



ATLAS 800^{PLUS}
USER MANUAL

Part Number 1200226L1

TRADEMARKS:

Windows is a registered trademark of Microsoft Corporation.

DMS 100 is a registered trademark of Northern Telecom.

5ESS is a registered trademark of Lucent.

Lucent Technologies is a registered trademark.



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

© 1998 ADTRAN, Inc.
All Rights Reserved.
Printed in U.S.A.

ABOUT THIS MANUAL

The ATLAS 800^{PLUS} system consists of the Base Unit and one or more modules. Each ATLAS 800^{PLUS} option module includes its own User Manual, containing specific information about installing, configuring, and testing the module.

This manual includes information you need to install, configure, test, and troubleshoot an ATLAS 800^{PLUS} system, often referring you to the individual module manual when applicable.

This manual is arranged so you can quickly and easily find the information you need. The following is an overview of the contents of this manual:

Introduction

- Chapter 1, *Introduction* on page 1-1, familiarizes you with the ATLAS 800^{PLUS} unit and provides some sample ATLAS 800^{PLUS} applications.

Getting Started

- Chapter 2, *Installation* on page 2-1, describes the rear panel layout and how to install the ATLAS 800^{PLUS}.
- Chapter 3, *Operation* on page 3-1, describes the front panel layout and the different ways to operate the ATLAS 800^{PLUS}.

Reference Information

- Chapter 4, *Front Panel Operation and Menu Structure* on page 4-1, describes how to navigate the front panel. This chapter also describes each option accessible through the front panel.
- Chapter 5, *Using the Terminal Menu* on page 5-1, describes how to navigate the terminal menus. This chapter also describes each option you can access through the terminal menus.

Working with the ATLAS 800^{PLUS}

- Chapter 6, *Creating a Dedicated Map* on page 6-1, provides step-by-step instruction on how to use the Dedicated Map commands.
- Chapter 7, *Creating a Dial Plan* on page 7-1, provides step-by-step instructions on how to create a dial plan for ATLAS.
- Chapter 8, *Updating Firmware* on page 8-1, provides step-by-step instruction on how to update the ATLAS 800^{PLUS} firmware.
- Chapter 9, *SNMP Management* on page 9-1, describes how to control the ATLAS 800^{PLUS} via SNMP.
- Chapter 10, *ADTRAN Utilities* on page 10-1, describes the Telnet, VT 100, and TFTP Server programs delivered with ATLAS 800^{PLUS}.

Appendices

- Appendix A, *System Event Logging* on page A-1, describes the events ATLAS 800^{PLUS} monitors.
- Appendix B, *Troubleshooting* on page B-1 describes how to diagnose different problems you may experience with the ATLAS 800^{PLUS}.
- Appendix C, *Warranty and Technical Support Information* on page C-1, describes your warranty and how to contact technical support.

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

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 and modular plug are 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 Installation Instructions 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 (205) 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	RJ48C
1.544 Mbps - SF and B8ZS	6.0N	04DU9-DN	RJ48C
1.544 Mbps - ESF	6.0N	04DU9-1KN	RJ48C
1.544 Mbps - ESF and B8ZS	6.0N	04DU9-1SN	RJ48C
ISDN	6.0N	04DU9-1SN	RJ48C

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 to file an affidavit with the local exchange carrier when connecting unprotected customer premise equipment (CPE) to 1.544 Mbps or subrate digital services.
- Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirement for subrate services is waived.

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

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

State of _____

County of _____

I, _____ (name), _____

(business address), _____ (telephone number) being

duly sworn, state:

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

- I attest that all operations associated with the establishment, maintenance, and adjustment of the digital CPE with respect to analog content and encoded billing protection information continuously complies with Part 68 of the FCC Rules and Regulations.
- The digital CPE does not transmit digital signals containing encoded analog content or billing information which is intended to be decoded within the telecommunications network.
- The encoded analog content and billing protection is factory set and is not under the control of the customer.

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

- A. A training course provided by the manufacturer/grantee of the equipment used to encode analog signals; or
- B. A training course provided by the customer or authorized representative, using training materials and instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or
- C. An independent training course (e.g., trade school or technical institution) recognized by the manufacturer/grantee of the equipment used to encode analog signals; or
- D. In lieu of the preceding training requirements, the operator(s)/maintainer(s) is (are) under the control of a supervisor trained in accordance with _____ (circle one) above.

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

_____ Signature

_____ Title

_____ Date

Transcribed and sworn to before me

This _____ day of _____, 199__

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.



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.

Table of Contents

List of Figures	xv
List of Tables	xvii
Chapter 1 Introduction	1-1
Product Overview	1-1
ATLAS 800 <i>PLUS</i> Base Unit	1-1
Frame Relay	1-2
Dedicated and Switched Connection Maps in a Single Platform.....	1-3
Signaling Conversion for Maximum Interoperability.....	1-3
Flexible Network Management and Maintainability	1-4
Digital Access Cross-Connect System (DACS)	1-4
T1 Bandwidth Manager.....	1-5
ISDN Access Switch	1-5
WAN Overbooking	1-5
ATLAS 800 <i>PLUS</i> Features	1-6
Configuration and Management.....	1-6
Software Upgrade	1-6
Signaling Support.....	1-6
ISDN Switch Types	1-7
Dedicated Connection Maps.....	1-7
Switched Connection Maps	1-7
Testing.....	1-7
Performance Monitoring	1-7
Chapter 2 Installation	2-1
Before Installing the ATLAS 800 <i>PLUS</i>	2-1
Contents of ADTRAN Shipments.....	2-1
Customer Provides	2-1
Checking the Power Connection	2-1
Grounding Instructions.....	2-2
Rear Panel	2-2
Control In/Chain In	2-3
Connection.....	2-3
Control Out/Chain Out.....	2-4
Connection.....	2-4
Network Connection.....	2-5
Connection.....	2-5
Ethernet 10BaseT Connection	2-6
Connection.....	2-6
MON (Monitor).....	2-6
Option Slot Arrangement	2-7
Installing Modules	2-7

Power Up Testing And Initialization	2-7
Self-Test	2-7
Chapter 3 Operation	3-1
Front Panel Layout.....	3-1
LCD Window	3-1
Enter.....	3-1
Up and Down Arrows.....	3-1
Cancel	3-1
Numeric Keypad.....	3-1
Shift	3-2
Operation Keys.....	3-3
System LED Description	3-3
Channel Service Unit (CSU) Status	3-4
Module Status LEDs.....	3-4
Operating the ATLAS 800 <i>PLUS</i>	3-5
Getting Started Using Terminal Menus.....	3-5
Telnet	3-6
VT-100 Operation	3-7
T-Watch Pro.....	3-8
Chapter 4 Front Panel Operation and Menu Structure.....	4-1
Navigating the Front Panel	4-2
Data Field.....	4-2
Status Field	4-2
Select and Activate a Menu Item.....	4-2
Set the Data Field.....	4-2
Exit Any Menu Field Operation Or Display.....	4-2
Front Panel Main Menu.....	4-3
Status Menu	4-4
Configuration Menu.....	4-5
Utility Menu	4-6
Alarm (ALRM) Menu.....	4-9
Chapter 5 Using the Terminal Menu.....	5-1
ATLAS 800 <i>PLUS</i> Terminal Menu Structure.....	5-1
Navigating the Terminal Menu.....	5-2
Menu Path.....	5-2
Window Panes	5-2
Right Window Pane Notation.....	5-5
Using the Keyboard Keys	5-5
Getting Help	5-7
System Information.....	5-7
System Status	5-9
System Configuration.....	5-12
System Utility	5-18
Modules.....	5-23
ATLAS 800 <i>PLUS</i> Controller T1/PRI Submenu Items.....	5-25
Dedicated Maps	5-28
Dial Plan.....	5-33
Global Parameters	5-39
Interface Configuration.....	5-41
Quad T1/PRI Module Interface Configuration.....	5-41
Quad T1/PRI Module (Network Termination/PRI).....	5-41

Quad T1/PRI Module (User Termination/PRI)	5-46
Quad T1/PRI Module (User Termination/RBS)	5-48
Quad Nx56/64 Module Interface Configuration	5-49
Quad Nx56/64 Module (User Termination)	5-50
Octal BRI Module Configuration	5-50
Octal BRI Module (Network Termination)	5-50
Octal BRI Module (User Termination)	5-51
Chapter 6 Creating a Dedicated Map	6-1
Overview	6-1
Dedicated Map Design	6-1
Chapter 7 Creating a Dial Plan	7-1
Overview	7-1
Understanding the Application	7-1
Understanding the Dial Plan	7-2
Configure the Ports	7-2
Plan the Dial Plan	7-3
Implement the Dial Plan	7-5
Chapter 8 Updating Firmware	8-1
Firmware Updating	8-1
XMODEM Firmware Updating	8-1
Update Firmware Using XMODEM	8-1
Update Firmware Using TFTP	8-4
Chapter 9 SNMP Management	9-1
Understanding SNMP	9-1
Basic Components	9-1
Network Manager	9-1
MIB	9-1
Traps	9-2
Defining a Trap Destination List	9-2
Filtering Traps	9-2
Standard Traps	9-2
DS1 Traps	9-3
DS1 Alarm Traps	9-3
DS1 Alert Traps	9-5
Chapter 10 ADTRAN Utilities	10-1
Utilities delivered with the ATLAS 800PLUS	10-1
Telnet	10-1
Menu Options	10-1
VT-100	10-3
Menu Options	10-3
Options Menu	10-4
TFTP Server	10-4
Menu Options	10-5
Saving the Current Configuration to a TFTP Server	10-6
To retrieve the configuration from a TFTP server	10-7
Appendix A System Event Logging	A-1
Appendix B Troubleshooting	B-1

Appendix C Warranty and Technical Support Information..... C-1
Index Index-1

List of Figures

Figure 1-1. Point-to-Point Circuit.....	1-2
Figure 1-2. Frame Relay Circuit	1-3
Figure 1-3. Digital Access Cross-Connect System (DACS)	1-4
Figure 1-4. T1 Bandwidth Management	1-5
Figure 1-5. WAN Overbooking.....	1-6
Figure 2-1. ATLAS 800PLUS Rear Panel.....	2-3
Figure 2-2. ATLAS 800PLUS Slot Designation (Rear View)	2-7
Figure 3-1. ATLAS 800PLUS Front Panel Layout.....	3-2
Figure 3-2. Example of Basic Front Panel Menu Navigation.....	3-5
Figure 4-1. Front Panel LCD	4-1
Figure 4-2. Front Panel Menu Tree	4-3
Figure 5-1. Top-Level Terminal Menu	5-4
Figure 5-2. System Information Menu	5-7
Figure 5-3. System Status Menu.....	5-9
Figure 5-4. System Configuration Menu.....	5-12
Figure 5-5. System Utility Menu	5-18
Figure 5-6. View Self-test Log.....	5-22
Figure 5-7. Modules Menu.....	5-23
Figure 5-8. Dedicated Maps Menu	5-29
Figure 5-9. Trunk Conditioning.....	5-31
Figure 5-10. Dial Plan Menu	5-33
Figure 6-1. Dedicated Map Overview Example.....	6-1
Figure 6-2. Slot 0 Module Configuration Menu.....	6-2
Figure 6-3. Completed Dedicated Map.....	6-4
Figure 7-1. Case 1: PSTN Connection.....	7-1
Figure 7-2. Case 2: Point-to-Point	7-1
Figure 7-3. Remote Access and Video Conferencing Setup	7-2
Figure 7-4. Completed Network Map	7-6
Figure 7-5. Completed User Map.....	7-7
Figure 8-1. Update Firmware Menu Interface	8-2
Figure 8-2. Update Firmware Menu Interface	8-5
Figure 10-1. Add New Dialog Box.....	10-2
Figure 10-2. Edit Entry Dialog Box	10-2
Figure 10-3. Port Settings Dialog Box.....	10-4
Figure 10-4. TFTP Server Interface	10-5

List of Tables

Table 2-1.	Control In/Chain In Pinout	2-4
Table 2-2.	Control Out/Chain Out Pinout	2-5
Table 2-3.	Network Pinout	2-6
Table 2-4.	Ethernet 10BaseT Pinout	2-6
Table 6-1.	Connections	6-2
Table 7-1.	Network Terminations	7-4
Table 7-2.	User Termination	7-5
Table 9-1.	Trap Destination List	9-2
Table 9-2.	Standard Trap	9-3
Table 9-3.	DS1 SNMP Traps	9-4
Table 9-4.	DS1 Current Alert SNMP Trap	9-5
Table 9-5.	Total Alert Traps	9-6
Table A-1.	Source: System	A-2
Table A-2.	Source: Switchboard	A-3
Table A-3.	Source: Nx 56/64	A-3
Table A-4.	Source Time	A-4
Table A-5.	Source: Ethernet.....	A-6
Table A-6.	Source: ISDN	A-6
Table A-7.	ISDN Cause Codes	A-9
Table A-8.	Cause Code Log Entries	A-11
Table A-9.	Source: ISDN L2 Messages	A-11
Table A-10.	Source: ISDN Call Control Messages	A-11
Table A-11.	Source: ISDN Information Elements	A-12
Table B-1.	Troubleshooting	B-1

PRODUCT OVERVIEW

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

With the ATLAS 800^{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 800^{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 800^{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 800^{PLUS} BASE UNIT

The ATLAS 800^{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, rackmount, or wallmount installations, the ATLAS 800^{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 800^{PLUS} Base Unit.

The modules include the following:

- Quad Nx 56/64 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 results 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.

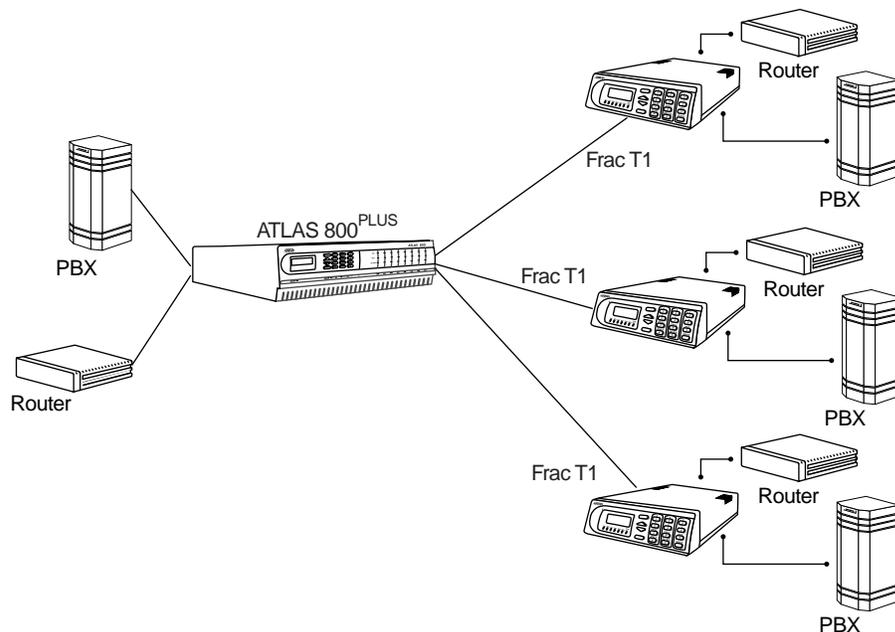


Figure 1-1. Point-to-Point Circuit

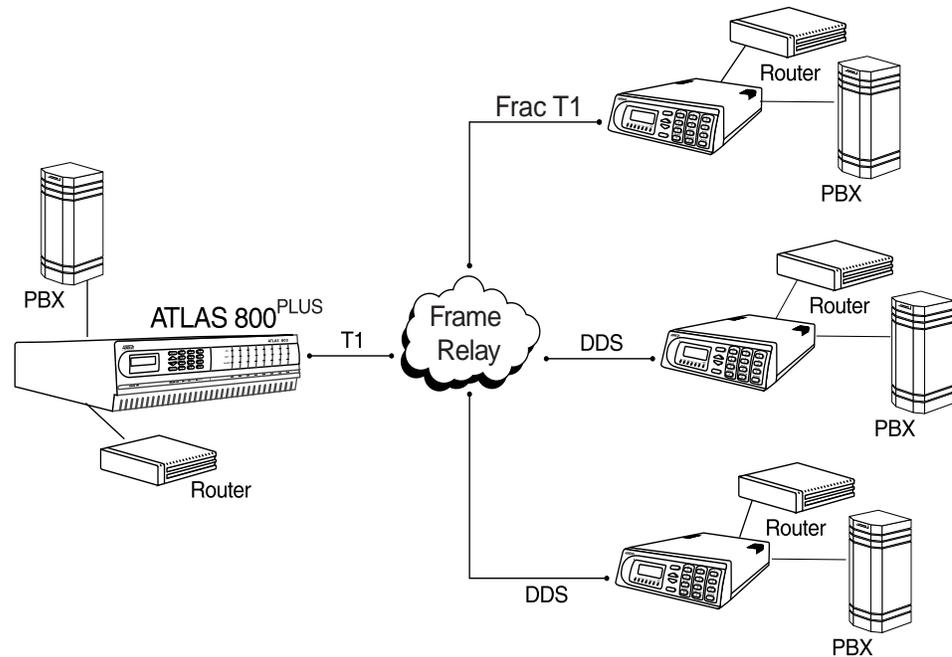


Figure 1-2. Frame Relay Circuit

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 800^{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 invoked manually or implemented automatically based on the time of day and day of the week.

Additionally, the ATLAS 800^{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 dial calls placed over basic rate ISDN, primary rate ISDN, or channelized T1.

Signaling Conversion for Maximum Interoperability

The ATLAS 800^{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 800^{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 can allow 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 front panel contains a 2x16 character backlit LCD display and an extensive array of LEDs for alarm and status information pertaining to the system and the individual modules. A front panel keypad allows navigation through the menu system and access to system testing.

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 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 800^{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).

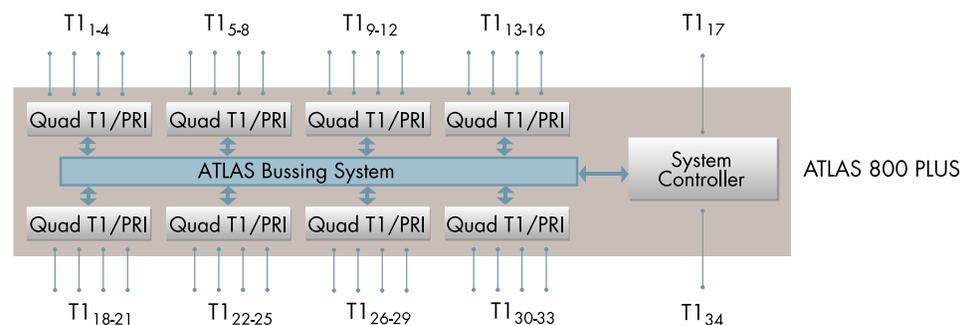


Figure 1-3. Digital Access Cross-Connect System (DACS)

T1 Bandwidth Manager

As a T1 Bandwidth Manager, ATLAS 800^{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).

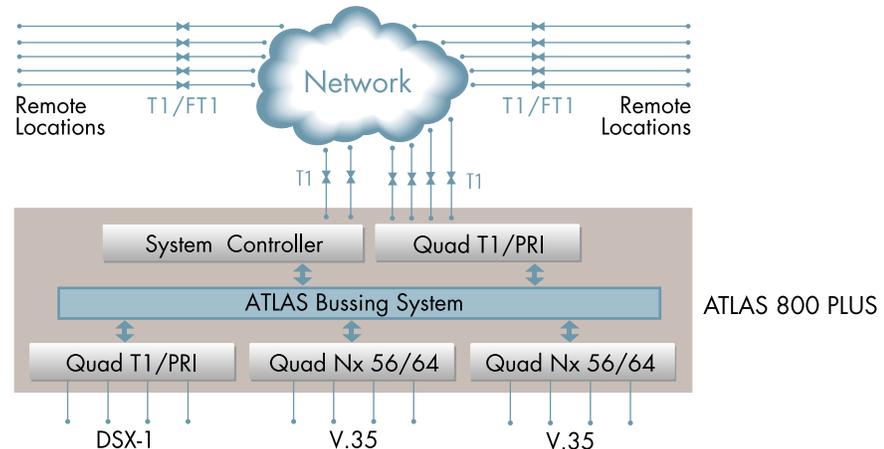


Figure 1-4. T1 Bandwidth Management

ISDN Access Switch

The ATLAS 800^{PLUS} includes an advanced access architecture for switching dial-up 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 PB 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 800^{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).

