LCV Thrs Exceeded
Total T1 Line Errored Seconds Threshold Exceeded	Warning	T1 Total LES Thrs Exceeded
Total T1 Path Code Violations Threshold Exceeded	Warning	T1 Total PCV Thrs Exceeded
Total T1 Severely Errored Framing Seconds Threshold Exceeded	Warning	T1 Total SEFS Thrs Exceeded
Total T1 Severely Errored Seconds Threshold Exceeded	Warning	T1 Total SES Thrs Exceeded
Total T1 Unavailable Seconds Threshold Exceeded	Warning	T1 Total UAS Thrs Exceeded
Tx Blue Alarm Cleared	Major	T1 Tx Blue Alarm Cleared

Table A-4. Time Events *(Continued)*

Event	Category	Console Log String
Tx Blue Alarm Set	Major	T1 Tx Blue Alarm Active
Tx Yellow Alarm Cleared	Major	T1 Tx Yellow Alarm Cleared
Tx Yellow Alarm Set	Major	T1 Tx Yellow Alarm Active
Yellow Alarm Cleared	Major	T1 Yellow Alarm Cleared
Yellow Alarm Set	Major	T1 Yellow Alarm Active

Table A-5. Ethernet Events

Event	Category	Console Log String
Not enough memory for Ethernet driver	Critical	No memory for driver structure

Table A-6. ISDN Events

Event	Category	Console Log String
BRI LT configuration successful	Normal	Configured BRI as LT
BRI NT configuration successful	Normal	Configured BRI as NT
Call busy	Information	Call to <called number> declared busy after leaving ATLAS
Call busy	Information	Call to <called number> refused: Busy
Call cleared	Information	Call to <called number> cleared from ATLAS end
Call connected	Information	Call to <called number> connected
Call disconnected	Information	Call to <called number> disconnected by far end
Call not accepted	Information	Call not accepted to <called number>: No channel available
Call received	Information	Call to ATLAS: <called number> received
Call Rejected	Normal	Rejected an incoming call for an unregistered SPID
Call ringing	Information	Call to <called number> ringing
D Channel Down	Major	D channel is DOWN
D Channel Up	Normal	D channel is UP
Dialing number	Information	Dialing <called number>
Incoming call accepted	Information	Incoming call to <called number> accepted
Incoming call refused	Information	Incoming call to <called number> refused

Table A-6. ISDN Events *(Continued)*

Event	Category	Console Log String
Incorrectly formatted IE	Major	<message>: Incorrectly formatted cause IE
ISDN line released	Normal	Released: No longer an ISDN line
No B channels for call	Normal	No outgoing B channel available for call to <number>
No BRI resources available	Critical	BRI configuration failed: No ISDN resources are available
No Matching SPID found	Warning	No SPID matches the call profile: <called number> <call type>
No Matching SPID found	Warning	No SPID with free B channels matches call type: <call type>
No PRI resources available	Critical	PRI configuration failed: No ISDN resources are available
PRI CO configuration successful	Normal	Configured PRI as central office emulator
PRI CPE configuration successful	Normal	Configured PRI as CPE
SPID Failed	Major	BRI NT: Spid <spid> was rejected
SPID Negotiation failed	Major	BRI NT: SPID Negotiations failed - resetting the link
SPID registered	Normal	BRI NT: Spid <spid> registered
SPID Registration complete	Normal	BRI LT: All SPIDs registered
SPID Registration complete	Normal	BRI NT: All SPIDs registered
SPID Registration in progress	Normal	BRI LT: Registering SPID <spid>
SPID Registration in progress	Normal	BRI NT Registering SPID <spid>
SPID Retry in progress	Minor	BRI NT: SPID Negotiations failed - Retrying
SPID Unregistration attempted	Warning	LT: Tried to call unregistered SPID <spid>
Unknown SPID received	Major	BRI LT: SPID <spid> received - NOT IN LIST

ISDN CAUSE CODES

In addition to the above events, certain recognized ISDN cause codes are sent to the event log from the ISDN message facility. Table A-7 lists the codes applicable to the ATLAS 810^{PLUS} and the minimum category required for logging the cause code event.