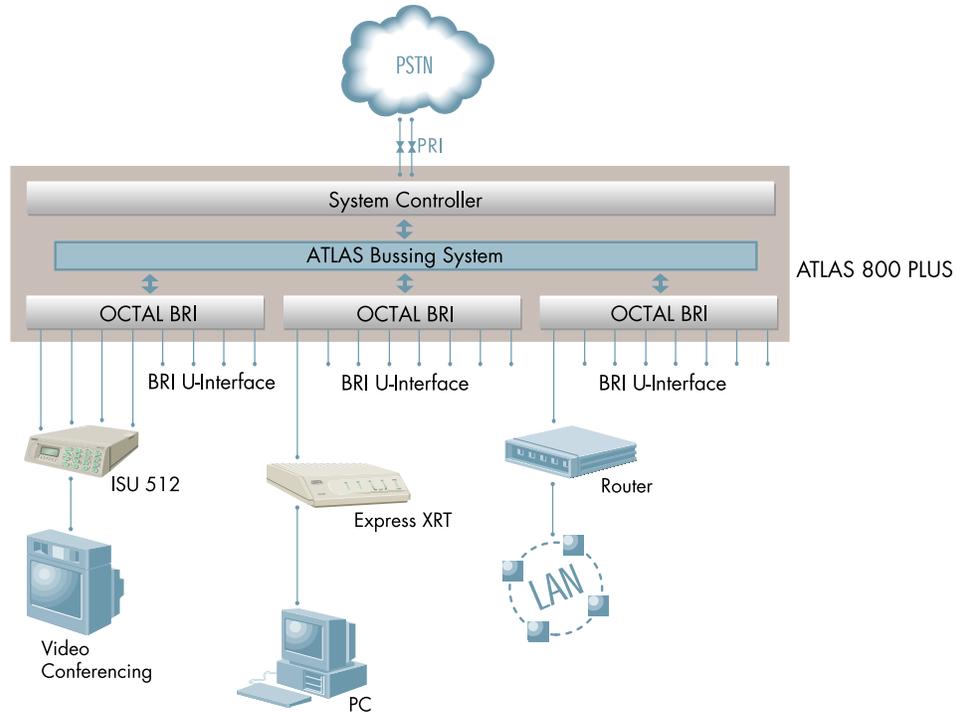


Figure 1-5. WAN Overbooking

ATLAS 800^{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
- LCD Front Panel
- 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

Dedicated Connection Maps

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

- Error counts: ES, SES, UAS, %AS, %EFSEC, Alarms, Error Rates
- Reports: Information stored for last 24 hours in 15 minute increments

BEFORE INSTALLING THE ATLAS 800^{PLUS}

Carefully inspect the ATLAS 800^{PLUS} 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 800^{PLUS} for repair or for verification of damage during shipment.

CONTENTS OF ADTRAN SHIPMENTS

The following items are included in the ADTRAN shipment:

- The ATLAS 800^{PLUS} Base Unit
- The ATLAS 800^{PLUS} *User Manual*
- Power cord
- Network cables (2)
- Rackmount brackets (left and right)
- RJ-45 to DB-25 adapter (modem and direct)
- RJ-45 control port cable (1)
- DSX-1 crossover cable (1)
- RJ-48 to DB-15 adapter (1)
- ADTRAN Utilities diskettes (3)

CUSTOMER PROVIDES

You must supply the 10BaseT cable.

CHECKING THE POWER CONNECTION

Each ATLAS 800^{PLUS} is equipped with a detachable 8-foot power cord with a three-prong plug which connects to a grounded power receptacle.



Power to the ATLAS 800^{PLUS} must be from a grounded 115 VAC, 60 Hz or 220 VAC, 50-60 Hz source.

GROUNDING INSTRUCTIONS

This section provides grounding instruction information from the Underwriters' Laboratory UL 1459 Standard for Safety: Telephone Equipment, of September 20, 1993.

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.

Bare, covered, or insulated grounding conductors are acceptable. A covered or insulated grounding conductor shall have a continuous outer finish that is either green, or green with one or more yellow stripes.

REAR PANEL

The ATLAS 800^{PLUS} unit is equipped with eight slots in the rear panel to house modules which provide a variety of additional resources and data ports. All slots are functionally identical except slots 7 and 8. These slots also accommodate an optional power supply for redundancy (see Figure 2-1 on page 2-3).

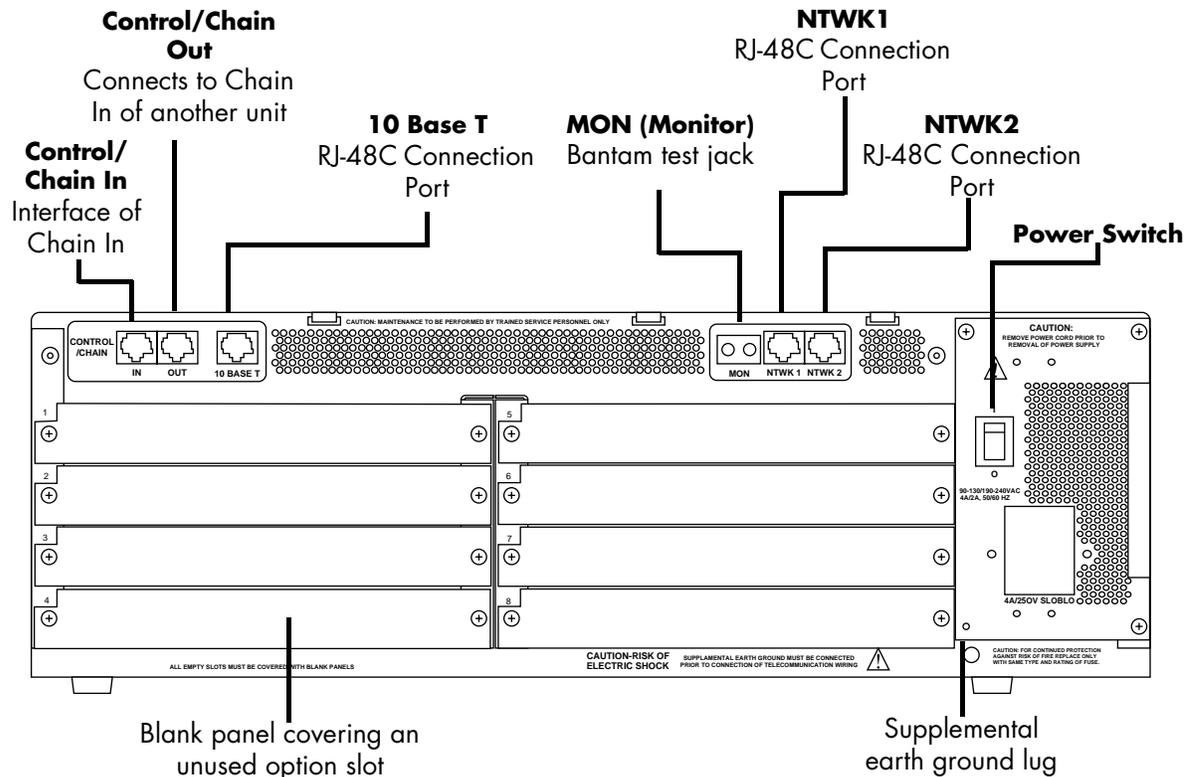


Figure 2-1. ATLAS 800^{PLUS} Rear Panel

Control In/Chain In

The Control In/Chain In port is an EIA-232 port for connection to a computer or modem (control in) or to another ATLAS 800^{PLUS} unit (Chain In). See Table 2-1 on page 2-4 for a description of the pinout.

The control port input provides the following functions:

- EIA-232 input from a PC or a modem for control of the ATLAS 800^{PLUS}
- Chain input
- 2400, 9600, 19200, or 38400 bps operation
- Acts as input for PC control or as input for a chained connection
- Interface for flash memory software downloads using XMODEM

Connection

The Control In/Chain In connection is as follows:

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

Table 2-1. Control In/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 800 ^{PLUS}
4	DTR	Data terminal ready
5	TXDATA	Date transmitted by the ATLAS 800 ^{PLUS}
6	CD	Carrier detect
7	UNUSED	—
8	CTS	Clear to send - flow control

Control Out/Chain Out

The Control Out/Chain Out is an RJ-48C port used to connect to another ATLAS 800^{PLUS} Chain In connector. See Table 2-2 on page 2-5 for the control out/chain out pinout.

The Control Out/Chain Out port output provides the following functions:

- EIA-232 output to chain control to other units
- 2400, 9600, 19200, or 38400 bps operation
- Automatic setup; no user input required

Connection

The control out/chain out connection is as follows:

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

Table 2-2. Control Out/Chain Out Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis. Connect to GND of next unit (pin 1).
2	UNUSED	—
3	TX DATA	Data transmitted to chained units by the ATLAS. Connect to RX DATA of the next unit (chain in pin 3).
4	UNUSED	—
5	RX DATA	Data received from chained units by the ATLAS. Connect to TX DATA of the next unit (chain in pin 5).
6,7,8	UNUSED	—

Network Connection

The two eight-position modular jacks labeled **NTWK 1** and **NTWK 2** provide network connection. Table 2-3 on page 2-6 shows the pinout for the network connectors.

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 test

Connection

The network connection is as follows:

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

Table 2-3. 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	—

Ethernet 10BaseT Connection

The 10BaseT port (RJ-48C) provides an Ethernet LAN connection, which is used for TFTP, SNMP, and Telnet connection. See Table 2-4 on page 2-6 for the pinout.

Connection

The network connection is as follows:

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

Table 2-4. 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	—

MON (Monitor)

The MON 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.

OPTION SLOT ARRANGEMENT

As viewed from the rear of the ATLAS 800^{PLUS}, the slots are numbered as shown in Figure 2-2. All slots are functionally identical except slots 7 and 8, which also accommodate an optional power supply for redundancy.

SLOT 1	SLOT 5	POWER SUPPLY
SLOT 2	SLOT 6	
SLOT 3	SLOT 7	
SLOT 4	SLOT 8	

Figure 2-2. ATLAS 800^{PLUS} Slot Designation (Rear View)

INSTALLING MODULES

After installing the base ATLAS 800^{PLUS} unit and connecting the required cables, you can install modules. If you need instructions for installing a module, refer to the User Manual for the module you want to install.

POWER UP TESTING AND INITIALIZATION

After installing the base unit and any modules, the ATLAS 800^{PLUS} is ready to be powered up.

When shipped from the factory, the ATLAS 800^{PLUS} is set to factory default conditions. When you power up the unit, it automatically executes a memory self test. You can run a full self test from the front panel and set a pass code (through the UTIL menu) and unit ID (through the CONFIG menu) from the front panel. See “Unit ID” on page 4-6 and “Set Passcode (Front Panel)” on page 4-8 for details.

Self-Test

Upon a power-up, the test LEDs light up and the LCD displays the message Memory Test Now Testing. When the self test is complete with no failures detected, the OK LED lights up and the LCD momentarily displays **All Tests Passed**. If a failure is detected, a list of failures displays in the LCD window. The full self test procedure consists of the following steps:

1. **Board-level tests.** The Controller contains an on-board processor which executes a series of tests checking the circuitry on the board.
2. **RAM tests; EPROM checksum.**
3. **TDM map tests.**
4. **On-board data path.** Sending a known test pattern through an on-board loop.

5. **Board-to-board interface test.** A test pattern is sent from the controller through a loopback on all other boards and checked on the controller. This verifies the data path, clocks, and control signals



If the front panel indicates a failure, see Troubleshooting on page B-1 to diagnose the problem.

FRONT PANEL LAYOUT

The ATLAS 800^{PLUS} front panel provides limited control of the unit. You can select and set up the method of connectivity for controlling the unit through the front panel and use it to monitor the operation and status of the unit. Figure 3-1 on page 3-2 identifies the display panels and operation keys.

LCD Window

Displays menu items and messages in two lines by 16 characters in a backlit liquid crystal display (LCD). It also displays alarm and status information.

Enter

Selects active menu items. To select a menu item, press the number of the item. The menu item flashes, indicating it is activated. Press Enter to select the menu item.

Up and Down Arrows

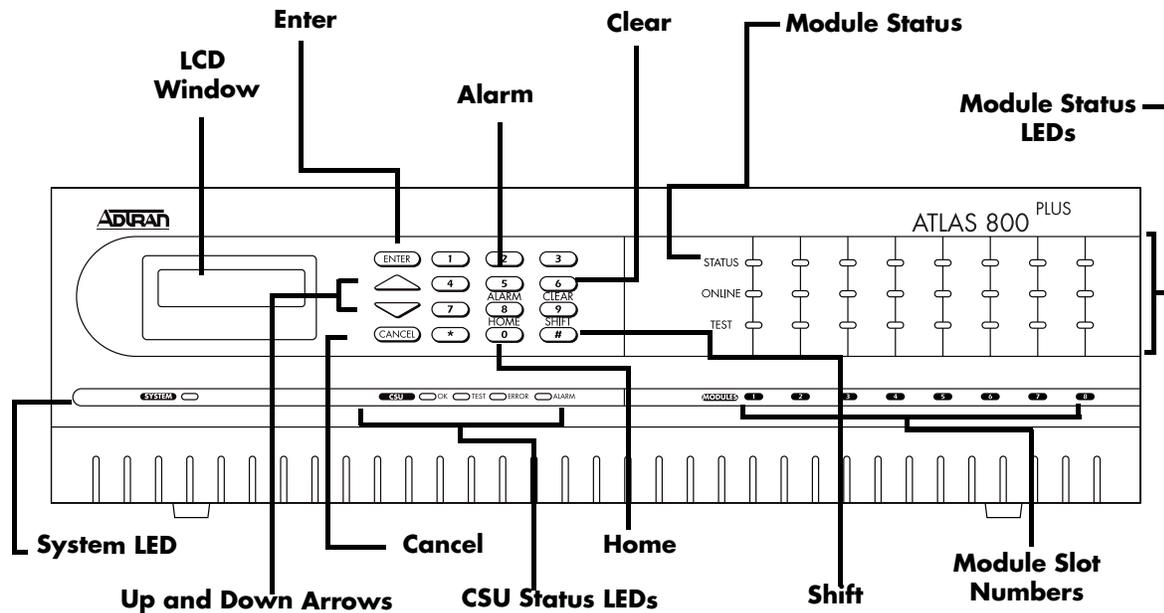
Up and down arrows scroll through and activate the submenu items available in the current menu. When the submenu items are scrolled, the flashing cursor indicates the active parameter.

Cancel

Pressing the Cancel key stops the current activity and returns to the previous menu. Repeat until you reach the desired menu level. When a submenu item displays, press Cancel to exit the current display and return to the previous menu.

Numeric Keypad

The numeric keypad contains the numbers 0 through 9, which you use to activate menu items and enter information (such as the IP address).



LCD	Displays menu items and messages in 2 lines by 16 characters.	Clear	Clear data/results fields.
Cancel	Stops current activity and returns to the previous menu.	CSU Status LEDs	Indicate the status of both network interfaces.
Home	Returns to the main menu.	Module Slot Numbers	LEDs correspond to the option modules installed in the unit.
Shift	Provides access to special function keys.	System LED	Indicates the status of the entire ATLAS 800 ^{PLUS} .
Enter	Selects active menu items.	Module Status	Displays the operational condition of modules installed in the option slots.
Alarm	Quick access to the active alarm display menus	Module Status LEDs	Indicates the status of each module.
Up & Down Arrows	Scroll through and activate the submenu items available in the current menu. The flashing cursor indicates the active parameter.		

Figure 3-1. ATLAS 800^{PLUS} Front Panel Layout

Shift

Activate the front panel operation keys (**Alarm**, **Clear**, and **Home**) by first pressing **Shift**. The next section describes all of the available operation keys.

If you press a key without using **Shift**, the numbered item becomes active instead of the operation key.

Operation Keys

Operation keys are ATLAS 800^{PLUS} front panel keys that perform alternate functions. To activate an operation key, simultaneously press the front panel shift key and the operation key that you want to activate.

To do this...	Press these front panel keys...
Quickly accesses the active alarm display menus. (This function can be activated while any other menu item is in use. When you exit the Alarm menu, the unit returns to the same menu that was active when you selected Alarm.)	Shift + Alarm
Clear data/result fields in various menus.	Shift + Clear
Return to the Main menu from any menu location.	Shift + Home

System LED Description

The System LED indicates the general status of the entire ATLAS 800^{PLUS}. A green light indicates that conditions are normal. A red light indicates a system problem or alarm condition.

This color light...	Indicates that...
Green (solid)	No diagnosed system faults were found.
Green (fast blink)	Flash download is in progress.
Yellow	Fault was diagnosed, but the condition no longer exists. The condition will be recorded in the system log.
Red (solid)	An error condition is present with either the power supply or temperature.
Red (fast blink)	A fatal error occurred during flash download.
Off	Power is not currently applied to the system.

Channel Service Unit (CSU) Status

The CSU Status LEDs indicate the status of both network interfaces.

This color light...	Indicates this CSU status...
OK (green)	Indicates normal, error-free operation of both network interfaces. If either interface experiences alarms, the OK LED remains off.
Test (yellow)	Indicates that 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)	The Error LED indicates an error such as BPV (bipolar violation), OOF (out of frame), or CRC (cyclic redundancy check).
Alarm (red)	Indicates 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 <i>View History</i> menu.

Module Status LEDs

The Module Status LEDs display, by row, the operational condition (**Status**, **Online**, and **Test**) of each module installed in the option slots.

This color light...	Indicates this 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.

Online

The **Online** LED indicates that the module is available for use or is currently in use. If the module is manually taken offline, this LED is turned off.

Test (yellow)

One or more ports in a module is in test.

OPERATING THE ATLAS 800^{PLUS}

You can access basic setup functions from the ATLAS 800^{PLUS} front panel. To access all of the ATLAS 800^{PLUS} functions, set up a Telnet session or use a VT-100. The following sections provide an overview of the different ways to operate the ATLAS 800^{PLUS}. After you understand the different ways to operate the ATLAS 800^{PLUS}, you will be ready to configure the unit.

Getting Started Using the Front Panel

With the ATLAS 800^{PLUS} powered-up, the front panel LCD window displays various menu items. To select a menu item, either press the corresponding number on the front panel keypad or press the front panel up and down arrows to scroll to the menu selection. The following steps describe how to set up the Unit ID from the front panel (see also Figure 3-2).

1. Activate Configuration (**CONFIG**) using the front panel **arrow keys** or by pressing **2**. (The cursor flashes on the number next to the activated selection.) Press **Enter**.
2. Use the **arrow keys** to view the submenu items.
3. Select **S0) SYSTEM**. Press **Enter**.
4. Activate **2) CHAIN PORT** using the **arrow keys** or by pressing **2**. Press **Enter**.
5. Activate **4) UNIT ID** using the **arrow keys** or by pressing **4**. Press **Enter**.
6. The Unit ID field displays. Type the new Unit ID in this field and press **Enter**. The new Unit ID is now set.

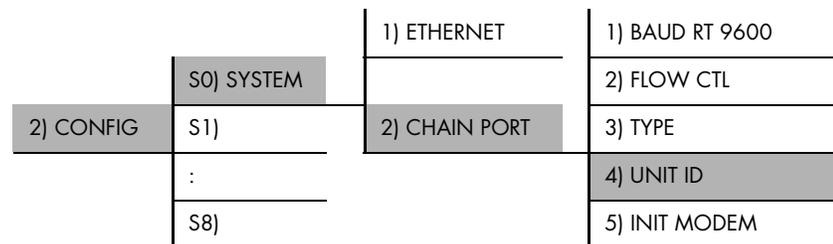


Figure 3-2. Example of Basic Front Panel Menu Navigation

For detailed information about the commands available through the front panel menus, see “Front Panel Operation and Menu Structure” on page 4-1.

Getting Started Using Terminal Menus

Terminal menus provide one of the primary means of monitoring and configuring the ATLAS 800^{PLUS}. The terminal menu interface uses the full capabilities of the VT-100 terminal to provide the quickest and most intuitive operation possible. 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 10-1 for details on the available programs.

You can access the terminal menu using a VT-100 terminal or a computer running VT-100 terminal-emulation software. The two basic connection methods supported by the ATLAS 800^{PLUS} are a direct connection through the EIA-232 Chain In port and a Telnet session. The following sections describe how to get started using both of these methods.

Telnet

To connect to the ATLAS 800^{PLUS} via Telnet, follow these steps:

Define the IP Address



NOTE You must define the IP address before attempting to connect via Telnet.

1. Obtain an IP address for the ATLAS 800^{PLUS} from your LAN administrator.
2. From the front panel, select **2) CONFIG**, then **S0) SYSTEM**, then **1) ETHERNET**.
3. When the submenu displays, select **1) IP ADDRESS**.
4. Enter the IP address by entering each number followed by **Enter** to move to the next field.
5. Press **Enter** after keying in the entire IP address.

Set the Subnet Mask

1. Obtain a subnet mask address from your LAN administrator.
2. From the front panel, select **2) CONFIG**, then **S0) SYSTEM**, then **1) ETHERNET**.
3. When the submenu displays, select **2) SUBNET MASK**.
4. Enter the subnet mask by entering each number followed by **Enter** to move to the next field.
5. Press **Enter** after keying in the entire subnet mask address.

Set the Default Gateway IP address (typically required)



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

1. From the front panel, select **2) CONFIG**, then **S0) SYSTEM**, then **1) ETHERNET**.
2. When the submenu displays, select **3) DEF GATEWAY**.
3. Enter the default gateway by entering each number followed by **Enter** to move to the next field.
4. Press **Enter** after keying in the entire address.

Start 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 5-16 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 5-12 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 5-13 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 which is recommended for optimum performance is delivered with the ATLAS 800^{PLUS}. See “VT-100” on page 10-3 for details.

For detailed information on the commands available during a Telnet session, refer to Chapter 5, “Using the Terminal Menu” on page 5-1.

VT-100 Operation

An EIA-232 serial connection is available via the chain-in port on the rear panel of the ATLAS 800^{PLUS}. The ATLAS 800^{PLUS} provides the front panel menus to a VT-100 type terminal. Follow these steps to set up the ATLAS 800^{PLUS} for VT-100 terminal mode:

1. Set the baud rate on the VT-100 terminal to 9600 baud (8/N/1).
2. Use the front panel to set the ATLAS 800^{PLUS} baud rate to match the terminal baud rate. Select **2) CONFIG, S0) SYSTEM, 2) CHAIN PORT, 1) BAUD RATE**.
3. 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 on the rear of the unit. This connection provides both local and remote configuration.
4. Repeatedly press **Enter** on the front panel until the *Login* Menu appears.

After connecting a VT-100 terminal or a computer running VT-100 terminal-emulation software to this port, you may need to press Ctrl-R to refresh the display. Refer to “Using the Terminal Menu” on page 5-1 for detailed information on using the terminal menus.

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 5-16 for details.

For detailed information on the commands available during a VT-100 session, refer to Chapter 5, “Using the Terminal Menu” on page 5-1.

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 800^{PLUS} using a graphic interface. Currently, you can choose ATLAS 800^{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 800^{PLUS} unit. Currently T-Watch PRO automatically receives SNMP traps from an ATLAS 800^{PLUS}.

ATLAS 800^{PLUS} FRONT PANEL MENU STRUCTURE

The ATLAS 800^{PLUS} uses a multilevel menu structure containing both menu items and data fields. All menu operations and data display in the LCD window. However, you only have access to limited configuration options through the front panel. To access all of the ATLAS 800^{PLUS} options, use the Terminal menu. See “Using the Terminal Menu” on page 5-1.

The front panel opening menu (Main menu) is the access point to all other operations. Each Main menu item has several functions and submenus to identify and access specific parameters.

The front panel LCD of the Main menu contains the menu options STATUS, CONFIG, UTIL, and ALRM (see Figure 4-1).

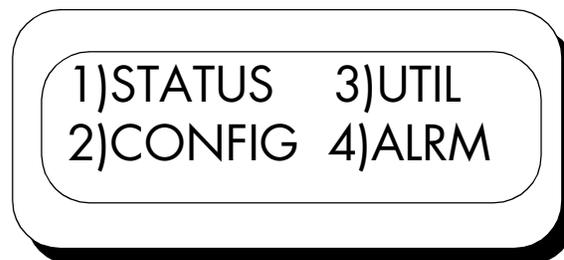


Figure 4-1. Front Panel LCD

To do this...	Go to this Main menu...	For more information...
Display the status of the ATLAS 800 ^{PLUS}	Status	See page 4-4.
Display the card type in each slot	Status	See page 4-4.
Perform limited configuration of the ATLAS 800 ^{PLUS}	Config	See page 4-5.
Monitor and modify miscellaneous settings	Util	See page 4-6.
View a log of system events	Alarm	See page 4-9.

Navigating the Front Panel

The following sections provide general information on how to navigate the front panel menus.

Data Field

Menu items followed by a colon (:) indicate a data field that you can edit.

Status Field

Menu items followed by an equal sign (=) indicate the state of the item (such as Online).

Select and Activate a Menu Item

To choose a menu item, place the cursor on the menu item by pressing the number corresponding to the menu item or by highlighting the menu item with the up or down arrows.

Set the Data Field

You can edit data fields preceded by a colon. With the cursor positioned on the submenu item number, press **Enter** on the front panel. The cursor moves to the data field (to the right of the submenu item name).

Using the front panel **arrows**, scroll to scan the available value settings. The value settings display one at a time. When the desired value displays, press **Enter** on the front panel to set the value. When the value is set, the cursor moves back to the submenu item position, indicating the operation is complete.

You can select another submenu field, or press **Cancel** to return to the submenu.

Pressing **Cancel** prior to pressing **Enter** voids any data changes. The original data value is restored and the cursor returns to the submenu field.

Exit Any Menu Field Operation Or Display

Press **Cancel** as many times as required to return to the desired menu level or press **Home** to return to the Main menu.

FRONT PANEL MAIN MENU

The front panel Main menu provides limited configuration and control of the ATLAS 800^{PLUS}. Figure 4-2 displays the submenu options offered through the front panel Main menu.

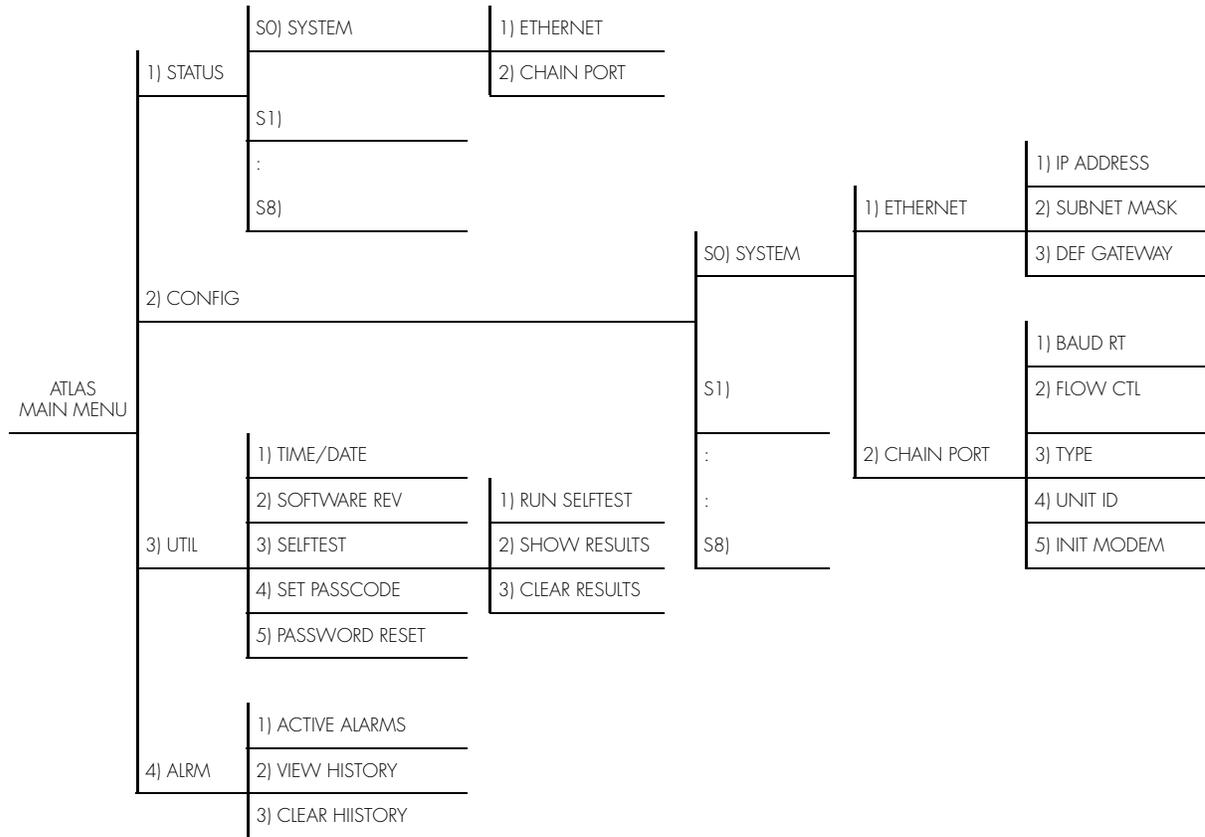


Figure 4-2. Front Panel Menu Tree

Status Menu

The *Status* menu branch lets you view the status of the ATLAS 800^{PLUS} Base Unit and any installed modules.

S0 System

The *S0 System* option displays status options that are available for the ATLAS 800^{PLUS} Base Unit. Choose from *Ethernet* (see “Ethernet Status” on page 4-4) or *Chain Port* (see “Chain Port Status” on page 4-4).

Ethernet Status

This read-only option shows the status of the 10BaseT Ethernet connection port. The following port status options display in the LCD window. An asterisk (*) indicates activity for the item.

Port status ...	Means that...
TX	Data is being transmitted from the 10BaseT port on the system controller.
RX	Data is being received on the 10BaseT port.
LNK	Indicates the current status of the 10BaseT link integrity test (should always be on when the unit is connected to a functional 10BaseT hub).

Chain Port Status

This read-only option indicates the status of the Chain Port. The following port status options display in the LCD window. An asterisk (*) indicates activity for the item.

Port status...	Means that...
RTS	Request to send.
CTS	Clear To send.
DTR	Data terminal ready.
DCD	Data carrier detect.

S1 through S8 (modules)

Select options *S1* through *S8* to display the current status of installed modules. *S1* corresponds to slot 1, *S2* to slot 2, and so on. When you select one of these options, an expanded description of the card status displays. The status types include **ON** (Online), **OFF** (Offline), **NRSP** (No Response), **NRDY** (Not Ready), and **RST** (Restarting).

Configuration Menu

The *Config* menu branch provides limited configuration control of the ATLAS 800^{PLUS}.

S0 System

S0) System displays configuration options that are available for the ATLAS 800^{PLUS} Base Unit. Choose from *Ethernet Configuration* (see “Ethernet Configuration” on page 4-5) or *Chain Port Configuration* (see “Chain Port Configuration” on page 4-5).

Ethernet Configuration

Ethernet Configuration allows you to create and change settings for the 10BaseT Ethernet connection.

IP Address

This is the address that uniquely identifies the ATLAS 800^{PLUS} on a TCP/IP network. 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. Enter the IP address by entering each number followed by **Enter** to move to the next field.

 **NOTE** You must define the IP address before attempting to use a Telnet program.

Subnet Mask

This option defines which part of a destination IP address is the Network number. This address is composed of four decimal numbers, each in the range of 0 to 255, separated by periods. This option is used along with the ATLAS 800^{PLUS} IP address to determine which nodes must be reached through the default IP gateway. Enter the subnet mask address by entering each number followed by **Enter** to move to the next field.

Def Gateway

This option allows you to define or change the default gateway. 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. Enter the default gateway address by entering each number followed by **Enter** to move to the next field.

Chain Port Configuration

The *Chain Port* menu option modifies selected items in its menu branch.

Baud Rt

This option displays and changes the baud rate. The supported baud rates for the chain port include 2400 and 9600 bps. If *Type* is set to **Dial**, make sure this field matches the modem baud rate.

Flow Ctl

This option sets the flow control for the chain port. You can configure the chain port flow control for **OFF** or **H/W** (hardware).

Type

Sets the *Port Type* to either **Direct** or **Dial**. Select **Direct** to connect to a local VT 100 and select **Dial** to connect via a modem.

Unit ID

This menu accesses the current Unit ID setting, which is the system identifier used for ADTRAN Data Link Layer Protocol (ADLP) configuration control (such as using T-Watch PRO).

Editing or changing the Unit ID requires the use of a passcode if a passcode is defined. See “Set Passcode (Front Panel)” on page 4-8 for details on working with passcodes. Unit Identification numbers must be between 2 and 9999. The number 1 is reserved for the PC.

Press **Enter** to record the Unit ID number and establish its availability when operating by remote control. Press **Cancel** at any time to end the editing process.

Init Modem

Selecting *Init Modem* provides the option to send the modem initialization string (e.g., ATE0V1&D2S0=1) from the chain port to a modem connected to the chain port. Configure this string in the terminal menus. See “Modem Initialization String” on page 5-14 for details on how to change this field.



NOTE *The Init Modem option is only used if Type is set to Dial.*

S1 through S8 (modules)

Select options **S1** through **S8** to display the current configuration options of installed modules. **S1** corresponds to slot 1, **S2** to slot 2, and so on. When you select one of these options, you can enable or disable the selected module. The current status, **ENA** (Enabled) or **DIS** (Disabled), displays next to the module name. Set this field to **DIS** (Disable) prior to removing a module from the ATLAS 800^{PLUS} unit.

Utility Menu

The *Utility* menu allows miscellaneous settings to be displayed or modified.

Time/Date

This menu option displays and/or edits the current time and date. The ATLAS 800^{PLUS} maintains the time and date during power off conditions.

After any numeric change, press **Enter** to record the entry and move to the next editing position. You can also move to a different field to edit by pressing **Enter** at the editing position without making any change, or by using the **up** and **down arrow keys**. Press **Cancel** at any time to end the editing process.

Software Rev

This option displays the current software revision level loaded into the base unit controller. This information is required when requesting assistance from ADTRAN Technical Support or when updates are needed. Press **Cancel** to exit this option.

Selftest

Selftest executes a system self-test, and the LCD displays the **Pass** or **Fail** when the test is complete.



CAUTION *The Selftest option disrupts data flow.*

Run Selftest

This command initiates a self-test. When you select this option, the prompt **Selftest, Are You Sure Y/N?** displays. To initiate the self-test, select **Y** and press **Enter**. Select **N** and press **Enter** to cancel the self-test.

If you select **Y** and proceed with the self-test, the LCD displays the message **Selftest in progress....** When the self-test is complete with no failures detected, the **OK** LED illuminates and the LCD momentarily displays **Self-Test Passed**. If failures are detected, a list of failures displays in the LCD window.

The full self-test procedure consists of the following steps:

1. **Board-level tests.**
The Controller contains an on-board processor which executes a series of tests checking the circuitry on the board.
2. **RAM tests;
EPROM checksum.**
3. **TDM map tests.**
4. **On-board data path.**
Sending a known test pattern through an on- board loop.
5. **Board-to-board interface test.**
A test pattern is sent from the controller through a loopback on all other boards and checked on the controller. This verifies the data path, clocks, and control signals.

During a self-test, ATLAS 800^{PLUS} checks data integrity and verifies processor control to each port. Each port is looped back and a data pattern is sent and tested.

Show Results

This option displays the types of tests performed during a self-test, as well as the results of the tests. Each item in the list displays either **Passed** or **Failed**. The following items display:

Test...	Checks this...
NVRAM	Non-volatile RAM
DSP RAM	Digital signal processor RAM
RTC RAM	Real time clock RAM
TDM MAP	TDM time slot mapping RAM
DRAM	Dynamic program memory used for program execution
Slot 1 – 8	Data path test to individual modules

A RAM test failure indicates a controller board problem. If a slot fails, the module in the slot may have a problem,

Clear Results

This option resets the self-test log that you access with the *Show Results* option. When you select this option, the message **Self-Test Log Clearing** displays. After the command is finished executing, the message **Self-Test Log Cleared** displays.



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

Set Passcode (Front Panel)

The *Set Passcode* option provides security for front panel access. You can change or set the front panel passcode at any time or eliminate it altogether through the *Set Passcode* option. By default, the front panel does not have a passcode.

The passcode can only be entered by using numbers (any number except zero). After entering the desired passcode, press **Enter**. The prompt **Verify Passcode** displays. Enter the passcode again and press **Enter**.

Set a null passcode by pressing **0** and then pressing **Enter**. When the **Verify Password** prompt displays, press **0** and **Enter** again. A null passcode grants unlimited access to front panel options.

Password Reset

You can create a list of system passwords with the terminal menus (see “Access Passwords” on page 5-16 for details). If you forget the password and are unable to log in to the terminal menus, use the *Password Reset* option. When you select this option, two items display in the LCD window: **CHALLENGE #** and **RESPONSE #**.

Call ADTRAN technical support, and tell them the challenge number. They use this to generate a random response number. Enter this response number in the **RESPONSE #** field, and ATLAS 800^{PLUS} inserts a default password into the system password list. You can then use the new default password to log into the terminal menus.

Alarm (ALRM) Menu

From the terminal menus you can view a log of system events. To control the types of events logged, a series of filters have been defined for each event source (System, T1/PRI, ISDN, Ethernet, etc.). Any event with a severity greater than, or equal to, the threshold defined in the event logging filter list is logged to the system event log. Events that do not appear in the event log do not appear in the front panel alarm lists. Therefore, the event logging filters are applied to both the terminal and the front panel menu lists. See “System Event Logging” on page 5-16 for details on setting the thresholds for event logging.

Active Alarms

This menu item displays a list of current alarms reported by the base controller. If no alarms are current, this menu item displays **End of List**. If there are current alarms, this display includes two lines of text. The top line is the alarm source. The bottom line is the alarm message.

View History

This option displays a time and date-stamped list of the alarms that have occurred in the ATLAS 800^{PLUS}. Some alarm types include **-A** to indicate the alarm is active and **-I** to indicate the alarm is inactive.

Clear History

This option clears the alarm history log.



When you clear the alarm history log, you cannot retrieve the data.

ATLAS 800^{PLUS} TERMINAL MENU STRUCTURE

The ATLAS 800^{PLUS} uses a multilevel menu structure that contains both menu items and data fields. All menus and data display in the terminal menu window, through which you have complete control of the ATLAS 800^{PLUS}. For details on connecting to the ATLAS 800^{PLUS} terminal menu, see “Getting Started Using Terminal Menus” on page 3-5.

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 work with the ATLAS 800^{PLUS} terminal menu.

To do this...	Go to this menu...	For more information...
Review and monitor general system information for the ATLAS 800 ^{PLUS}	<i>System Info</i>	See page 5-7.
Review and monitor system status for the ATLAS 800 ^{PLUS}	<i>System Status</i>	See page 5-9.
Set up the operational configuration for the ATLAS 800 ^{PLUS}	<i>System Config</i>	See page 5-12.
Update settings, transfer files, perform system diagnostics, and reboot the ATLAS 800 ^{PLUS}	<i>System Utility</i>	See page 5-18.
Review and configure settings for each installed module, including the ATLAS 800 ^{PLUS} base unit	<i>Modules</i>	See page 5-23.

To do this...	Go to this menu...	For more information...
Assign dedicated connections between any two ports in the ATLAS 800 ^{PLUS}	Dedicated Maps	See "Dedicated Maps" on page 5-28.
Set global ATLAS 800 ^{PLUS} switch parameters or set individual parameters for each port in ATLAS 800 ^{PLUS} that handles a switched call	Dial Plan	See "Dial Plan" on page 5-33.



NOTE To edit terminal menu items, you must have the appropriate password (security) level. Each menu item description in the following sections indicates the required password (security) level for read and write access. See "Access Passwords" on page 5-16 for detailed information on working with passwords.

NAVIGATING THE TERMINAL MENU

The following sections provide information on navigating through the terminal menu. Figure 5-1 shows the top-level terminal menu and describes various window areas.

Menu Path

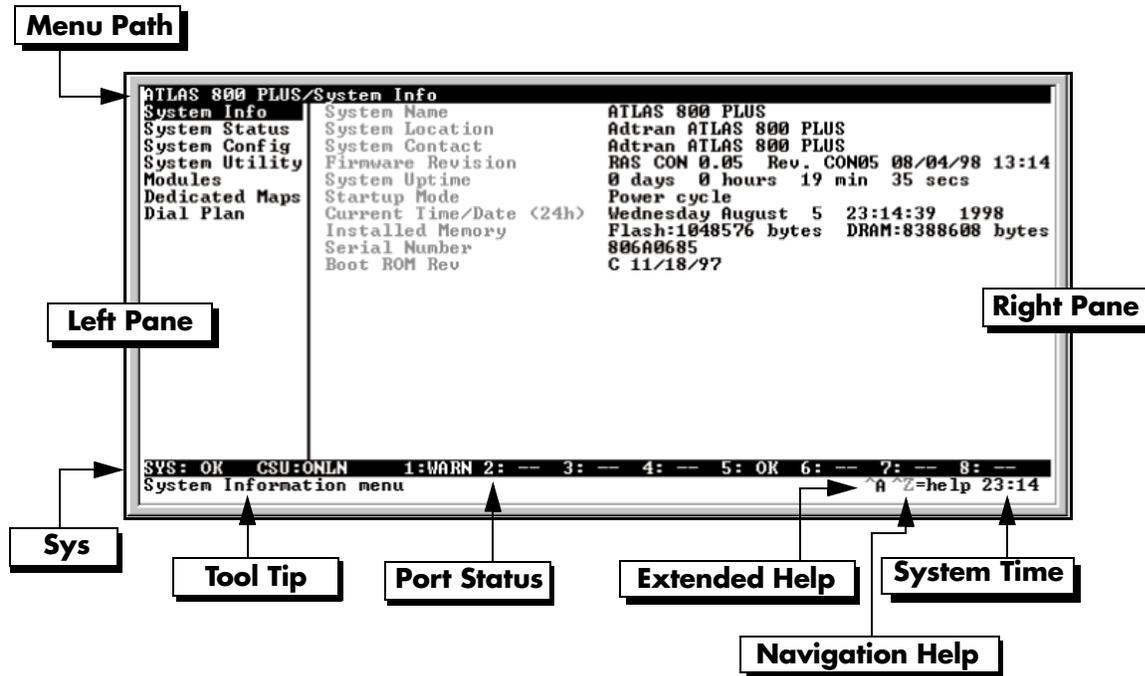
The first line of the window (menu path) shows this session's current path (position) in the menu structure. Figure 5-1 shows the top-level menu with the cursor on the *System Info* submenu; therefore, the menu path reads ATLAS 800 PLUS/ System Info.