Table A-7. ISDN Cause Code Events

Cause Code Event	Category	Code
ACCESS_INFO_DISCARDED	Warning	43
BAD_INFO_ELEM	Major	99
BEAR_CAP_NOT_AVAIL	Minor	58
CALL_REJECTED	Information	21
CAP_NOT_IMPLEMENTED	Minor	65
CHAN_DOES_NOT_EXIST	Major	82
CHAN_NOT_IMPLEMENTED	Minor	66
CHANNEL_UNACCEPTABLE	Information	6
DEST_OUT_OF_ORDER	Information	27
FACILITY_NOT_IMPLEMENTED	Major	69
FACILITY_NOT_SUBSCRIBED	Minor	50
FACILITY_REJECTED	Information	29
INCOMING_CALL_BARRED	Minor	54
INCOMPATIBLE_DEST	Major	88
INTERWORKING_UNSPEC	Major	127
INVALID_CALL_REF	Major	81
INVALID_ELEM_CONTENTS	Major	100
INVALID_MSG_UNSPEC	Major	95
INVALID_NUMBER_FORMAT	Information	28
MANDATORY_IE_LEN_ERR	Major	103
MANDATORY_IE_MISSING	Major	96
NETWORK_CONGESTION	Warning	42
NETWORK_OUT_OF_ORDER	Warning	38
NO_CIRCUIT_AVAILABLE	Warning	34
NO_ROUTE	Information	2
NO_USER_RESPONDING	Information	18
NONEXISTENT_MSG	Major	97
NORMAL_CLEARING	Information	16
NUMBER_CHANGED	Information	22
OUTGOING_CALL_BARRED	Minor	52

Table A-7. ISDN Cause Code Events *(Continued)*

Cause Code Event	Category	Code
PRE_EMPTED	Warning	45
PROTOCOL_ERROR	Major	111
REQ_CHANNEL_NOT_AVAIL	Warning	44
RESP_TO_STAT_ENQ	Information	30
SERVICE_NOT_AVAIL	Minor	63
TEMPORARY_FAILURE	Warning	41
TIMER_EXPIRY	Major	102
UNASSIGNED_NUMBER	Information	1
UNSPECIFIED_CAUSE	Information	31
USER_BUSY	Information	17
WRONG_MESSAGE	Major	98
WRONG_MSG_FOR_STATE	Major	101

CAUSE CODE LOG ENTRIES

Cause Code IEs that are non-Q.931 (i.e., the Coding Standard field is not 0) are logged with the following format:

<message> : <coding standard> code <cause code>

The coding standard field is one of the following: Reserved, National, or Local. Each Cause Code IE log entry ends with a location designation. Table A-8 shows these designations.

Table A-8. Cause Code Log Entry Location Designations

Code	Location
IN0TL	International network
INWK	Network beyond internetworking point
LN	Public network serving the local user
LPN	Private network serving the local user
RLN	Public network serving the remote user
RPN	Private network serving the remote user
TN	Transit network
U	User

Table A-9. ISDN L2 Messages

Event	Category	Console Log String
ISDN Layer 2 (LAPD) Message[a]	Information	<message contents>

a. Provides a hex dump of the entire LAPD frame.

Table A-10. ISDN Call Control Messages

Event	Category	Console Log String
ISDN Call Control Messages	Information	Host>>CC <tag><call ID> <message>
ISDN Call Control Messages	Information	CC>>Host <tag><call ID> <message>

Table A-11. Source: ISDN Information Elements

Event	Category	Console Log String
ISDN Information Element[a]	Information	<message contents>

a. Provides a hex dump of the ISDN IE sent with a call control message.