Window Panes

When you first start a terminal menu session, the terminal menu window is divided into left and right panes. The left pane shows the current list of submenus, while the right pane shows the contents of a selected submenu. Use the following chart to assist you in moving between and within the window panes.

To do this...	Press one of these keys...
Move from left pane to right pane	Tab Enter Left arrow Right arrow

To do this...	Press one of these keys...
Move from right pane back to left pane	Tab Escape Left arrow Right arrow
Move around in each pane	Up arrow Down arrow Left arrow Right arrow



Menu Path	Describes current position in the terminal menu structure.
Left Pane	Lists available menus.
Right Pane	Shows contents of currently selected menu.
Sys	Describes ATLAS base unit.
Tool Tip	Brief description of currently selected command.
Port Status	Displays information about ports 1 – 8.
Extended Help	Displays information about selected commands (Ctrl-A).
Navigation Help	Lists characters used for navigating the terminal menu (Ctrl-Z).
System Time	Displays current time. See "Current Time/Date (24h)" on page 5-8 for details on editing the time.

Figure 5-1. Top-Level Terminal Menu

Right Window Pane Notation

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.

Using the Keyboard Keys

You can use various keystrokes to navigate 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.

Terminal Menu Navigation	
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.	Arrow Keys
Edit a selected menu item.	Enter
Cancel an edit.	Escape
Close pop-up help screens.	Escape
Move between the left and right panes.	Tab Arrow Keys
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 these keys...
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 <i>Modules</i> 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: <ul style="list-style-type: none"> • 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 <i>Slot #</i> field in the <i>Modules</i> 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.	<

Configuration Keystrokes (Continued)	
To do this...	Press this key...
Insert a new list item. For example, add a new item to the <i>Dedicated Map</i> connection list by pressing I while the cursor is over the index number.	I
Delete a list item. For example, delete an item from the <i>Dedicated Map</i> connection list by pressing D while the index number is active.	D

Getting Help

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

Press Ctrl-Z to activate a help screen that displays the available keystrokes you can use to navigate the terminal menu.

SYSTEM INFORMATION

The *System Info* menu provides basic information about the unit as well as data fields for editing information. Figure 5-2 displays the submenus that are available when you select this menu item.

```

ATLAS 800 PLUS/System Info
System Info      System Name      ATLAS 800 PLUS
System Status    System Location  Adtran ATLAS 800 PLUS
System Config    System Contact   Adtran ATLAS 800 PLUS
System Utility    Firmware Revision RAS COM 0.05 Rev. CON05 08/04/98 13:14
Modules          System Uptime    0 days 0 hours 19 min 35 secs
Dedicated Maps  Startup Mode     Power cycle
Dial Plan        Current Time/Date (24h) Wednesday August 5 23:14:39 1998
                 Installed Memory Flash:1048576 bytes DRAM:8388608 bytes
                 Serial Number    806A0685
                 Boot ROM Rev     C 11/18/97

SYS: OK  CSU:ONLN  1:WARN 2: -- 3: -- 4: -- 5: OK 6: -- 7: -- 8: --
System Information menu                               ^Z=help 23:14
  
```

Figure 5-2. System Information Menu

System Name

Write security: 3; Read security: 5

Provides a user-configurable text string for the name of the ATLAS 800^{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).

System Location

Write security: 3; Read security: 5

Provides a user-configurable text string for the location of the ATLAS 800^{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

Write security: 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 800^{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. This field is read-only.

System Uptime

Read security: 5

Displays the length of time the ATLAS 800^{PLUS} system has been running. Each time you reset the system, this value resets to 0 days, 0 hours, 0 min and 0 secs. This field is read-only.

Startup Mode

Read security: 5

Displays details about the last system startup. This field is read-only.

Current Time/Date (24h)

Write security: 3; Read security: 5

Displays the current date and time, including seconds. You can edit this field. 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, 09-30-1997).

Installed Memory

Read security: 5

Displays the type and amount of memory in use (including Flash memory and DRAM). This field is read-only.

Serial Number

Read security: 5

Displays the serial number for the unit. This field is read-only. The serial number of the ATLAS 800^{PLUS} will automatically display in this field.

Boot ROM Rev

Read security: 5

Displays the boot ROM revision. This field is read-only.

SYSTEM STATUS

The *System Status* menu provides information on the status of the unit. Figure 5-3 shows the submenu functions available in the *System Status* menu.

```

ATLAS 800 PLUS/System Status
System Info      Event Log          [empty]
System Status   Clear System Event Log  <+>
System Config   Ethernet Port         [+ ]
System Utility  Clear System LED      <+>
Modules         System Alarms         Temp Fail[-] PS1 Fail[-] PS2 Fail[-]
Dedicated Maps System Timing Source  PRIMARY : Locked
Dial Plan       System Resource Usage [+ ]
                Chain Port Signal Leads RTS[*] CTS[*] DTR[*] DCD[-]
                Chain Port Tx Bytes    17298
                Chain Port Rx Bytes    68
                Chain Port Overrun Errs 0
                Chain Port Framing Errs 0
                Clear Chain Port Countrs <+>

|

SYS: OK  CSU:ONLN  1:WARN 2:  3:  4:  5: OK  6:  7:  8:
System Status menu          ^Z=help 23:16_

```

Figure 5-3. System Status Menu

Event Log

Read security: 5

Displays the last 250 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. These fields are read-only. The following options are available to review:

Time Event Log/Time

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

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 “System Event Logging” on page 5-16 for details.

Slot

Displays the slot number in which the event occurred. If this field displays a dash (—), the event occurred in the ATLAS 800^{PLUS} Base Unit.

Port

Displays the port in which the event occurred.

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. These fields are read-only. An asterisk (*) indicates activity for the item.

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 800^{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. These fields are read-only. The following options 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 800^{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 5-12 and "Backup Timing Source" on page 5-12 for details.

System Resource Usage

Write Security: 4 Read Security: 5

Indicates resource use (Analog Modems; Digital modems; Voice Compression).

Data Tables

This statistic...	Does this...
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.

This option...	Does this...
Display Format	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.

This option...	Indicates this state...
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. This field is read-only.

Chain Port Rx Bytes

Read security: 5

Displays the number of received data bytes. This field is read-only.

Chain Port Overrun Errs

Read security: 5

Displays the number of overrun errors. This field is read-only.

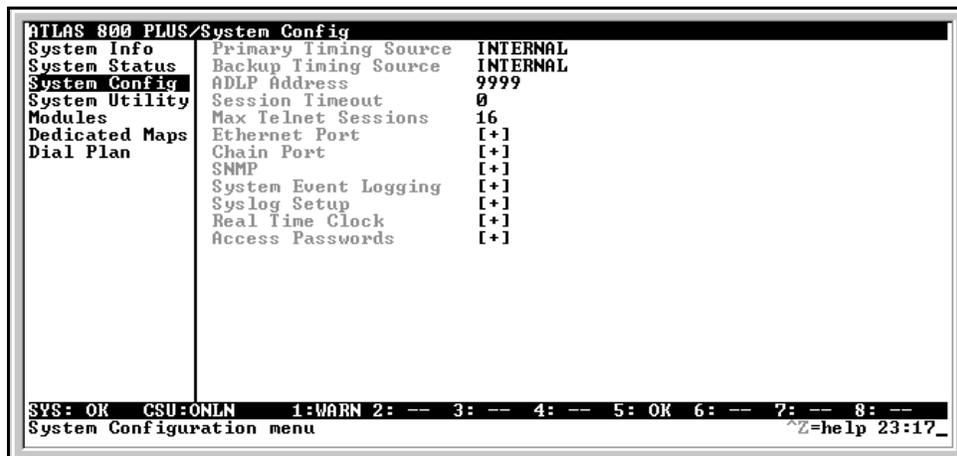
Chain Port Framing Errs

Read security: 5

Displays the number of received framing errors. This field is read-only.

SYSTEM CONFIGURATION

The *System Config* menu allows you to set up the ATLAS operational configuration. Figure 5-4 shows the items included in this menu.

**Figure 5-4. 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 800^{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 800^{PLUS} IP address to determine which nodes must be reached through the default IP gateway.

Chain Port

Write security: 2; Read security: 5

Supplies options 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 or 9600. 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

This option sets the flow control for the chain port. You may configure the chain 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 800^{PLUS}. For detailed information on SNMP, refer to “SNMP Management” on page 9-1. The following options are available for review and editing:

SNMP Access

Write security: 3; Read security: 5

Defines whether SNMP access to the ATLAS 800^{PLUS} is enabled or disabled. Select the appropriate option.

SNMP Communities

Write security: 3; Read security: 5

Defines SNMP manager(s) characteristics. The following options are available for review and editing:

This option...	Does this...
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. The following options are available:

This option...	Does this...
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. (See also "Trap Filtering" below.)

Trap Filtering

You can set filters for the system controller, the switchboard, the Quad Nx56/64 module, the Quad T1/PRI module, and ISDN events. 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 800^{PLUS} MIB for a listing of all traps and their severity levels.)

You can set the following threshold levels for the available selections:

- Disabled
- Major
- Warning
- Info
- Critical
- Minor
- Normal

System Event Logging

Write security: 3; Read security: 5

Sets the system event severity level threshold for each of the ATLAS 800^{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).

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

Write security: 3; Read security: 5

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

Write security: 3; Read security: 5

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/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.



NOTE Passwords are case-sensitive.

Follow this procedure to add or delete passwords:

1. To add new passwords, select the first column **(0)** and press I.
2. To delete a password, select the first column **(0)** and press D.

Each of the six password security levels are described in “Access Rights” on page 5-17.



NOTE *If you lose or forget the ATLAS 800^{PLUS} system administrator password, contact ADTRAN technical support for help in resetting the password. In order to reset the password, you must have access to the front panel. For details on resetting the password, see Password Reset on page 1-30.*

Label

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

Access Rights

Write security: 0; Read security: 5
Defines the password level for the corresponding label. You can select from six different password levels.

If you want the user to...	Select level...
Have read-only permission for all menu items— minimum rights	5
Have read permission for all menu items and permission to use test commands	4
Have access to all commands except passwords, flash download, authentication methods, and interface configurations	3
Have access to all commands except passwords, flash download, and authentication methods	2
Have access to all commands except passwords	1
Have permission to edit every menu item, including creating and editing passwords— maximum rights	0

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 (*****).



NOTE *Passwords are case-sensitive.*

To change the password, follow this procedure:

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.

Active

Read security: 5

Displays the number of users for each label that are currently logged into the system.

SYSTEM UTILITY

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



Figure 5-5. System Utility Menu

Update Firmware

Write security: 1; Read security: 5

Updates firmware when ATLAS 800^{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. 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, see “Updating Firmware” on page 8-1.

NOTE *The available update options change 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. Press Enter, and a new field displays allow-

ing you to select *Slot 1* through *Slot 8* or *All Modules of a Type* (this is useful if there are several identical modules installed in the ATLAS 800^{PLUS}).

Module Type

Write security: 1; Read security: 5

Displays the type of module that is selected in the *Module Slot* option.

If you selected *All Modules of a Type* in the *Module Slot* field, the *Module Type* option allows you to select a particular module type to update all modules of that type.

Transfer Method

Write security: 1; Read security: 5

Indicates the configured transfer method to use in updating firmware. XMODEM transfers files by connecting to a communications program that supports XMODEM uploading to the terminal interface. TFTP transfers software using TFTP protocol 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.

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 module that is being updated. *Restart Immediately After Update* restarts the module immediately after the update is complete. *Restart At Specified Date and Time* allows you to select when the updated module will restart. If 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 day and time to restart the system after updating firmware. 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, 09-30-1998). This field only displays if *Restart Schedule* is set to *Restart At Specified Date and Time*.

Current Update Status

Read security: 5

Displays the status of the current update. This field is read-only.

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

This field...	Does this...
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.

Previous Update Status

Read security: 5

Displays the status of the previous update.

Begin Firmware Update

Write security: 1; Read security: 5

Begins updating the firmware for the selected modules.

Update Status

Read security: 5

Displays the status of the current firmware update. All items are read-only. All of the fields are defined in the previous section, “Current Update Status” on page 5-19.

Config Transfer

Write security: 3; Read security: 5

Transfers a file containing the ATLAS 800^{PLUS} configuration to a file on a TFTP server using the TFTP protocol (a TCP/IP user protocol) through the 10BaseT Ethernet port. *Config Transfer* lets you save the ATLAS 800^{PLUS} configuration as a backup file. You can then use the same configuration with multiple ATLAS 800^{PLUS} units.

You can also use *Config Transfer* to retrieve a configuration file from a TFTP server. ADTRAN delivers a TFTP program with ATLAS 800^{PLUS} called *TFTP Server*. You can configure any PC running Microsoft Windows with this software to store the configuration file. See “TFTP Server” on page 10-4 for details on how to use the TFTP Server software with these menu items to transfer configuration files.



Before using this command, the ATLAS 800^{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 800^{PLUS} unit’s transferred configuration to allow sending identical configurations 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 will transfer to or retrieve from the 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.



CAUTION *If you execute this command, the ATLAS 800^{PLUS} system 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 the TFTP Server Filename field to the server identified in the TFTP Server IP Address field.



CAUTION *Before using this command, you must have identified a valid TFTP server in the TFTP Server IP Address field.*

System Self-test

Conducts a system self-test. The self-test consists of memory tests and data paths to each installed module.



CAUTION *Self-tests disrupt data flow.*

Self-test Run

Write security: 3; Read security: 5

Activates the self-test.

View Self-test Log

Read security: 5

Displays a read-only, time-stamped log of the tests conducted and the Pass/Fail results. The tests associated with the system controller include the following:

This test...	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.

The self-test also verifies 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 test on each installed port is listed with Pass/Fail results. A typical test log is shown in Figure 5-6.

Idx	Time	SI	Pt	Event	Result
1	10:09:14 10/02	0	0	Selftest Started	
2	10:09:15 10/02	0	0	Flash Test	Passed
3	10:09:15 10/02	0	0	Bootrom Test	Passed
4	10:09:15 10/02	0	0	DSP RAM Test	Passed
5	10:09:15 10/02	0	0	RTC RAM Test	Passed
6	10:09:15 10/02	0	0	TDM RAM Test	Passed
7	10:09:32 10/02	0	0	DRAM Test	Passed
8	10:09:36 10/02	0	2	Port Test	Passed
9	10:09:40 10/02	0	1	Port Test	Passed
10	10:09:45 10/02	3	4	Port Test	Passed
11	10:09:49 10/02	3	3	Port Test	Passed
12	10:09:54 10/02	3	2	Port Test	Passed
13	10:09:58 10/02	3	1	Port Test	Passed
14	10:09:59 10/02	0	0	Selftest Completed	Passed

SYS: OK CSU:ONLN 1:WARN 2: -- 3: -- 4: -- 5: OK 6: -- 7: -- 8: --
^Z=help 23:10_

Figure 5-6. View Self-test Log**Clear Self-test Log**

Write security: 3; Read security: 5

Clears the self-test log.

Reboot System

Write security: 2; Read security: 5

Reboots the ATLAS 800^{PLUS}. When you select this command, the following message displays:

Warning! This will reboot the entire system! Confirm (y/n).

Select Y to reboot the system, or N to exit the command.

MODULES

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 5-7 shows the *Modules* menu. (Write security: 3; Read security: 5)

ATLAS 800 PLUS/Modules									
	Slot	Type	Menu	Alarm	Test	State	Status	Rev	
System Info	0	Sys Ctrl	[+]	[OK]	[OFF]	ONLINE	Online		J
System Status	1	ASYNC-16	[+]	[n/a]	[n/a]	ONLINE	Not Ready		A
System Config	2	EMPTY				ONLINE	Empty		-
System Utility	3	EMPTY				ONLINE	Empty		-
Modules	4	EMPTY				ONLINE	Empty		-
Dedicated Maps	5	M56K-16	[+]	OK	OFF	ONLINE	Online		C
Dial Plan	6	EMPTY				ONLINE	Empty		-
	7	EMPTY				ONLINE	Empty		-
	8	EMPTY				ONLINE	Empty		-

SYS: OK CSU:ONLN 1:WARN 2: -- 3: -- 4: -- 5: OK 6: -- 7: -- 8: --
 Access module menus ^Z=help 23:19_

Figure 5-7. 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.

Slot

Write security: 3; Read security: 5

Identifies the slot number. Slot 0 refers to the ATLAS 800^{PLUS} base unit. This field is read-only.

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 800^{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.



NOTE 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.



NOTE *If a module is installed, the module type automatically displays the name of the installed module, and 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 “ATLAS_ 800PLUS Controller T1/PRI Submenu Items” on page 5-25.



NOTE *Only the submenu items for the base T1/PRI menus are described in this manual.*

Alarm

Read security: 5

Displays whether there is an alarm condition on the ATLAS 800^{PLUS} base unit. Press Enter to access the Alarm menu. (Read-only field.)

Test

Read security: 5

Displays whether the ATLAS 800^{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 5-24 for details. Press Enter to access the Test menu.

State

Write security: 3; Read security: 5

Displays whether the module is online or 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.



NOTE *Once a module is installed, you must change the state 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 800^{PLUS} T1/PRI ports and other installed modules. The following messages may display:

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.

Rev

Read security: 5

Displays the hardware revision of the ATLAS 800^{PLUS}.

ATLAS 800^{PLUS} Controller T1/PRI Submenu Items

The *Modules/Menu* submenu 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 T1/PRI controller port (the ATLAS 800^{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 800^{PLUS} Base Unit and T1/PRI ports. The following items are read-only.

- Part Num** Displays the part number of the ATLAS 800^{PLUS}.
- PLL Status** Indicates whether the clock is locked to its specific source.
(Phase Lock Loop)

Alarm Status

Read security: 5

Displays any active alarms. These fields are read-only.

This alarm...	Means this...
Prt	Displays the port number.
Loss of Signal (LOS)	No signal detected on port interface.
Red Alarm (RED)	Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF).
Yellow Alarm (YELLOW)	Remote alarm indicator (RAI) being received on port.
Blue Alarm (BLUE)	Receiving unframed all ones from the port alarm indicator signal (AIS).

This alarm...	Means this...
D Channel Sync (D-Chan)	HDLC framing is operational on PRI D channel. This indication only applies when operating in PRI mode.
Receive Level (Rx 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. These options are read-only.

DS0 status...	Means this...
*	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

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: Current

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. All of these options (except CLR) are read-only. The parameters monitored include the following:

Field...	Provides this status information...
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.

Field...	Provides this status information...
UAS	Unavailable Seconds.
LCV	Line Code Violations.
RCV	Path Code.
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: Current” on page 5-26 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: Current” on page 5-26 for a detailed description.

Configuration

All of the configurable parameters apply to whether the port is connected to a Primary Rate ISDN circuit or a Channelized T1 circuit—dedicated or switched.

This Configuration submenu...	Does this...
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 (Auto Tx Yellow Alarm) Write security: 3; Read security: 5	Enables and disables the transmitting of yellow alarms.
Tx PRMs (Transmit PRMs) Write security: 3; Read security: 5	Enables and disables the sending of PRM data on the facility data link (FDL). The PRM data continues to be collected even if XMIT PRM is disabled (possible only with ESF format).
LBO (Line Build Out) Write security: 2; Read security: 5	Depends on whether the circuit is provisioned for DS1 by the telephone company.
LB Accept (Loopback Accept) Write security: 3; Read security: 5	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 commands temporarily disrupt service.

This Test submenu...	Does this...
Prt	Identifies the port number.
Loc LB (Local Loopback) Read security: 5	Causes loopback on near-end port Line - Metallic loopback Payld - Payload loopback - framing and clocking are regenerated.
Remote LB (Remote Loopback) Write security: 4; Read security: 5	Sends a loopback code to a remote CSU. ANSI FDL Line (Requires ESF mode) ANSI FDL Pyld (Requires ESF mode) AT1 Inband line
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 (Test Pattern Results) Read security: 5	Suppresses excess zeros—indication of sync and errors of received data pattern.
Clr (Test Pattern Results Clear) Write security: 4; Read security: 5	Clears current error counters on test pattern results menu.
Inj (Test Pattern Error Inject) Write security: 4; Read security: 5	Injects errors into transmitted test pattern.

Dedicated Maps

The *Dedicated Maps* menu (Figure 5-8) assigns dedicated connections between any two ports in the unit. For a detailed description of how to set up dedicated maps, refer to “Creating a Dedicated Map” on page 6-1.



Figure 5-8. Dedicated Maps Menu

Activate Map

Write security: 3; Read security: 5

ATLAS 800^{PLUS} allows you to have up to five different dedicated maps with an optional name designator. You can manually activate a map by pressing Enter in this field, and then selecting the appropriate map. You can also select *Auto*, which permits the maps to activate automatically depending on the time and day settings defined in the field *Activate Time* (a submenu of “Create/Edit Maps” on page 5-29).

Current Map

Read security: 5

Displays the name of the currently active dedicated map. This field is read-only.

Create/Edit Maps

This option allows you to create new maps and define settings. To add a new map, press I when the cursor is in the first column. You can also use this option to edit existing maps. ATLAS 800^{PLUS} names the maps in the sequence they are created (Map 1, Map 2, and so on). You can change the names with *Map Name*.

Map Name

Write security: 3; Read security: 5

Displays the name of the dedicated map. You can edit the name by pressing Enter. The name can contain up to 57 alphanumeric characters, including spaces and special characters.

Sort To/From

Write security: 3; Read security: 5

Specifies which field group will be used to sort the connections (sorted on the FROM end point or the TO end points). This is beneficial 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 submenu.



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

#

Displays the number of the dedicated map connection. If you press **l** in this field, ATLAS 800^{PLUS} adds another dedicated map connection, numbered consecutively.

FROM Slot

Write security: 3; Read security: 5

Specifies the slot to use for the FROM 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

Specifies the port in the selected slot to use for the FROM connection.

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 Slot** option. You must input the following information—based on the module type:

DS0 Selection

Write security: 3; Read security: 5

If the selected entry is 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 Read-only.

Indicates which DS0s of the T1 are assigned. DS0 assignment is depicted 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

If the FROM slot is an Nx port, use this field to define the data rate per DS0. You can choose from 64 Kbps or 56 kbps. If the FROM slot is an Nx port, the data rate per DS0 must be set.

Trunk Conditioning

Trunk conditioning is a process which sets known values in the signaling bits and the data field for outgoing DS0s which are cross connected to a T1 port which is experiencing alarms (see Figure 5-9). The trunk conditioning process consists of a 2.5-second transmission (indicating call termination), followed by a continuous transmission signaling the final condition (Seized or Idle) as chosen by the user.

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

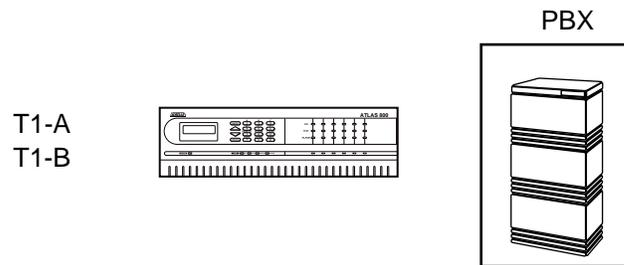


Figure 5-9. Trunk Conditioning

Example:

Voice traffic received on T1-A, and T1-B is groomed onto T1-C to the PBX. If T1-A fails, the DS0s which were cross connected to T1-C would receive trunk conditioning.

Trunk conditioning includes Fault Signaling (setting the state of the signaling bits) and Fault Data Code (setting the state of the data bits). Trunk conditioning can be set for each end of each T1 to T1 connection in a dedicated map. This is simplified by using the copy command (pressing C). The state of the signaling bits will be different for connections to the Network versus connections to user equipment (PBX).

Defining Trunk Conditioning

Write security: 3; Read security: 5

Fault Signaling	Defines to ATLAS the type of signaling being used on the trunk (E&M; LS/GS Network or User; SW56; Custom).
Fault State	Final fault signaling state (Trunk Idle or Seized). Idle would normally be used for one-way trunks (only used for outgoing or incoming calls—not both). Seized would normally be used for two-way trunks. This would prevent the PBX from attempting to use a failed trunk for an outgoing call.
Custom	This permits the user to define the Fault signaling to use in the form of A/B set to 1/0.



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

TO Slot

Write security: 3; Read security: 5

This is the same as *From Slot* (described on page 5-30) except this option designates the second end of a connection.

Port

Write security: 3; Read security: 5

This option selects which port of the *To Slot* will be 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.

RBS (robbed bit signaling)

Write security: 3; Read security: 5

Defines whether the connection has active robbed bit signaling.

Where RBS is not an option, ATLAS 800^{PLUS} automatically assigns the correct setting. (For example, a T1-to-Nx connection is set to Off.)

On 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 will become active if you select AUTO in the *Activate Map* field. Enter this time in hh:mm:ss 24-hour format. If you use this

option, you can select AUTO in the *Activate Map* field (see “Activate Map” on page 5-29).

Enbl Day

Write security: 3; Read security: 5

Specifies which days of the week the map is active.

Dial Plan

Write security: 3; Read security: 5

Dial Plan includes menus for setting global ATLAS switch parameters and for setting individual parameters for each port in ATLAS that handles a switched call (see Figure 5-10). The individual ports are separated into two groups—network ports which terminate a connection from the Network and User ports which terminate incoming calls and in turn may be connected to user equipment.

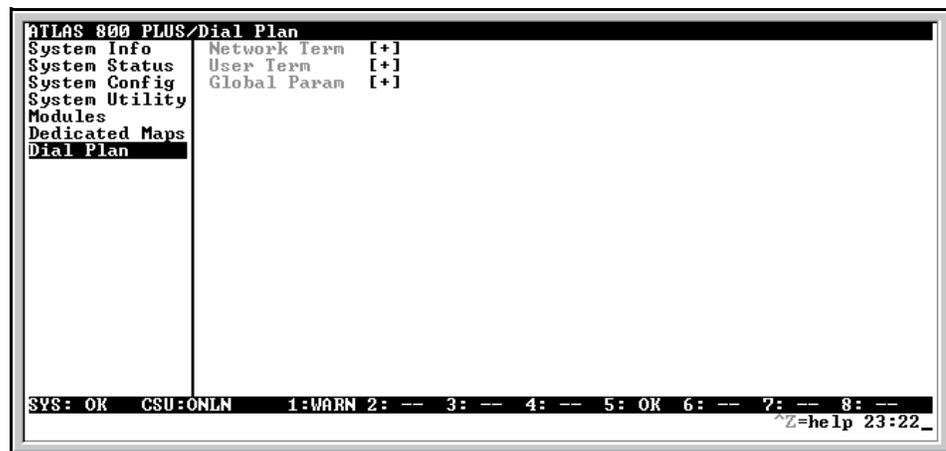


Figure 5-10. Dial Plan Menu



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

Network Term (Terminations)

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



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.



This menu includes a submenu (Interface Configuration) which varies with port type. The section “Interface Configuration” on page 5-41 reflects the options for port types which existed at the release of this manual. This information will also be reflected in the manuals for individual option module types. If the option mod-

ule type being used is not reflected in the Interface Configuration section, please refer to the option module manual for information on the interface parameters.

Slot/Port

Write security: 3; Read security: 5

These fields are used to select the ATLAS port that terminates a Network connection.



There may be more than one “end point” 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 “end points” (trunks) over a single physical port.

Sig (Signalling)

Write security: 3; Read security: 5

Defines the type of signaling being used for this connection (end point). RBS would be for a T1 using Robbed Bit Signaling while PRI designates a Primary Rate ISDN interface. This selection is only necessary if a T1/PRI is selected as the Slot/Port type.

Outgoing#Accept

Write security: 3; Read security: 5

This submenu defines the parameters for the outgoing calls that ATLAS sends to the Network.

Source ID

Write Security: 3 Read Security: 5

This field identifies the ID of the call sources that this endpoint will accept calls from. The Source ID field is used to simplify 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 endpoint is 0 and all accept #'s is 0. This results in all calls being routed based on the dialed number.

Accept Numbers

This field designates which numbers this end point will pass on toward the Network (PSTN). The accept list may consist of multiple entries. The numbers are defined using “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

Example: 1-800-\$ would only permit toll free long distance calls to 1-800. If this were used, then a second accept # would need to be specified - NXX-XXXX. This would permit local numbers to be dialed.



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

Data 64 kbps, Analog, Speech, and Treat Call As

These options reflect 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.

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.

Search

Write Security: 3 Read Security: 5

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 end point if all Primary end points were unavailable.

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.

Out#Rej

Write security: 3; Read security: 5

This submenu defines the parameters for the outgoing calls that ATLAS will not send to the Network.

Reject Numbers

This field identifies which numbers this end point 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.



NOTE *The Reject list takes precedence over the Accept list.*

Examples:

1- 900-\$ would reject all 1-900 long distance calls.

1-\$ would reject all long distance calls.

Data 64 Kbps, Analog, Speech, and Treat Call As.

These items allow ATLAS to reject outgoing calls based on call type.

Example:

A “\$” for the Reject Number and Digital 56/64 enabled and Audio & Speech Disabled would reject all digital calls while not rejecting analog calls.



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

Interface Configuration

This menu sets configuration parameters for the end point. These parameters will vary by the type of port selected. For detailed information on the interface configuration for all of the available modules, refer to “Interface Configuration” on page 5-41.

User Terminations

This menu allows you to define option parameters for ports which terminate a connection from user equipment. In this case, ATLAS 800^{PLUS} is acting like the Network.



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 (set up as a User Termination), while the ATLAS at the opposite end would be terminating a Network connection.

Slot/Port (Select list of option modules/ports)

Write security: 3; Read security: 5

These fields are used to select the ATLAS port that terminates a User connection.



There may be more than one “end point” 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 would constitute multiple “end points” over a single physical port.

Signaling: (User Selection - RBS; PRI)

Write security: 3; Read security: 5

Defines the type of signaling being used for this connection (end point). RBS would be for a T1 using Robbed Bit Signaling while PRI designates 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

This submenu defines the parameters for incoming calls that ATLAS 800^{PLUS} will accept from the Network.

Source ID

Write Security: 3 Read Security: 5

This field identifies the ID of the call sources that this endpoint will accept calls from. The Source ID field is used to simplify the creation of a Dial Plan in applications where the criteria 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 endpoint is 0 and all accept #'s is 0. This results in all calls being routed based on the dialed number.

Accept Numbers

Write security: 3; Read security: 5

This field designates which numbers this end point will accept (terminate) from the Network (PSTN). The accept list may consist of multiple entries. The numbers are defined using “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

Example:

963-8000 would be a specific incoming number that would be accepted by this end point. If this end point 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 end point “A” was designated as \$ while end point “B” accepted 963-800X, then an incoming call to 963-800X would only be accepted by end point “B.”

Search

Write Security: 3 Read Security: 5

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 end point if all Primary end points were unavailable.

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 64kbps/Data 56kbps/Analog/Speech

Write security: 3; Read security: 5

This reflects the bearer capability that the attached user equipment (typically a TA) has. If the attached TA can only handle digital calls, then a voice call sent to this end point would be rejected.

Treat Call As

Write security: 3; Read security: 5

This allows you to treat an incoming voice call (as designated by the ISDN call type identifier) as a data call. This is useful if the ISDN lines are provisioned for voice but are actually being used for data.

Out#Rej (Outgoing Number Reject List)

Write security: 3; Read security: 5

This submenu is used to define the parameters for outgoing calls that ATLAS 800^{PLUS} will not send to the Network.

Reject Numbers

This field designates which numbers this particular end point will NOT pass on toward the Network (PSTN). This is used when the outgoing call filter is different for different users. The “wild cards” are identical as in Outgoing Call Accept.

Example:

If desired, each user termination port can be set to reject different numbers.



[0,1]-\$ would reject all long distance calls, but only for this user termination. If permitted in the Network Termination end point, this user could not dial long distance numbers while other users could.

Data 56kbps/Data 64kbps/Audio/Speech

These items allow ATLAS 800^{PLUS} to reject outgoing calls based on call type.

Example: A “\$” for the Reject Number, Digital 56/64 enabled, and Audio & Speech Disabled would reject 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.

Interface Configuration

This menu sets configuration parameters for the end point. These parameters will vary by the type of port selected. For detailed information on the interface configuration for all of the available modules, refer to “Interface Configuration” on page 5-41.

Global Parameters

These menus set ATLAS options which will apply to all switched operations, both incoming and outgoing calls.

End of Number Timeout

Write security: 3; Read security: 5

This parameter sets the length of time ATLAS will wait 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.

Area Code

Write security: 3; Read security: 5

The local area code. This is used for sending caller ID to the Network.

Number Complete Template

Write security: 1; Read security: 5

For any outgoing call, ATLAS must be able to recognize when the phone number is complete. For example, a local number will be seven digits long while a long distance (1+ #) will be 11 digits long. The ATLAS defaults will cover almost any installation, and these templates should not require any additional user input except for unusual circumstances. The template allows the use of “wildcard” 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

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.

Number Type Templates

Write security: 1; Read security: 5

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 national long distance call type while a “011 +” prefix would be 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. 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

WARNING *Use extreme caution when disabling this option!*

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.

Interface Configuration

The *Interface Configuration* option for the *Dial Plan* menu sets configuration parameters for the end point. These parameters vary by the type of port selected. The following sections describe the configuration options for each available type of module and port that existed when this manual was released. Configuration information for specific modules is also located in the manual for each module. If configuration information for a particular module you are using is not described in the following sections, please refer to the module manual for information on the interface parameters.

Quad T1/PRI Module Interface Configuration

This section describes the Network Termination and User Termination configuration settings for the Quad T1/PRI module when using the *Dial Plan* menus.

Quad T1/PRI Module (Network Termination/PRI)

When you are working in the Network Termination section of the *Dial Plan* menu, the 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 following options are available:

- Lucent 5E
- Northern DMS 100
- National ISDN
- AT&T 4ESS

First DS0

Number of DS0s

Write Security: 3 Read Security: 5

These two items permit fractional PRI to be defined. These menu items define the first active DS0 and 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

This item 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

This option allows a selected quantity of the Most Significant Digits (MSD) of a dialed number for ATLAS to be stripped prior to being forwarded out of the port.

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

This option allows for the definition of specific facility IEs be sent to the Network. This would be used if the customer has subscribed to special facilities 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

This option allows for the definition of specific facility IEs be sent to the Network. This would be used if the customer has subscribed to special facilities 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

Some PRI switches may be provisioned to only send a portion of the called number (like DID). This menu item allows ATLAS to know how many 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.

Outgoing Caller ID

Write Security: 3 Read Security: 5

This item allows the user to insert a called ID based on selection. 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 will insert a User defined ID value if no value is received. If set to **Substitute Always**, then ATLAS will always insert the user-defined ID in place of the value 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).

Source ID

The *Source ID* field simplifies the creation of a Dial Plan in applications where the criteria for switching calls to a certain end point is a function of which end point originated the call.

- Default value = 0. The default ID for all end points is 0 and for all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple end points 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.

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

This option 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 will cause the ATLAS switchboard to use ANI to route the call. The accept # in the dial plan must use the ANI number, not the DNIS number.

Quad T1/PRI Module (Network Termination/RBS)

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

First DSO

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.

DSOs Available

Read security: 5

Indicates which DSOs of the T1 have been defined in this switched end point (indicated by “!”), in another switched end point (indicated by “s”), or in a Dedicated Map (indicated by “n”). This field is read-only.

The following symbols may display in this field:

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

Trunk Type (Voice/SW56)

Write security: 3; Read security: 5

This is used if the incoming service on this trunk is Switched 56 digital instead of standard voice.

Signaling Method

Write security: 3; Read security: 5

This 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 following choices are available:

- E&M Immediate
- E&M Wink
- Loop Start
- Ground Start

Direct Inward Dialing

Write security: 3; Read security: 5

This defines to ATLAS whether or not 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 end point 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

When the Network connection does not provide DID digits, then ATLAS must be given a number to use to determine which user end point should receive the incoming call. This field only displays when Direct Inward Dialing is set to Disabled.



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

Example: If a certain incoming DS0 (trunk) is meant to connect to an end point with the accept number of 963-8615, the trunk number would be set to 963-8615.

Strip MSD

Write Security: 3 Read Security: 5

This option 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.

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.



NOTE 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

The *Source ID* field is used to simplify the creation of a Dial Plan in applications where the criteria for switching calls to a certain end point is a function of which end point originated the call.

- Default value = 0. The default ID for all end points is 0 and all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple end points 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.

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, the 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.

- Lucent 5E
- AT&T 4ESS

First DSO

Number of DSOs

Write Security: 3 Read Security: 5

These two items permit fractional PRI to be defined. These menu items define the first active DSO and the number of DSOs used for calls on this PRI. DSO 24 is assumed to be used by the PRI for the “D” channel.

Strip MSD

Write Security: 3 Read Security: 5

This option allows a selected quantity of the Most Significant Digits (MSD) of a dialed number for ATLAS to be stripped prior to being forwarded out of the port.

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.



NOTE 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

This option defines the specific facility IEs be sent to the Network. This would be used if the customer has subscribed to special facilities 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

This option defines the specific facility IEs be sent to the Network. This would be used if the customer has subscribed to special facilities 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

This item allows the user to insert a called ID to be added 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 will insert a User defined ID value if no value is received. If set to **Substitute Always**, then ATLAS will always insert the User defined ID in place of the value received.

ID Presentation

Defines control information for the presentation of Caller ID to be inserted: (**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

The *Source ID* field simplifies the creation of a Dial Plan in applications where the criterion for switching calls to a certain end point is a function of which end point originated the call.

- Default value = 0. The default ID for all end points is 0 and all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple end points 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.

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

This option 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.



NOTE *This swap will occur after the ATLAS switchboard has routed the call. The accept # in the dial plan must use the number in the DNIS position prior to swapping.*

Quad T1/PRI Module (User Termination/RBS)

When you are working in the User Termination section of the Dial Plan menu, the 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 end point. 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 end point (indicated by “! “), in another switched end point (indicated by “s”), or in a Dedicated Map (indicated by “n”).

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 endpoint.
s	This DS0 is used elsewhere in the switched dialplan.
S	This DS0 is in the switched dialplan and conflicts with this endpoint.
n	This DS0 is used in one or more dedicated maps.
N	This DS0 is in one or more dedicated maps and conflicts with this endpoint.

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 choices are:

- E&M Immediate
- E&M Wink
- Loop Start
- Ground Start



NOTE ATLAS converts signaling types between Network and User Terminations.

Direct Inward Dialing

Defines to ATLAS whether DID is used by the user equipment. If DID is **Enabled**, then the following information must be defined:

DID Digits Transferred

Defines the number of digits ATLAS is to send on to the user equipment. This field only displays if *Direct Inward Dialing* is set to **Enabled**.

Caller ID Number

Defines the number for ATLAS to use to provide Caller ID to the Network for outgoing calls sent through this end point. This option only displays if *Direct Inward Dialing* is set to **Disabled**. This item is optional.



NOTE *The Caller ID number must be specific (i.e., no “wild cards”).*

Strip MSD

Write Security: 3 Read Security: 5

This option 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.

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.



NOTE *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

The *Source ID* field simplifies the creation of a Dial Plan in applications where the criteria for switching calls to a certain end point is a function of which endpoint originated the call.

- Default value = 0. The default ID for all end points is 0 and all accept # s is 0. With default values, all calls are routed based only on dialed number.
- Multiple end points 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.

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 Interface Configuration

This section describes the *User Termination* configuration settings for the Quad Nx56/64 Module when using the *Dial Plan* menus.



The Quad Nx56/64 can only serve as a user termination end point

Quad Nx56/64 Module (User Termination)

When you are working in the *User Termination* section of the *Dial Plan* menu, and the *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 end point (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.

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 Configuration

This section describes the *Network Termination* and *User Termination* configuration settings for Octal BRI module when using the *Dial Plan* menus.

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 the *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. Choices include the following:

- Lucent 5E
- Northern DMS 100
- 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 is capable of acting like the Network while interfacing to user equipment (terminal adapters). When you are working in the *Network Termination* section of the *Dial Plan* menu and the *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 following options are available:

- Lucent 5E
- Northern DMS 100
- 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	This entry will define 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.
 NOTE	<i>ATLAS 800^{PLUS} does not support autoSPID detection software which some terminal adapters offer.</i>

Calls	For User terminations, the number of calls is fixed at 2.
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.

OVERVIEW

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 capable of supporting dedicated bandwidth.

Figure 6-1 shows an example of a dedicated map:

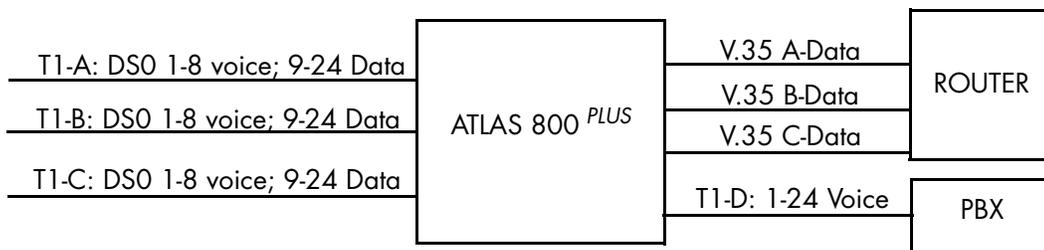


Figure 6-1. Dedicated Map Overview Example

For this example, there are three T1s (T1-A, T1-B, T1-C) with dedicated bandwidth from three remote sites. Each includes DS0s for data and for voice. At the central site, each incoming DS0 for data must be mapped to a separate V.35 port for connection to the router, while the voice connections must be collected together (groomed) and sent to the PBX over a single T1 (T1-D).

Dedicated Map Design**Connections**

The first step is to determine what connections need to be made and which ports are involved. For the T1 ports, you also need to decide which DS0s will be used. Table 6-1 on page 6-2 shows the connections used in the following example.