Appendix B Troubleshooting

Power-up Self Test Fails

Modules seated improperly, module failure

Remove all modules and cycle power to the unit. If self test still fails, call Technical Support and report the results. If the self test now passes, re-insert modules one at a time, running the self test after installing each module. When an installed module causes the self test to fail, note it and report results to tech support.

System Timing Source Unlocked

(Displayed on Terminal Interface, “System Status”)

Selected Timing Source is not present or clock is out of tolerance

- Verify that system timing is correctly configured for the desired clock.
- Verify that the interface cable to clock source is present.
- Temporarily configure the system to operate off of internal timing. Verify that the system can lock to this clock.

Cannot establish Telnet session with ATLAS

Max Telnet sessions set to 0, IP address of ATLAS does not match remote host IP address

- Verify that the Ethernet connection is in place, check IP addresses programmed in ATLAS and in the Telnet client, verify that session timeout value is not set too low.
- Check for ethernet port activity on the front panel. Make sure the link is up, and data is being transmitted and received.

Cannot pass data from T1 interface to V.35 port

Misconfiguration, improper cabling

- Verify that the T1 signal is being received. If not, check that the cabling is correct.
- Verify that the T1 is being received without errors. If not, double-check that framing and coding are set properly.
- Verify that desired dedicated map is active.
- Verify that bandwidth is mapped to the correct V.35 port.
- Verify that the V.35 port is set to the correct data rate (terminal interface).
- Check T1 performance using the terminal interface; if excessive errors, report fault to the Telco.
- Verify proper state of DTE signals via the terminal interface or the LCD front panel.

Switched calls are not working

Misconfiguration

- Verify that the end point has proper call accept / reject criteria. For RBS applications, check signaling bit status on the terminal interface for proper operation.
- Verify that the end point is set up for correct signaling.

Cannot communicate with ATLAS USING VT-100 connected to the Control/Chain In Port

Misconfiguration, improper cabling

- Verify that ATLAS is receiving commands (press keys on terminal and verify that the received byte count in the front panel increments).
- Check cabling, verify that the chain port rate matches that of the attached terminal; check chain port status leads on the front panel.

Appendix C Warranty and Technical Support Information

WARRANTY AND CUSTOMER SERVICE

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

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

For Service, RMA requests, or more information, see the following sections for the correct toll-free contact number.

PRODUCT SUPPORT INFORMATION

Pre-sales Inquiries and Applications Support

Please contact your local distributor, ADTRAN Applications Engineering, or ADTRAN Sales:

Applications Engineering	(800) 615-1176
Sales	(800) 827-0807

Post-Sale Support

Please contact your local distributor first. If your local distributor cannot help, please contact ADTRAN Technical Support and have the unit serial number available.

Technical Support	(888) 4ADTRAN

Repair and Return

If ADTRAN Technical Support determines that a repair is needed, Technical Support will coordinate with the Customer and Product Service (CAPS) department to issue an RMA number. For information regarding equipment currently in house or possible fees associated with repair, contact CAPS directly at the following number:

CAPS Department (256) 963-8722

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

ADTRAN, Inc.
6767 Old Madison Pike
Progress Center
Building #6 Suite 690
Huntsville, Alabama 35807

RMA # _____

Appendix D Acronyms and Abbreviations

AMI	alternate mark inversion
ANI	automatic number identification
B8ZS	bipolar eight zero substitution
BRI	Basic Rate ISDN
bps	bits per second
CPE	customer premise equipment
CSU	channel service unit
CTS	Clear to send
DACS	Digital Access Cross-Connect System
DCE	data communications equipment
DNIS	dialed number identification service
DS0	digital service, level 0 (64 kbps)
DSU	data service unit
DTE	data terminal equipment
DTMF	dual tone multifrequency
ESF	extended superframe
FTP	File Transfer Protocol
ISDN	Integrated Services Digital Network.
kbps	kilobits per second
LAN	local area network
LCD	liquid crystal display
LED	light emitting diode
Mbps	Mega bits per second.
MIB	management information base
NT1	network termination 1
PBX	private branch exchange
PRI	Primary Rate ISDN
PSTN	public switched telephone network

SNMP	simple network management protocol
RBS	robbed bit signaling
TCP/IP	Transmission Control Protocol / Internet Protocol
TDM	time division multiplexing
TFTP	Trivial File Transfer Protocol
TSU	terminal service unit
WAN	wide area network

Appendix E Glossary

10BaseT Ethernet connection
The ATLAS 800 RJ-48C port that provides Ethernet LAN connection for TFTP, SNMP, and Telnet.