Table 6-1. Connections

Name	ATLAS 800 <i>PLUS</i>	DSOs	Name	ATLAS 800 <i>PLUS</i> Port	DSOs
T1-A Data	Controller T1 Slot 0 Port 1	9-24 RBS Off	V.35 - A	Quad V.35 Slot 2/Port 1	N/A
T1-B Data	Controller T1 Slot 0/Port 2	9-24 RBS Off	V.35 - B	Quad V.35 Slot 2/Port 2	N/A
T1-C Data	Quad T1/PRI Slot 1/Port 1	9-24 RBS Off	V.35 - C	Quad V.35 Slot 2/Port 3	N/A
T1-A Voice	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-B Voice	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-C Voice	Quad T1/PRI Slot 1/Port 1	1-8 RBS On	T1-D	Quad/PRI DSX Slot 1/Port 2	17-24 RBS On

Configure the Ports

1. From the Terminal menu, navigate to the Module menu and select *Controller T1/PRI port (slot 0)*. Select Menu [+], then the *Configuration* submenu, then set the line framing parameters. Once properly configured to match the framing parameters of the T1 line being provided by the Telco, copy the configuration information by navigating to the first column (*port index number*) of this port and pressing C. (See Figure 6-2.)

```

ATLAS 800 PLUS/Modules[0]/Sys Ctrl Menu/Configuration[2]/Transmit PRMs
Controller Info
Alarm Status
DS0 Status
Sig Status
Performance: Curr
Performance: 15 Min
Performance: 24 Hr
Configuration
Test

```

Prt	Port Name	Frame Code	Ix Vel	Ix PRM	LR0	LR Accept
1	T1-A	ESF AMI	On	Off	0 dB	Accept
2	T1/PRI	ESF B8ZS	Off	Off	0 dB	Accept

```

SYS: OK   CSU:ONLN  1:WARN 2: -- 3: -- 4: -- 5: OK 6: -- 7: -- 8: --
Ix PRM each Second                                     ^Z=help 23:30_

```

Figure 6-2. Slot 0 Module Configuration Menu

2. Navigate to the **Port** index number of the second port and paste the configuration by pressing **P**. Repeat for the first port of the T1/PRI card located in Slot 1.
3. Navigate to the **V.35 Port Configuration** menu and repeat the configuration of the first port followed by copy and paste to the second and third ports.

Implement the Map

1. Navigate to the **Dedicated Map** menu and select **Create /Edit Map**. If desired, enter a name for the map by pressing **Enter** when the cursor is over **Map Name**. Type the desired name in the entry box.
2. Select the **Connects** submenu. Using Table 6-1 on page 6-2, define each of the connections necessary to route the bandwidth as desired. For the example, there will be a connection for each of the connections shown in Table 6-1 on page 6-2. The entries are made as follows (a completed map is shown in Figure 6-3).
 - A. Select the **FROM Slot** for Data A (i. e., Controller T1).
 - B. Select the **FROM Port** (i.e. Port 1 for T1-A Data).
 - C. Using the **FROM Configuration** submenu select the DS0s (i.e. 9-24 for Data A).
 - D. Select the **TO Slot** and **TO Port** the same way (V.35 in Slot2 / Port 1 for Data A).
 - E. Using the **Configuration** submenu, set the V.35 to operate at 56k / 64k per DS0.
 - F. Repeat for the remaining Data connections (i. e., Data B and Data C).
 - G. Insert new connection lines by typing **I** with the cursor over the **Index #** of the first connection.
 - H. Copy the first connection by pressing **C** with the cursor on the **Index #**.
 - I. Paste this onto a new connection line by typing **P** with the cursor over the index numbers of the new connections.
 - J. Modify these connection lines to complete the connections for data.
 - K. Select the **FROM Slot** and **FROM Port** for the first voice connection (i. e., Slot 0/Port 1 for T1-A Voice).
 - L. Repeat step C to select the voice DS0s (i. e., 1 through 8 for Voice A).
 - M. Select the **TO slot/Port** (PBX Connection) as in D above (i. e., Quad T1/PRI in Slot 1/Port 2).
 - N. Using the **Configuration** submenu, 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 sets the **DACSing** between the T1s.

- O. Set **RBS** to **On** for the *Voice* connections.
- P. **(Optional)** Using the *Configuration* submenu, set the trunk conditioning (Signaling and *Data* code) desired for T1 failure.
- Q. Repeat for the remaining *Voice* connections as in steps F through J above.



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.

ATLAS 800 PLUS/Dedicated Maps/Create/Edit Maps						
Create/Edit Maps						
	Map Name	Sort	IO/PROH	Connects	Activate Time	Enbl Day
1	Map 1		FROM	[Cncts=0]	00:00:00	[Enable]
2	Map 2		FROM	[Cncts=0]	00:00:00	[Disabl]
3	Map 3		FROM	[Cncts=0]	00:00:00	[Disabl]
4	Map 4		FROM	[Cncts=0]	00:00:00	[Disabl]
5	Map 5		FROM	[Cncts=0]	00:00:00	[Disabl]

SYS: OK CSU:ONLN 1:WARN 2: --- 3: --- 4: --- 5: OK 6: --- 7: --- 8: ---
 ^Z=help 23:36

Figure 6-3. Completed Dedicated Map

OVERVIEW

The ATLAS Dial Plan acts as the numbering plan for switched connections. This menu defines to ATLAS the phone numbers and features associated with dial-up ports. ATLAS supports Robbed Bit Signaling (RBS) T1 interfaces using DTMF dialing, Primary Rate ISDN (PRI) and Basic Rate ISDN (BRI). In order to operate as a switch, ATLAS must be able to terminate network connections (Network Terminations) and emulate the Network into other termination equipment (User Terminations).

Understanding the Application

In order to create a switched Dial Plan successfully, the topology of the configuration must be understood. First you have to understand which of the connections are acting as Network Terminations and which are acting as User Terminations.

The examples provided in Figure 7-1 and Figure 7-2 are used to clarify these definitions:

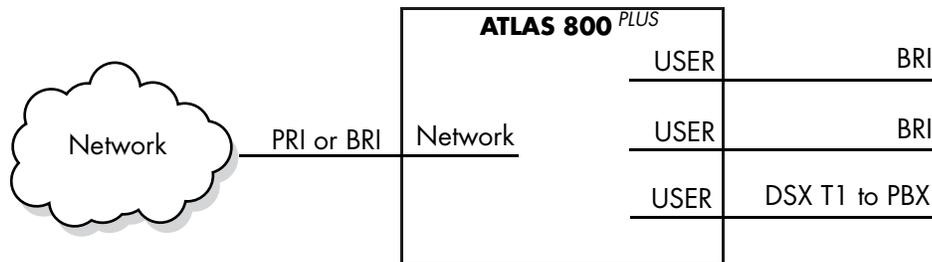


Figure 7-1. Case 1: PSTN Connection

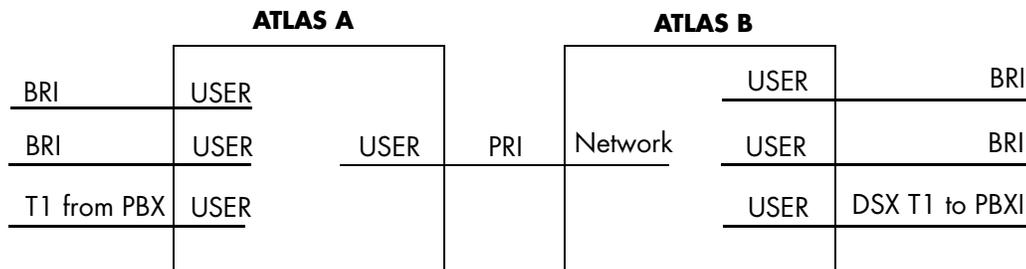


Figure 7-2. Case 2: Point-to-Point

One ATLAS 800^{PLUS} (A) operates as the network while the other (B) “terminates” the network. In the example in Figure 7-2, ATLAS A is emulating the network and the PRI interface is a User Termination, while the PRI interface of ATLAS B is a Network Termination.

Understanding the Dial Plan

The Dial Plan menus are subdivided into three separate menus. These include menus to enter the numbering plan for Network Terminations and User Terminations, and a menu to set global parameters.

A corporate office has T1 RBS service for voice, but wants to add a PRI for video conferencing and remote access. They would like to use the PRI for all functions but still want to use the incoming BRI to supply added bandwidth. They want to provide BRI lines to the video equipment, provide a PRI to the remote access server (RAS) and send an RBS T1 to the PBX. (see Figure 7-3).

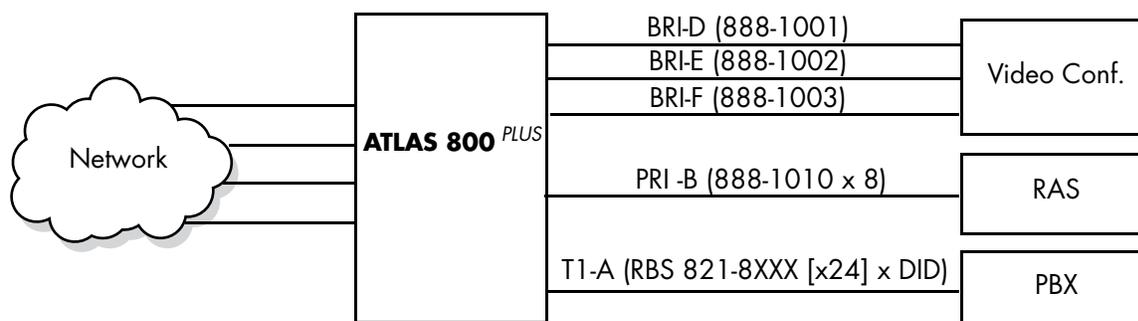


Figure 7-3. Remote Access and Video Conferencing Setup

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 to be restricted.

Also assume that the Network Termination BRI lines (BRI A, B, C) should only allow outgoing calls to other local corporate offices for Video conferencing. The numbers fall in the range of 888-0100 to 888-0120

Configure the Ports

Follow the steps described in the “Creating a Dedicated Map” on page 6-1 to configure the Controller T1/PRI interfaces. This configuration action only brings up the T1 transport.

The BRI configuration (SPID and phone number) is part of the Dial Plan.

Plan the Dial Plan

1. Determine the provisioning of the Network, and the attached equipment (video equipment and PBX).

Network PRI	<p>Type of PRI switch being provided: National ISDN DMS 100 custom 4ESS custom 5ESS custom DID- Number of digits</p> <p>Type of BRI switch being provided: National ISDN DMS 100 custom 5ESS custom SPID(s) and phone number(s) provisioned for the BRI line</p>
--------------------	---

User Equipment	<p>PRI Switch type the user equipment expects to interface to (ATLAS supports 5ESS custom.</p> <p>DID Number of digits.</p> <p>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.</p> <p>T1 RBS DID enabled on PBX/Number of digits; Signaling (E&M/Loop Start/Ground Start).</p>
-----------------------	--

2. Enter the local Area Code number (needed for Caller ID operation) under the Global Parameter submenu below the Dial Plan menu.
3. Determine which ports are Network Terminations and which are User Terminations. Define the phone number acceptance and rejection criteria for each.

For our example there is one PRI port terminating the network (PRI - A) and three BRIs (BRI A, B, C). (See Table 7-1 on page 7-4.)

Table 7-1. 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,B,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, and 888-1010 (All)

For User Termination, there is one PRI, one RBS T1, and three BRIs (see Table 7-2 on page 7-5).

Table 7-2. User Termination

NAME	PORT	INCOMING ACCEPT #	OUTGOING REJECT #	OTHER
BRI D,E,F	Octal BRI Slot 1, Port 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 numbers: 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 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 Accepts all calls beginning with 821-8.	1-900-\$ Rejects all calls beginning with 1-900.	RBS 1st DSO=1; #DSO = 24 Signalling = E&M wink DID = Enable/# of digits = 4

Implement the Dial Plan

1. Using the terminal menus, navigate to the Dial Plan menu.
2. Select the Global Parameter submenu. Select the Area Code option and enter the area code. Press Enter when you're done.
3. Navigate to the Dial Plan submenu and select Network Term (Terminations).
4. For PRI A, select Slot 0/Port 1. Select PRI under Sig to define to ATLAS the interface type to be PRI.

5. Select the Out (Outgoing) # Accept submenu. Enter \$ in the number field. Leave all other selections set to default (Enabled).
6. Select the Out (Outgoing)# Reject submenu. Since no outgoing numbers need to be rejected at this port, no entry is required.
7. Select Interface Configuration (Ifce Config) submenu. Select the PRI switch type (National ISDN).
8. Press **ESC** to back out of the connection to the index number column.
9. Type **I** three times to insert another three connections in the list for the BRI lines.
10. Select Slot 1/ Port 1 for BRI A. Enter the Outgoing Accept and Reject numbers as in steps 5 and 6. The Outgoing Accept numbers have two entries:

```
888-01[0,1]X
888-0120
```

11. This allows all numbers 888-0100 to 888-0120.
12. Navigate to the Interface Configuration submenu. Select the BRI switch type the network is using (National ISDN). Descend into the SPID submenu and enter the SPID numbers and phone numbers which match the network provisioning for this BRI line.
13. Press **ESC** to return to the Index # column.
14. While on the entry for BRI A, type **C** to copy the entire BRI A entry.
15. Move to the next connection list entry and type **P** to paste all of the BRI data. Move to each field and modify as appropriate for BRI B.
16. Repeat 13 and 14 for BRI C.
17. After completing the network entries, the network connection map should appear (see Figure 7-4).

ATLAS 800 PLUS/Dial Plan/Network Tern							
Network Tern	#	Slot	Port	Sig	Out#Accept	Out#Rej	Ifce Config
User Tern	1	0>Sys	Ctrl	1>T1-A	PRI	[+]	[+]
Global Param							[+]

SYS: OK CSU:ALRM 1:WARN 2: -- 3: -- 4: -- 5: OK 6: -- 7: -- 8: --
Terminations of connections to the network ^Z=help 23:43

Figure 7-4. Completed Network Map

After completion, the User Map should appear (see Figure 7-5).

ATLAS 800 PLUS/Dial Plan/User Term							
Network Term	#	Slot/Vec	Port/Link	Sig	In#Accept	Out#Rej	Ifce Config
User Term	1	1>ASYNC-16	1>Async1/		[963-0001]	[+]	[port 1]
Global Param	2	1>ASYNC-16	2>Async1/		[963-0002]	[+]	[port 2]
	3	1>ASYNC-16	3>Async1/		[963-0003]	[+]	[port 3]
	4	1>ASYNC-16	4>Async1/		[963-0004]	[+]	[port 4]
	5	1>ASYNC-16	5>Async1/		[963-0005]	[+]	[port 5]
	6	1>ASYNC-16	6>Async1/		[963-0006]	[+]	[port 6]
	7	1>ASYNC-16	8>Async1/		[963-0008]	[+]	[ports 8-15]

SYS: OK CSU-ALRM 1:WARN 2: -- 3: -- 4: -- 5: OK 6: -- 7: -- 8: --
Termination of connections to user equipment ^Z=help 23:45

Figure 7-5. 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.

FIRMWARE UPDATING

To provide feature enhancements in the future, the ATLAS supports firmware updating by field personnel. Two transfer methods are available for use in updating any modules that contain Flash memory, including the system controller of the ATLAS. The first transfer method provided is via the ATLAS Chain-In port using XMODEM protocol. The second transfer method provided by ATLAS 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 use in updating any upgradable module within ATLAS. The following sections describe the procedure for updating using either transfer method.

**NOTE**

Please consult the appropriate ATLAS module manual to determine if the module supports flash upgrading.

XMODEM FIRMWARE UPDATING

The ATLAS 800^{PLUS} supports firmware updating to any upgradable module using XMODEM transfer protocol via the base unit's Chain-In port. This transfer protocol can be found in most PC communications software packages. To configure the Chain-In port's data rate and other communication parameters, consult the Chain Port Configuration section in the chapter "Installation" on page 2-1.

**NOTE**

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

Update Firmware Using XMODEM

1. Obtain the appropriate update file for the particular module from ADTRAN Technical Support. For more information on how to contact ADTRAN Technical Support, refer to "Warranty and Technical Support Information" on page C-1.
2. Log in to ATLAS using a VT-100 terminal emulation communication software package which contains XMODEM protocol support.



A Level 2 password is required for performing updates of any module within ATLAS. Please consult the ATLAS administrator if you do not know the password.

3. Select the *System Utility* menu.
4. Select *Update Firmware*. Figure 8-1 shows the *Update Firmware* menu.

```

ATLAS 800 PLUS/System Utility/Update Firmware/Module Slot
Update Firmware      Module Slot      Slot 0
Update Status        Module Type      Sys Ctrl
Config Transfer      Transfer Method  TFTP
System Utilization   TFTP Server IP  0.0.0.0
System Selftest      TFTP Server File
Restart Schedule     Restart Schedule Restart Immediately after Update
Current Update Status Idle
Previous Update Status Has not been attempted
Begin Firmware Update <+>

SYS: OK  CSU:ALARM  1:WARN 2: -- 3: -- 4: -- 5: OK 6: -- 7: -- 8: --
Select module slot number                               ^Z=help 23:46_

```

Figure 8-1. Update Firmware Menu Interface

5. Move to the *Module Slot* field.
6. Press Enter and select the appropriate module slot to update.



To update multiple modules of the same type, select *All Modules of a Type* from the *Module Slot* field.

After selecting a slot number, the *Module Type* field updates to reflect the type of unit selected. This field is read-only.

7. The *Module Type* field is normally a read-only field indicating the type of module that is currently in the selected slot. If you choose *All Modules of a Type* for the *Module Slot* field, the *Module Type* field becomes configurable to indicate what type of modules to update in the ATLAS. Select the appropriate module type for the particular update.



Only modules which are upgradable are displayed as choices for the *Module Type* field when updating all modules of a type in the ATLAS.

8. Select *XMODEM* for the *Transfer Method* field.
9. In the *Restart Schedule* field, select the desired time for the module to perform a restart after completing the update process. Restarting the ATLAS 800^{PLUS} invokes the new code. For the system controller, you can select either *Restart Immediately After Update* or *Restart at Specified Date and Time*. The *Restart Immediately After Update* option instructs ATLAS to automatically restart the module immediately after the update process has

completed. The *Restart at Specified Date and Time* option allows you to select a date and time at which the ATLAS will automatically restart the module after the update process has completed. For modules which reside in expansion slots, the *Restart at Specified Date and Time* option is not available since the modules are unable to maintain normal operation during the update process.

10. If you select the *Restart at Specified Date and Time* option in the *Restart Schedule* field, the *Restart Date and Time* field displays to allow entering a date and time at which the restart of the module will occur.
11. The *Current Update Status* field displayed next is a read-only field indicating the progress of the current firmware update or any errors encountered during the download process. This field displays **Idle** if no firmware update is currently in progress. At the end of an update, the *Current Update Status* field's contents are copied into the *Previous Update Status* field, which is displayed next. If *All Modules of a Type* is selected for the *Module Slot* field, the *Current Update Status* field becomes a menu selection which allows the firmware update status of all the modules to display.
12. The *Previous Update Status* field indicates the results of the last firmware update for the particular slot chosen. If a firmware update has not been attempted for the particular slot, the *Previous Update Status* will display: **Has not been attempted**.
13. After completing the configuration of all the above parameters, select *Begin Firmware Update* to start the update process. This field requires user confirmation and will set up the module to receive the XMODEM upload from the VT-100 terminal emulation software.
14. 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.
15. In the terminal emulation software, begin an XMODEM upload by using the appropriate command sequence. Please refer to terminal emulation software documentation for help. When specifying the filename, make sure the file transferred is the one provided by ADTRAN. Otherwise, the update will not complete successfully.
16. 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 point in time within the terminal emulation software. Please consult the documentation provided by the terminal emulation software for instructions.
17. When the update process has completed successfully, the menu screen will display **Idle** in the *Current Update Status* field and *Module Update Complete* in the *Previous Update Status* field. In the event an error occurred during the update process, the *Previous Update Status* field will display the appropriate error message.
18. If the update of the module was successful, the module will restart either immediately and resume operation or restart at the specified time and day of the week, depending on your selection.
19. To update additional modules, go to Step 6 and select the appropriate slot.

TFTP FIRMWARE UPDATING

The ATLAS product supports updating of firmware to any module via the 10BaseT port using TFTP from a network server. The network server must be capable of supporting TFTP server requests from the TFTP Client within ATLAS.

Update Firmware Using TFTP

1. Obtain the appropriate update file for the particular module from ADTRAN Technical Support. For more information on how to contact ADTRAN Technical Support, refer to “Warranty and Technical Support Information” on page C-1.
2. Copy the update file provided by ADTRAN to a network server that supports TFTP server requests. Please record the IP address of the server and full path location of the update file to be downloaded by the ATLAS TFTP client.
3. Log in to ATLAS using a Telnet program.



NOTE *A Level 2 password is required for performing updates of any modules within ATLAS. Please consult the ATLAS administrator if this password is not known.*

4. Select the *System Utility* menu.
5. Select the *Update Firmware* option to gain access to the *Update Firmware* menu interface for performing updates. This menu is shown in Figure 8-2.
6. Move to the *Module Slot* field.
7. Press Enter and select the appropriate slot of the module to update.



NOTE *To update multiple modules of the same type, select All Modules of a Type for the Module Slot field.*

After selecting a slot number, the *Module Type* field updates to reflect the type of unit selected (this field is read-only).

8. The *Module Type* field is normally a read-only field indicating the type of module that is currently in the selected slot. If you choose *All Modules of a Type* for the *Module Slot* field, the *Module Type* field becomes configurable to indicate the type of modules to update in the ATLAS. Select the appropriate module type for the particular update (see Figure 8-2 on page 8-5).

```

Telnet Connection - 127.0.0.1
Session Edit Options Capture About
ATLAS 800 PLUS/System Utility/Update Firmware/Module Slot
Update Firmware Module Slot Slot 0
Update Status Module Type Sys Ctrl
Config Transfer Transfer Method TFTP
System Selftest TFTP Server IP Address 0.0.0.0
TFTP Server Filename
Restart Schedule Restart Immediately after Update
Current Update Status Idle
Previous Update Status Has not been attempted
Begin Firmware Update <+>

SYS:ALARM CSU:ONLN 1:ALARM 2:ALARM 3:ALARM 4:ALARM 5:ALARM 6:ALARM 7:ALARM 8:ALARM
Select module slot number                               Z=help 15:01

```

Figure 8-2. Update Firmware Menu Interface

NOTE Only Modules which are upgradable display as choices for the Module Type field when updating all modules of a type in the ATLAS.

9. Select TFTP for the *Transfer Method*. The ATLAS menu now displays two additional fields which must be entered for TFTP transfers.
10. In the field *TFTP Server IP Address*, enter the IP address of the network server that was recorded in Step 2. ATLAS uses this field to locate the network server on which the update file resides.
11. In the field *TFTP Server Filename*, enter the full path name and file name of the update file that was recorded in Step 2.
12. In the *Restart Schedule* field, select the desired time at which the module will perform a restart after completing the update process. For the system controller, you can select either *Restart Immediately After Update* or *Restart at Specified Date and Time*. The *Restart Immediately After Update* option informs ATLAS to automatically restart the module immediately after the update process has completed. The *Restart at Specified Date and Time* option allows you to select a date and time at which the ATLAS will automatically restart the module after the update process has completed. For modules which reside in expansion slots, the *Restart at Specified Date and Time* option is not available since they are unable to maintain normal operation during the update process.
13. If the *Restart at Specified Date and Time* option is selected in the *Restart Schedule* field, the *Restart Date and Time* field is provided to allow entering a date and time at which the restart of the module will occur.
14. The *Current Update Status* field displayed next is a read-only field indicating the progress of the current firmware update or any errors encountered during the download process. This field displays *Idle* if no firmware update is currently in progress. At the end of an update, the contents of the *Current Update Status* field are copied into the *Previous Update Status* field, which is displayed next. If *All Modules of a Type* is selected for the *Module Slot* field, the *Current Update Status* field becomes a menu selection which allows the firmware update status of all the modules to display.

15. The *Previous Update Status* field indicates the results of the last firmware update for the particular slot chosen. If a firmware update has not been attempted for the particular slot, the *Previous Update Status* will display **Has not been attempted**.
16. After completing the configuration of all the above parameters, select the *Begin Firmware Update* field to activate the update process. This field requires user confirmation and will set up the module to initiate a TFTP upload with the specified network server. Once the update process begins, this field changes to **Cancel Update** to allow you to cancel the current update in progress.
17. During the TFTP upload process, various status messages will be provided in the *Current Update Status* field to indicate progress. These are described as follows:

TFTP - 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.
TFTP - 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.
TFTP - Completed	Indicates the ATLAS product successfully received the update file.
TFTP - 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.
TFTP - 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.
TFTP - Error: Illegal Operation	An unknown operation was detected by ATLAS when transferring the update file from the TFTP network server.
TFTP - Error: User aborted	Indicates the user selected Cancel Update to abort reception of the update file from the TFTP network server.

18. When the update process has completed successfully, the menu screen will display **Idle** in the *Current Update Status* field and **Module Update Complete** in the *Previous Update Status* field. In the event an error occurred during the update process, the *Previous Update Status* field will display the appropriate error message. Please go to step 7 and attempt the update process again. If the same error occurs, please contact ADTRAN Technical Support.
19. If the update of the module was successful, the module will either restart immediately and resume operation or restart at the specified time and day of the week, depending on your selection.
20. To update additional modules, go to Step 6 and select the appropriate slot.

UNDERSTANDING SNMP

As local area network (LAN) environments became standardized over the past ten years, multi-vendor equipment grew with competition. It became necessary to manage the various vendor equipment from a single control console. Thus, 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 MIB (Management Information Base).

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 within a network device. It defines the operating parameters that can be controlled or monitored. When requesting the network manager to retrieve or modify a particular piece of information about a network device, the network manager transmits the request to that 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 the data from the various network devices and presents it in a consistent form.

TRAPS

An SNMP trap is a message sent by a Network Device, such as the ATLAS, to report an operational anomaly or alarm condition.

DEFINING A TRAP DESTINATION LIST

For each trap event, a trap message will be sent to each member of the Trap Destination List. You can configure this list via Telnet session or VT100 menu. The ATLAS will support up to four trap destinations. By default, the destination list is empty.

To configure the trap destination list, select SNMP/TRAP DESTINATION from the terminal menu (see Table 9-1). Options similar to the following will be displayed.

Table 9-1. 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 the ATLAS will send 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 events.

FILTERING TRAPS

You may disable the generation of trap events in three different ways. First, from the user menu, you can select SNMP/TRAP TRANSMISSION to DISABLED. If DISABLED, the ATLAS will not generate any trap messages. Second, trap thresholds can be defined to disable specific trap events. Each trap event has a severity level (DISABLED, INFORMATIONAL, NORMAL, WARNING, MINOR, MAJOR, CRITICAL) associated with it. Consider the example of 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 be generated to that destination because the coldStart severity level is defined as NORMAL. Refer to the ATLAS MIB in Appendix X for a description of each enterprise trap event supported by the ATLAS. Finally, certain traps can be controlled through SNMP management of specific MIB variables supported by the ATLAS. These variables will be outlined in the following sections.

STANDARD TRAPS

Table 9-2 describes the standard traps supported by ATLAS.

Table 9-2. Standard Trap

Index	Trap Names	Severity	Description
0	coldStart	NORMAL	the ATLAS is such that its configuration may be altered; this trap will be generated on power up
1	warmStart	NORMAL	the 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	the ATLAS has received a protocol message that has failed authentication

In RFC1213, or MIB II, the object type `snmpEnabledAuthenTraps` is defined. 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

The ATLAS will support RFC1406, the DS1 standard MIB, as well as the ADTRAN DS1 MIB, an extension to RFC1406. The ADTRAN DS1 groups provide the capability to send traps for DS1 Alarm failures and Performance Threshold Crossing Alerts. The DS1 Alarm Table, defined in the ADTRAN DS1 extension MIB, contains entries for enabling 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 9-3 describes the DS1 Alarm Traps supported by the ATLAS.

Table 9-3. 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, the ATLAS will send 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 the ATLAS will send an Alarm Trap message. A single Alarm Trap message may report multiple event changes. The ATLAS 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 the ATLAS to send an Alert Trap message to each member of the Trap Destination List when accumulated error statistics exceed these threshold values. Table 9-4 describes the Alert Traps supported by the ATLAS for events that have occurred in the last 15-minute interval.

Table 9-4. DS1 Current Alert SNMP Trap

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 unavailable
adATLAS800CurrentCSS	WARNING	the current interval path code violation has 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, the ATLAS will send 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 the ATLAS will send an Alert Trap message. A single Alert Trap message may report multiple event changes. The ATLAS clears the event bits after sending the Trap message or sending the response to a Get request for the adDS1CurrentAlert variable. The ATLAS 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 9-5 describes the Total Alert Traps, which describe events that have occurred in the last 24-hour interval.

Table 9-5. 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 violation 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, the ATLAS will send 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 the ATLAS will send an Alarm Trap message. A single Alert Trap message may report multiple event changes. The ATLAS clears the event bits after sending the Trap message or sending the response to a Get request for the adDS1TotalAlert variable.

The Current and Total Alerts described above are Near End events. The ATLAS will also support Current and Total Alerts 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.

UTILITIES DELIVERED WITH THE ATLAS 800^{PLUS}

ADTRAN delivers several software utilities on three diskettes with the ATLAS 800^{PLUS} to make it easier for you to interface with the terminal menus and to transfer configuration files to and from TFTP servers. The diskettes also include the ATLAS 800^{PLUS} MIB for use with SNMP (located in the MIB directory). The utilities all run on Microsoft Windows 3.1 or higher. The following sections describe the Telnet, VT-100, and TFTP Server utilities.

Telnet

The Telnet utility delivered with ATLAS 800^{PLUS} provides enhancements from standard Telnet programs that make it easier to work with ATLAS 800^{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 5-2, and for a detailed description of the Telnet interface, see Figure 5-1 on page 5-4.

If you need help setting up the ATLAS 800^{PLUS} for a Telnet session, refer to “Telnet” on page 3-6.

Menu Options

The Telnet utility provides several extra options. This section describes some of the features that you may find useful.

Session Menu**Connect**

This option establishes a Telnet session. Either select an existing **Host Name** from the list, or click the **Add New** button to add a new host name. Click **Connect** to establish the session (see Figure 10-1).

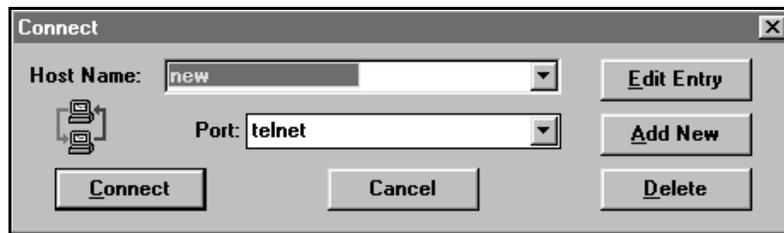


Figure 10-1. Add New Dialog Box

Port

You can choose several options from the Port pulldown menu:

- Telnet: establishes a Telnet session
- Echo: provides a loopback for troubleshooting
- Discard: bit bucket; discards data
- Daytime: returns the time
- Chargen: displays a unique character stream. Used for self-tests.

Edit Entry

The **Edit Entry** button allows you to change either the name or the IP address of each host (see Figure 10-2).

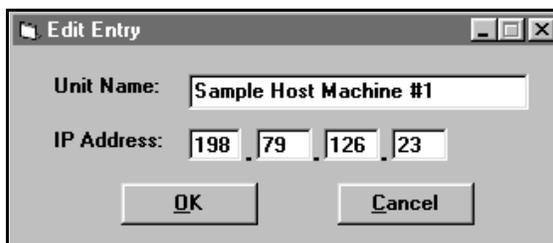


Figure 10-2. Edit Entry Dialog Box

You can press either **Tab**, **Return**, or a period (.) after each number in the IP address to move to the next field. These options also clear the existing data from the field.

Add New

The **Add New** button adds a new host name to the list. Type a new host name and IP address in the dialog box. The dialog box is the same as the **Edit Entry** dialog box (see Figure 10-2).

Delete

The **Delete** button deletes a host name from the list. Select the host name you want to delete and click this button.

Disconnect

Terminates the Telnet session. To re-establish the session, select **Connect** from the **Session** menu.

Exit

Ends the Telnet session and dismisses the Telnet screen.

Edit Menu

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

Options Menu**Colors**

Allows you to change the color of the background window, bold highlights, and 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

The **Capture** option 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.

About Menu**IP Status**

The **IP Status** option displays the local port address and the status of the connection.

VT-100

The VT-100 allows you to configure an ATLAS 800^{PLUS} when the PC is directly connected to an ATLAS 800^{PLUS}. 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 5-2 and for a detailed description of the VT-100 interface, see “VT-100 Operation” on page 3-7.

If you need help setting up the ATLAS 800^{PLUS} for a VT-100 session, refer to “VT-100 Operation” on page 3-7.

Menu Options**Session and Edit Menus**

The **Session** and **Edit** menu commands are identical to the Telnet options. See “Session Menu” on page 10-1 and “Edit Menu” on page 10-3 for details.

Port Menu

This option allows you to change various serial COM port settings (see Figure 10-3).

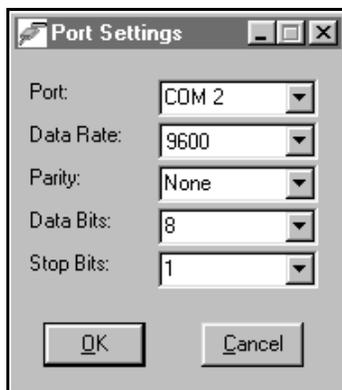


Figure 10-3. Port Settings Dialog Box

Options Menu

Connect

Provides the options **Transmit Wakeup** and **Transmit Refresh**.

Refresh Screen

Redraws the screen.

Colors

These commands change the color of the background screen and text.

Local Echo and Auto Repeat

These options are the same as in the Telnet interface (see page 10-3 for details).

Capture Menu

The **Capture** option copies the text on the current VT-100 screen to the clipboard. You can open any word processor and paste the clipboard contents into the program. This option is helpful when debugging.

TFTP Server

The TFTP Server utility transfers ATLAS 800^{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 800 can be saved offline as a backup file. The saved file may also be used to send the same configuration to multiple ATLAS 800 units. Configuration file transfers are accomplished using the TFTP protocol (a TCP/IP user protocol) through the 10BaseT Ethernet port. The ATLAS 800 must have a valid IP address, subnet mask, and default gateway (if required), and must be connected to an Ethernet network before proceeding. Figure 10-4 shows the TFTP Server interface.

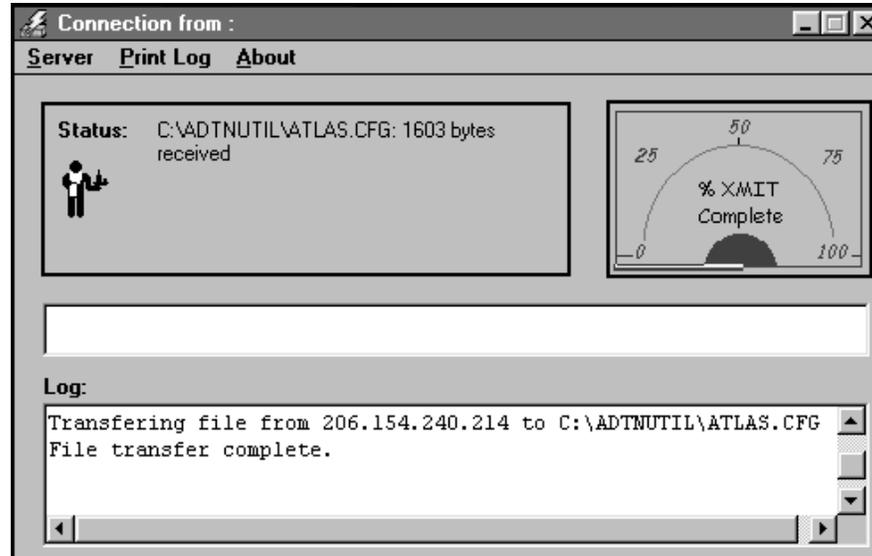


Figure 10-4. TFTP Server Interface

Only one configuration transfer session (upload or download) may be active at a time. The TCP/IP parameters are not saved or overwritten as part of an ATLAS 800 unit's transferred configuration to allow sending identical configurations to multiple units.

When you start this program, a port is automatically opened.

Menu Options

Server Menu

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

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.

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.

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

1. Make sure the TFTP server is running on a remote machine. If you are using the ADTRAN TFTP Server program, just start the program and the server is automatically enabled.
2. Log in using Telnet to the ATLAS 800 for which you want to save the configuration file.

**NOTE**

A Level 3 or better password is required for performing a configuration download, the same level required to modify most configuration parameters. Please consult the ATLAS administrator if level 3 access is not available.

3. Select the **System Utility** menu, then the **Config Transfer** menu.
4. Set **TFTP Server IP Address** to the IP address of the machine running the TFTP server program.

**NOTE**

If you are using the ADTRAN TFTP server, the IP address displays in the Status field.

5. Change **TFTP Server Filename** to a unique filename. This will be the name of the configuration file to save to the remote server.

**NOTE**

You must enter the entire directory path to the file name.

Some TFTP servers constrain the format of the filename depending on the operating system of the server. For example, a TFTP server running on a PC under Windows 3.1 may only permit 8.3 format filenames (8 characters, period, and three extension characters).

6. Move to the **Save Config Remotely** activator button and press Enter to proceed with the transfer. Respond with Y to the confirmation request.
7. The **Current Transfer Status** field indicates the progress of the transfer.
8. Once complete, the **Previous Transfer Status** field indicates success or failure of the transfer. If successful, it will indicate **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.*

There are various reasons why a configuration download may fail, and a specific error message is displayed in this case. 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 file (although configuration files are not normally large). 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.

To retrieve the configuration from a TFTP server

1. Make sure a TFTP server is running on a remote machine. If you are running the ADTRAN TFTP Server program, just start the program and the server is automatically enabled.
2. Log in using Telnet to the ATLAS 800 to which you want to upload a configuration file.

NOTE *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.*

3. Select the **System Utility** menu, then the **Config Transfer** menu.
4. Set **TFTP Server IP Address** to the IP address of the machine running the TFTP server program.

NOTE *If you are using the ADTRAN TFTP server, the IP address displays in the Status field.*

5. Change **TFTP Server Filename** to the filename of a previously saved configuration you wish to load. Enter the complete directory path to the file.
6. Move to the **Load And Use Config** activator button and press Enter to proceed with the transfer. Respond with Y to the confirmation request.

WARNING *The ATLAS 800 is rebooted immediately after a configuration is successfully loaded. No additional confirmation is requested, and any online sessions will be terminated.*

7. The **Current Transfer Status** field indicates the progress of the transfer.

8. If the upload completes successfully, the unit reboots automatically and runs using the new configuration. If the upload fails, an error message is present in the **Previous Transfer Status** field. If the TFTP server cannot be contacted, the attempt takes approximately 20 seconds to timeout.

This section 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.



CAUTION *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 shown in Tables A-1 through A-11 are of use primarily during troubleshooting and should be turned off in normal operation.