AMI
alternate mark inversion. A Layer 1 line code used in a T1 carrier. Zeros are transmitted as zero volts, and ones are transmitted as pulses that alternate polarity. Although B8ZS is an enhancement to AMI, B8ZS and AMI are normally referred to as mutually-exclusive options for a T1. (See also *B8ZS*.)

ANI
Automatic Number Identification. Service provided by a local phone company that provides incoming Caller ID information.

Async-232 Module
One of the ATLAS 800 option modules. The Aysnc-232 provides sixteen asynchronous EIA-232 DTE ports and serves as an interface between terminal servers and other DTE equipment.

ATLAS 810^{PLUS}
A bandwidth management system which functions as a central site multiplexer. (See also *Integrated Access System*.)

B8ZS
bipolar eight zero substitution. In a T1 carrier system, a specific eight bit pattern containing two deliberate bipolar violations which replaces eight consecutive customer zero bits. (See also *10BaseT Ethernet connection*.)

B channel
bearer channel. Bearer channels of an ISDN service carry provide data transmission. Compare with D channel.

bandwidth
The transmission capacity of a communications channel, stated in megabits per second (Mbps).

Basic Rate ISDN
See *BRI*.

bit
Bit is a contraction of the term binary digit. It is the smallest unit of information a computer can process representing either high or low, yes or no, or 1 or 0. It is the basic unit in data communications. A bit can have a value of zero (a mark) or one (a space).

bps
Bits per second. A measure of the speed of data communications.

byte
Eight bits of information composed of zeros or ones, one of which may include a parity bit.

BRI
Basic Rate ISDN. An ISDN service that offers two bearer (B) channels. One channel (64 kbps) is used for data transfer and as a data-link. The second channel (16 kbps) is used for signaling and control information.

clocking
An oscillator-generated signal that provides a timing reference for a transmission link. A clock provides signals used in a transmission system to control the timing of certain functions. The clock has two functions, (1) to generate periodic signals for synchronization and (2) to provide a time base.

CPE
Customer premise equipment. All telecommunications terminal equipment located on the customer premises, including telephone sets, private branch exchanges (PBXs), data terminals, and customer-owned coin-operated telephones.

CSU
channel service unit. A device that functions similarly to a modem except that the CSU works with digital signals rather than analog signaling.

CS
See CTS.

CTS
Clear to send. A signal on the DTE interface indicating that the DCE is clear to send data.

DACS
Digital Access Cross-Connect System. A system, such as the ATLAS 800, that assigns and redistributes (grooms) any DS0 on any T1 circuit to any other DS0 on any other T1 circuit in the system.

DCE
Data communications equipment. The part of a computer or data terminal that connects to a communications channel or network.

D channel
delta channel. Controls the operation of the ISDN connection.

dedicated bandwidth
Bandwidth which has been set aside (dedicated) for a specific number.

Dial plan
The numbering plan for ATLAS ports (user and network) handling switched connections. Individual dial plans contain phone number and features associated with DTMF dialing, PRI and BRI.

Digital Access Cross-Connect System
See *DACS*.

DNIS
Dialed Number Identification Service. Service provided by a telephone company that allows the caller to see what number has been dialed.

DS0
Digital signal (or service) having a transmission rate of 64 kbps intended to carry one voice channel (a phone call). Also called a fractional T1 because it bridges the gap between 56-kbps direct dial service (DDS) and a full T1 implementation (24 channels).

DSU
data service unit. A device used with a CSU to support digital communications by converting signals. (See also CSU.)

DTE
Data terminal equipment. The portion of a data terminal that interfaces to the end-user's equipment. The main difference between DCE and DTE is that pins 2 and 3 are reversed on the EIA-232.

DTMF dialing
dual tone multifrequency dialing. The tones used by customer equipment to signal the network.

E1 circuit
European equivalent to the T-1.

ESF
extended superframe. A method of grouping T1 carrier frames into larger superframes, each containing 24 consecutive T1 frames.

flash memory
A kind of non-volatile storage device, similar to EEPROM, where erasing can only be done in blocks or the entire chip.

flash upgrades
Upgrades that can be downloaded into the flash memory.

FTP
File Transfer Protocol. The TCP/IP protocol used to log in to a network, list files and directories, and transfer files.

hot swappable
A device is hot swappable if it can be installed without powering down the main unit.

Integrated Access System
A chassis-based product that supports a number of end-user applications on the subscriber side and a number of carrier interfaces on the trunk side. The ATLAS 800 is an Integrated Access System designed to provide significant wide-area cost savings through the consolidation of voice, data, fax, and video.

ISDN
Integrated Services Digital Network. A network architecture that enables end-to-end digital connections. The network supports diverse services through integrated access arrangements and defines a limited set of standard, multipurpose interfaces for equipment vendors, network providers, and customers. Interworking with a public switched telephone network is retained.

kbps
Kilobits per second. 1,000 bits per second.

LAN
local area network. Group of computers and peripheral devices connected by a communications channel, limited by distance.

LCD
liquid crystal display. Alphanumeric characters that appear in a display area as a result of light reflecting off a special crystalline substance.

leased line
A telecommunication facility or link reserved for the exclusive use of one customer. Also called a dedicated line.

local loop
In telephony the wire pair that connects a subscriber to a phone company end office, typically containing two wires. Four-wire local loops are common, however, especially with leased voice grade circuits.

loopback
A diagnostic procedure where data is sent to the device being tested, and the output of the device is fed directly back to its input, looped around, and the returning data is checked against that which was sent.

LED
light emitting diode. Alphanumeric characters that glow when supplied with a specified voltage.

Mbps
Mega bits per second. A measure of the amount of information travelling across a network or communications link.

MIB
management information base. The MIB is an index to the organized data stored within a network device.

Modem 16 Module
One of the ATLAS 800 option modules. The Modem 16 Module supports sixteen 56Kflex modem (analog) calls or sixteen ISDN connections.

multiplexer
(mux) A device that takes several low-speed channels and merges them into one high-speed channel at one end of a link. Another multiplexer at the other end of the link reverses this process.

NT1
Network termination 1. A unit that provides physical and electromagnetic termination of the U-interface, 2-wire transmission line; converts between Layer 1 formats used at the U- and T- reference points; and performs some maintenance functions.

nonvolatile memory
Any form of memory that retains its contents when power is removed (for example, ROM, EPROM, etc.)

Octal BRI/U Module
One of the ATLAS 810^{PLUS} option modules. The Octal BRI/U Module provides eight basic rate ISDN U interfaces, each capable of operating in NT or LT mode.

option modules
Any optional, hot-swappable module that can be added to the ATLAS 800 system for a variety of applications. See also

overbooking
ATLAS 810^{PLUS} feature that reduces telecommunications expenses by allowing you to over-subscribe switched bandwidth for situations where simultaneous access to the network by every subscriber is not required.

PBX
private branch exchange. A telephone system usually owned by the customer that serves a particular location. It provides connections from one phone extension to another and connects to the external telephone network.

PRI
Primary Rate ISDN. An ISDN service that provides 23 B (bearer) channels (64 kbps each) and 1 D (data) channel (64 kpbs). The combined capacities are equivalent to one T1 channel.

Quad Nx56/64 Module
(*Nx* is pronounced "en-by.") One of the ATLAS 800 option modules. The Quad Nx56/64 Module provides four synchronous V.35 DTE ports, each of which can operate at any rate that is a multiple of 56 or 64 kbps, up to 1.536 Mbps.

Quad T1/PRI Module
One of the ATLAS 810^{PLUS} option modules. The Quad T1/PRI Module provides four channelized T1 or Primary Rate ISDN (PRI) interfaces. Each interface can operate independently in DS-1 or DSX-1 mode, and any port can serve as the primary or backup timing source for the entire system.

Remote Access
The ability to connect to non-local communications equipment.

robbed bit signaling
A type of in-band signaling used with voice transmissions for multiplexing multiple voice circuits onto a T1.

SNMP
Simple Network Management Protocol. A control and reporting scheme widely used to manage devices from different vendors. SNMP operates on top of the Internet protocol.

synchronous
1.The condition occurring when two events happen in a specific time relationship with each other, both under control of a master clock.

2 A method of data transmission requiring the transmission of timing pulses to keep the sender and receiver synchronized in their communication used to send blocks of information. Synchronous data transmission is used in high speed data circuits because there is less overhead than asynchronous transmission of characters which contain two extra bits per character to affect timing.

T1 circuit
Also T-1. A digital transmission link with a capacity of 1.544 Mbps. T1 uses two pairs of normal twisted wires. T1 normally can handle 24 voice conversations with each conversation being digitized at 64 kbps. With more advanced digital voice encoding techniques, it can handle more voice channels. T1 is a standard for digital transmission in North America.

T3 Module
One of the ATLAS 810^{PLUS} option modules. The T3 Module provides one or two channelized T3 interfaces.

TCP/IP
Transmission Control Protocol / Internet Protocol. A set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, and terminal emulation.

TDM
Time Division Multiplexing. A method for sending two or more signals over a common transmission path by assignment the path sequentially to each signal, each assignment being for a discrete time interval.

Telco
Telephone company.

Telnet
A terminal emulation protocol, part of the TCP / IP suite of protocols, that provides remote terminal-connection services. (See also *VT-100*.)

TFTP
Trivial File Transfer Protocol. A simplified version of the TCP / IP file transfer protocol that does not include password protection or user-directory capability.

trunk
A direct line between two telephone switching centers.

TSU
terminal service unit.

T-Watch PRO
The ADTRAN Microsoft Widows-based management software program designed to control TSU units from a remote PC. It also provides limited control over the configuration of the ATLAS 800 using a graphical user interface.

VT-100
A non-intelligent terminal or terminal emulation mode used for asynchronous communications. Used to configure the ADTRAN ATLAS 810^{PLUS}.

WAN
wide area network. A network that connects users across large distances.

XMODEM

An error-correcting file transfer, data transmission protocol used to transmit files between PCs. The XMODEM protocol sends information in 128 byte blocks of data. Some sums (check sums) are done on each block and the result is sent along with the block. If the result does not check out at the other end, the computer at the other end sends a request (a NAK - negative acknowledgment) to retransmit that block again). If the block checks out, the computer sends ACK (an acknowledgment). In this way, relatively error-free transmissions can be accomplished.

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

Product Support Information

Presales Inquiries and Applications Support

Please contact your local distributor, ADTRAN Applications Engineering, or ADTRAN Sales:

Applications Engineering	(800) 615-1176
Sales	(800) 827-0807

Post-Sale Support

Please contact your local distributor first. If your local distributor cannot help, please contact ADTRAN Technical Support and have the unit serial number available.

Technical Support	(888) 4ADTRAN

Repair and Return

If ADTRAN Technical Support determines that a repair is needed, Technical Support will coordinate with the Custom and Product Service (CAPS) department to issue an RMA number. For information regarding equipment currently in house or possible fees associated with repair, contact CAPS directly at the following number:

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
6767 Old Madison Pike
Building #6 Suite 690
Huntsville, Alabama 35807

RMA # _____