Table	Title	Page #
A-1	Source: System	2
A-2	Source: Switchboard	3
A-3	Source: Nx 56/64	3
A-4	Source Time	4
A-5	Source: Ethernet	6
A-6	Source: ISDN	6
A-7	ISDN Cause Codes	9
A-8	Cause Code Log Entries	11
A-9	Source: ISDN L2 Messages	11
A-10	Source: ISDN Call Control Messages	11
A-11	Source: ISDN Information Elements	12

Table A-1. Source: System

Event	Category	Console Log String	Front Panel Display
System Cold Start – generated 5 seconds after the completion of system initialization.	Normal	Cold Start	COLD START
SNMP Authentication Failure – 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.	Info	SNMP Authentication Failure	AUTHEN FAIL
Module removed or not responding	Warning	Module Not Responding	MODULE OUT -A
Module found	Information	Module Found	MODULE FOUND
Console login failure – three consecutive login attempts were attempted and failed	Minor	Login Failure	LOGIN FAILURE
An ATLAS 800 configuration file was loaded into the system and was activated	Critical	System Configuration Uploaded	CONFIG UPLOADED
The internal system temperature is too high	Critical	Internal Temperature Warning	TEMP WARN -A
The internal system temperature has returned to normal	ICritical	Internal Temperature Warning Cleared	TEMP WARN -I
The primary power supply is present but is not operating properly	Critical	Main Power Supply Failure	PS1 WARNING -A
The primary power supply is operating properly or has been removed	Critical	Main Power Supply Failure Cleared	PS1 WARNING -I
The backup power supply is present but is not operating properly	Critical	Backup Power Supply Failure	PS2 WARNING -A
The backup power supply is operating properly or has been removed	Critical	Backup Power Supply Failure Cleared	PS2 WARNING -I

Table A-2. Source: Switchboard

Event	Category	Console Log String	Front Panel Display
Call rejected – no such number in dial plan	Warning	<number> rejected: No such number	n/a
Call rejected – number is on outgoing reject list	Normal	<number> rejected: Outgoing reject list	n/a
Call successfully routed	Normal	<number> accepted: <slot> <port>	n/a
Call rejected – all end points busy	Normal	<number> rejected: Busy	n/a

Table A-3. Source: Nx 56/64

Event	Category	Console Log String	Front Panel Display String
Clock Slip Alarm Active	Major	Nx 56/64 Clock Slip Alarm Active	Nx CLK SLIP -A
Clock Slip Alarm Cleared	Major	Nx 56/64 Clock Slip Alarm Cleared	Nx CLK SLIP -I
PLL Alarm Active	Major	Nx 56/64 PLL Alarm Active	Nx PLL ALM -A
PLL Alarm Cleared	Major	Nx 56/64 PLL Alarm Cleared	Nx PLL ALM -I
External Clock Alarm	Major	Nx 56/64 External Clock Alarm Active	Nx EXT CLK ALM-A
External Clock Alarm Cleared	Major	Nx 56/64 External Clock Alarm Cleared	Nx EXT CLK ALM-I
Excessive Zeros from DTE	Warning	Nx 56/64 Excessive Zeros Alarm	Nx XS0 ALM-A
Excessive Zeros condition cleared	Warning	Nx 56/64 Excessive Zeros Alarm Cleared	Nx XS0 ALM-I
Bilateral Loopback Activated	Warning	Nx 56/64 Bilateral Loopback Active	Nx BI-LAT LBK -A
Bilateral Loopback Deactivated	Warning	Nx 56/64 Bilateral Loopback Cleared	Nx BI-LAT LBK -I
511 Test Pattern Activated	Warning	Nx 56/64 511 Test Pattern Active	Nx TEST PTRN -A

Table A-3. Source: Nx 56/64 (Continued)

Event	Category	Console Log String	Front Panel Display String
511 Test Pattern Deactivated	Warning	Nx 56/64 511 Test Pattern Cleared	Nx TEST PTRN -I
DTR Asserted	Information	Nx 56/64 DTR Asserted	n/a
DTR Dropped	Information	Nx 56/64 DTR Dropped	n/a
RTS Asserted	Information	Nx 56/64 RTS Asserted	n/a
RTS Dropped	Information	Nx 56/64 RTS Dropped	n/a
DCD Asserted	Information	Nx 56/64 DCD Asserted	n/a
DCD Dropped	Information	Nx 56/64 DCD Dropped	n/a
CTS Asserted	Information	Nx 56/64 CTS Asserted	n/a
CTS Dropped	Information	Nx 56/64 CTS Dropped	n/a

Table A-4. Source Time

Event	Category	Console Log String	Front Panel Display String
Red Alarm Set	Major	T1 Red Alarm Active	T1 RED ALRM -A
Red Alarm Cleared	Major	T1 Red Alarm Cleared	T1 RED ALRM -I
Yellow Alarm Set	Major	T1 Yellow Alarm Active	T1 YELW ALRM -A
Yellow Alarm Cleared	Major	T1 Yellow Alarm Cleared	T1 YELW ALRM -I
Blue Alarm Set	Major	T1 Blue Alarm Active	T1 BLUE ALRM -A
Blue Alarm Cleared	Major	T1 Blue Alarm Cleared	T1 BLUE ALRM -I
LOS Alarm Set	Major	T1 LOS Active	T1 LOS -A
LOS Alarm Cleared	Major	T1 LOS Cleared	T1 LOS -I
Tx Blue Alarm Set	Major	T1 Tx Blue Alarm Active	T1 TX BLUE -A
Tx Blue Alarm Cleared	Major	T1 Tx Blue Alarm Cleared	T1 TX BLUE -I

Table A-4. Source Time (Continued)

Event	Category	Console Log String	Front Panel Display String
Tx Yellow Alarm Set	Major	T1 Tx Yellow Alarm Active	T1 TX YELW -A
Tx Yellow Alarm Cleared	Major	T1 Tx Yellow Alarm Cleared	T1 TX YELW -I
D Channel Alarm Set	Major	T1 D Channel Alarm Active	T1 D CH ALRM -A
D Channel Alarm Cleared	Major	T1 D Channel Alarm Cleared	T1 D CH ALRM -I
Line Loopback Active	Warning	T1 Line Loopback Active	T1 LINE LB -A
Payload Loopback Active	Warning	T1 Payload Loopback Active	T1 PYLD LB -A
Loopback Cleared	Warning	T1 Loopback Cleared	T1 LBK -I
Current T1 Errored Seconds Threshold Exceeded	Warning	T1 Curr ES Thrs Exceeded	T1 CUR ES THRS
Current T1 Severely Errored Seconds Threshold Exceeded	Warning	T1 Curr SES Thrs Exceeded	T1 CUR SES THRS
Current T1 Severely Errored Framing Seconds Threshold Exceeded	Warning	T1 Curr SEFS Thrs Exceeded	T1 CUR SEFS THRS
Current T1 Unavailable Seconds Threshold Exceeded	Warning	T1 Curr UAS Thrs Exceeded	T1 CUR UAS THRS
Current T1 Controlled Slip Seconds Threshold Exceeded	Warning	T1 Curr CSS Thrs Exceeded	T1 CUR CSS THRS
Current T1 Path Code Violations Threshold Exceeded	Warning	T1 Curr PCV Thrs Exceeded	T1 CUR PCV THRS
Current T1 Line Errored Seconds Threshold Exceeded	Warning	T1 Curr LES Thrs Exceeded	T1 CUR LES THRS
Current T1 Line Code Violations Threshold Exceeded	Warning	T1 Curr LCV Thrs Exceeded	T1 CUR LCV THRS
Total T1 Errored Seconds Threshold Exceeded	Warning	T1 Tot ES Thrs Exceeded	T1 TOT ES THRS
Total T1 Severely Errored Seconds Threshold Exceeded	Warning	T1 Total SES Thrs Exceeded	T1 TOT SES THRS

Table A-4. Source Time (Continued)

Event	Category	Console Log String	Front Panel Display String
Total T1 Severely Errored Framing Seconds Threshold Exceeded	Warning	T1 Total SEFS Thrs Exceeded	T1 TOT SEFS THRS
Total T1 Unavailable Seconds Threshold Exceeded	Warning	T1 Total UAS Thrs Exceeded	T1 TOT UAS THRS
Total T1 Controlled Slip Seconds Threshold Exceeded	Warning	T1 Total CSS Thrs Exceeded	T1 TOT CSS THRS
Total T1 Path Code Violations Threshold Exceeded	Warning	T1 Total PCV Thrs Exceeded	T1 TOT PCV THRS
Total T1 Line Errored Seconds Threshold Exceeded	Warning	T1 Total LES Thrs Exceeded	T1 TOT LES THRS
Total T1 Line Code Violations Threshold Exceeded	Warning	T1 Total LCV Thrs Exceeded	T1 TOT LCV THRS

Table A-5. Source: Ethernet

Event	Category	Console Log String	Front Panel Display String
Not enough memory for ethernet driver	Critical	No memory for driver structure	n/a

Table A-6. Source: ISDN

Event	Category	Console Log String	Front Panel Display String
No BRI resources available	Critical	BRI configuration failed: No ISDN resources are available	NO MORE ISDN AVL
No PRI resources available	Critical	PRI configuration failed: No ISDN resources are available	NO MORE ISDN AVL
Unknown SPID received	Major	BRI LT: SPID <spid> received - NOT IN LIST	SPID FAILED
SPID Negotiation failed	Major	BRI NT: SPID Negotiations failed - resetting the link	SPIDS FAILED

Table A-6. Source: ISDN (Continued)

Event	Category	Console Log String	Front Panel Display String
SPID Failed	Major	BRI NT: Spid <spid> was rejected	SPID FAILED
D Channel Down	Major	D channel is DOWN	D CHAN DOWN
Incorrectly formatted IE	Major	<message>: Incorrectly formatted cause IE	n/a
SPID Retry in progress	Minor	BRI NT: SPID Negotiations failed - Retrying	SPID RETRY
SPID Unregistration attempted	Warning	LT: Tried to call unregistered SPID <spid>	n/a
No Matching SPID found	Warning	No SPID matches the call profile: <called number> <call type>	n/a
No Matching SPID found	Warning	No SPID with free B channels matches call type: <call type>	n/a
ISDN line released	Normal	Released: No longer an ISDN line	RELEASED
BRI LT configuration successful	Normal	Configured BRI as LT	CONFIG BRI LT
BRI NT configuration successful	Normal	Configured BRI as NT	CONFIG BRI NT
PRI CO configuration successful	Normal	Configured PRI as central office emulator	CONFIG PRI CO
PRI CPE configuration successful	Normal	Configured PRI as CPE	CONFIG PRI CPE
No B channels for call	Normal	No outgoing B channel available for call to <number>	n/a
SPID Registration in progress	Normal	BRI LT: Registering SPID <spid>	REGISTER SPID
SPID Registration complete	Normal	BRI LT: All SPIDs registered	SPIDS COMPLETE
SPID registered	Normal	BRI NT: Spid <spid> registered	SPID REGISTERED

Table A-6. Source: ISDN (Continued)

Event	Category	Console Log String	Front Panel Display String
SPID Registration complete	Normal	BRI NT: All SPIDs registered	SPIDS COMPLETE
SPID Registration in progress	Normal	BRI NT Registering SPID <spid>	REGISTER SPID
Call Rejected	Normal	Rejected an incoming call for an unregistered SPID	n/a
D Channel Up	Normal	D channel is UP	D CHAN UP
Dialing number	Information	Dialing <called number>	n/a
Call not accepted	Information	Call not accepted to <called number>: No channel available	n/a
Call cleared	Information	Call to <called number> cleared from ATLAS end	n/a
Call busy	Information	Call to <called number> declared busy after leaving ATLAS	n/a
Call connected	Information	Call to <called number> connected	n/a
Call ringing	Information	Call to <called number> ringing	n/a
Call busy	Information	Call to <called number> refused: Busy	n/a
Call disconnected	Information	Call to <called number> disconnected by far end	n/a
Call received	Information	Call to ATLAS: <called number> received	n/a
Incoming call refused	Information	Incoming call to <called number> refused	n/a
Incoming call accepted	Information	Incoming call to <called number> accepted	n/a

In addition to the tables above, certain recognized ISDN cause codes are sent to the event log from the ISDN Message facility. The codes applicable to the ATLAS 800^{PLUS} are shown in Table A-7, along with the minimum category required for logging the cause code event.

Table A-7. ISDN Cause Codes

Cause Code Message	Code	Category
UNASSIGNED_NUMBER	1	Information
NO_ROUTE	2	Information
CHANNEL_UNACCEPTABLE	6	Information
NORMAL_CLEARING	16	Information
USER_BUSY	17	Information
NO_USER_RESPONDING	18	Information
CALL_REJECTED	21	Information
NUMBER_CHANGED	22	Information
DEST_OUT_OF_ORDER	27	Information
INVALID_NUMBER_FORMAT	28	Information
FACILITY_REJECTED	29	Information
RESP_TO_STAT_ENQ	30	Information
UNSPECIFIED_CAUSE	31	Information
NO_CIRCUIT_AVAILABLE	34	Warning
NETWORK_OUT_OF_ORDER	38	Warning
TEMPORARY_FAILURE	41	Warning
NETWORK_CONGESTION	42	Warning
ACCESS_INFO_DISCARDED	43	Warning
REQ_CHANNEL_NOT_AVAIL	44	Warning
PRE_EMPTED	45	Warning
FACILITY_NOT_SUBSCRIBED	50	Minor
OUTGOING_CALL_BARRED	52	Minor
INCOMING_CALL_BARRED	54	Minor
BEAR_CAP_NOT_AVAIL	58	Minor
SERVICE_NOT_AVAIL	63	Minor
CAP_NOT_IMPLEMENTED	65	Major

Table A-7. ISDN Cause Codes (Continued)

Cause Code Message	Code	Category
CHAN_NOT_IMPLEMENTED	66	Major
FACILITY_NOT_IMPLEMENTED	69	Major
INVALID_CALL_REF	81	Major
CHAN_DOES_NOT_EXIST	82	Major
INCOMPATIBLE_DEST	88	Major
INVALID_MSG_UNSPEC	95	Major
MANDATORY_IE_MISSING	96	Major
NONEXISTENT_MSG	97	Major
WRONG_MESSAGE	98	Major
BAD_INFO_ELEM	99	Major
INVALID_ELEM_CONTENTS	100	Major
WRONG_MSG_FOR_STATE	101	Major
TIMER_EXPIRY	102	Major
MANDATORY_IE_LEN_ERR	103	Major
PROTOCOL_ERROR	111	Major
INTERWORKING_UNSPEC	127	Major

Cause Code IEs that are non-Q.931 (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:

- Reserved
- National
- Local

Each Cause Code IE log entry will end with a location designation. These designations are shown in Table A-8:

Table A-8. Cause Code Log Entries

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

Table A-9. Source: ISDN L2 Messages

Event	Category	Console Log String	Front Panel Display String
ISDN Layer 2 (LAPD) Message. Provides a hex dump of the entire LAPD frame	Information	<message contents>	n/a

Table A-10. Source: ISDN Call Control Messages

Event	Category	Console Log String	Front Panel Display String
ISDN Call Control Messages	Information	Host>>CC <tag> <call ID> <message>	n/a
ISDN Call Control Messages	Information	CC>>Host <tag> <call ID> <message>	n/a

Table A-11. Source: ISDN Information Elements

Event	Category	Console Log String	Front Panel Display String
ISDN Information Elements. Provides a hex dump of the ISDN IE sent with a call control message	Information	<message contents>	n/a

Table B-1. Troubleshooting

SYMPTOM	POSSIBLE CAUSES	TROUBLESHOOTING TIPS
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	<ul style="list-style-type: none"> • 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 pass data from T1 interface to V.35 port	Misconfiguration, improper cabling	<ul style="list-style-type: none"> • 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.

Table B-1. Troubleshooting (Continued)

SYMPTOM	POSSIBLE CAUSES	TROUBLESHOOTING TIPS
Switched calls are not working	Misconfiguration	<ul style="list-style-type: none"> • 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 with VT 100 connected to the Control/Chain In Port	Misconfiguration, improper cabling	<ul style="list-style-type: none"> • 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.
Cannot establish Telnet session with ATLAS	Max Telnet sessions set to 0, IP address of ATLAS does not match remote host IP address	<ul style="list-style-type: none"> • Verify that the ethernet connection is in place, check IP addresses programmed in ATLAS and in the Telnet client, verify that session time-out 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.

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:

RMA 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 # _____

Index

Symbols

5-30

Numerics

10-BaseT

- connection 2-6
- pinout 2-6
- port 2-2
- status 5-10

15 minutes

- performance 5-27

24 hour

- performance 5-27

A

abort 10-5

accept numbers 5-35, 5-38

access

- passwords 5-16

access rights 5-17

activate

- dedicated map 5-29
- front panel 3-2
- menu item 4-2
- time 5-32

active alarm 4-9

add

- new (Telnet utility) 10-2

add password 5-17

address

- ADLP 5-12

ADLP address 5-12

ADTRAN

- utilities 10-1

ADTRAN data link layer protocol address 5-12

alarm

- blue 5-25
- red 5-25
- status 5-25
- system 5-10
- yellow 5-25, 5-27
- yellow auto TX 5-27

alarm key 3-2, 3-3

alarm LED 3-4

alarm log

- view 4-9

alarm menu 4-9

alarms

- active 4-9
- module 5-24
- view log 5-9

all

- ones 5-28
- zeros 5-28

alarm menu 4-9

AMI 2-5

analog

- accept 5-35, 5-38
- reject 5-36

applications engineering C-1

area code 5-40

arrow keys

- down 3-2
- up 3-2

arrows 3-1, 3-2

assign dedicated connections 5-2

AT&T 4ESS 5-41

ATLAS 800 PLUS

- before installing 2-1
- configuring 5-1
- general system information 5-1
- grounding instructions 2-2
- installing 2-1
- operating 3-1, 3-5
- shipping contents 2-1
- system status 5-1
- terminal menu structure 5-1

audio

- reject 5-39

authenticate trap transmission 5-15

auto daylight savings 5-16

auto repeat 10-3, 10-4

auto TX yellow alarm 5-27

automatic

- routeback rejection 5-40

available DS0s 5-44, 5-48

B

B8ZS 2-5

backup timing source 5-12

bantam test jack 2-2

baud rt 4-5

begin firmware update 5-20

BES 5-26

blinking green module status LED 3-4

blinking green system LED 3-3

blinking red module status LED 3-4

blinking red system LED 3-3

blue alarm 5-25

boot ROM rev 5-8

bootROM 5-22

bursty errored seconds 5-26

C

- called digits transferred 5-42, 5-47
- caller ID number 5-49
- cancel 3-1, 3-2
 - menu 4-2
- cancel key 3-2
- capture 10-3, 10-4
- category 5-9
 - logging A-1
- chain in 2-3
 - pinout 2-4
- chain out 2-2, 2-4
 - pinout 2-5
- chain port
 - configure 5-13
 - framing errs 5-12
 - overrun errs 5-12
 - Rx bytes 5-11
 - signal leads 5-11
 - status menu 4-4
 - Tx bytes 5-11
- chain port configuration 4-5
- chain-in port 2-2
- chain-out port 2-2
- challenge # 4-8
- clear
 - performance data 5-26
 - selftest log 5-22
 - system event log 5-9
 - system LED 5-10
 - test pattern 5-28
- clear history 4-9
- clear key 3-2, 3-3
- clear log 10-6
- clock 5-16
- CLR 5-26
- code 5-27
- colors 10-3, 10-4
- community
 - trap destination 5-15
- completed network map 7-6
- completed user map 7-7
- config 4-5
- config menu
 - ethernet configuration 4-5
 - S0 system 4-5
 - S1-S8 4-6
- config transfer 5-20
- configuration
 - from port 5-30
 - get from TFTP server 10-7
 - interface 5-36, 5-39, 5-41
 - Octal BRI 5-50
 - load 5-21
 - module 5-27
 - Nx 56/64 5-49
 - Quad T1/PRI interface 5-41
 - save to server 5-21
 - save to TFTP server 10-6
 - use 5-21
- configuration file
 - get from server 5-20
 - send to server 5-20
- configuration menu 4-5

- configure 5-13
 - chain port 5-13
 - configure
 - port type 5-14
 - default gateway 5-13
 - ethernet port 5-13
 - ethernet port name 5-13
 - event logging 5-16
 - flow control 5-14
 - IP address 5-13
 - module slots 5-23
 - port name 5-13
 - subnet mask 5-13
- configuring ATLAS 800 PLUS 5-1
- configuring Syslog 5-16
- connect
 - Telnet menu 10-1
- connection
 - activate 5-29
 - control in / chain in 2-3
 - create/edit 5-29
 - current 5-29
 - dedicated 5-28
 - ethernet 10BaseT 2-6
 - from 5-30
 - LAN 2-6
 - name 5-29
 - network 2-5
 - power 2-1
- connections 2-2
- connects 5-29
- contents of shipment 2-1
- control in 2-3
 - pinout 2-4
- control out 2-4
- controlled slip seconds 5-26
- controller
 - revision 5-8
- controller board slots 5-23
- controller info 5-25
- control-Z 5-5
- create
 - dedicate map 5-29
- creating
 - dedicated map 6-1
 - dial plan 7-1
- CSS 5-26
- CSU status LED 3-2
- CTS
 - chain port status 4-4
 - clear to send 5-11
- current
 - dedicate map 5-29
 - performance 5-26
- current date/time 5-16
- current time/data 5-8
- current transfer status 5-21
- current update status 5-19
- customer service C-1

D

- D channel sync 5-26
- D4 2-5
- DACS

- description 1-4
 - data
 - 56 kbps
 - accept 5-38
 - 56 kpbs
 - reject 5-39
 - 64 kbps
 - accept 5-35, 5-38
 - reject 5-36, 5-39
 - data field 4-2
 - set 4-2
 - data tables 5-11
 - configuring 5-11
 - date 4-6
 - current 5-16
 - restart schedule 5-19
 - restart system 5-19
 - set 5-8
 - daylight savings 5-16
 - DCD
 - chain port status 4-4
 - data carrier detect 5-11
 - D-chan 5-26
 - dedicate map
 - create/edit 5-29
 - DS0 available 5-30
 - Dedicated 1-3
 - dedicated and switched connection maps
 - description 1-3
 - dedicated map 5-28
 - activate 5-29
 - activate time 5-32
 - connections 6-1
 - creating 6-1
 - current 5-29
 - design 6-1
 - DS0 selection 5-30
 - enter connections 5-29
 - from connection 5-30
 - implement 6-3
 - insert connection 5-30
 - map name 5-29
 - module configuration 6-2
 - number of connections 5-30
 - overview example 6-1
 - dedicated maps menu 5-28
 - def gateway 4-5
 - default
 - password 5-17
 - default gateway
 - configure 5-13
 - define
 - passwords 5-16
 - define IP address 3-6
 - defining trunk conditioning 5-32
 - delete
 - alarm history 4-9
 - event log 5-9
 - password 5-17
 - selftest log 5-22
 - description of event 5-9
 - dial plan 5-33
 - complete 7-6
 - creating 7-1
 - example 7-1
 - implementing 7-5
 - network terminations 5-33
 - plan 7-3
 - provision network 7-3
 - remote access setup 7-2
 - sample network terminations 7-4
 - sample user termination 7-5
 - signaling 5-34
 - slot/port 5-34
 - understanding 7-2
 - video conferencing setup 7-2
 - dial plan menus 5-33
 - DID 5-44, 5-49
 - digits transferred 5-44, 5-49
 - prefix 5-45
 - digital access cross-connect system (DACs) 1-4
 - direct inward dialing 5-44, 5-49
 - disable 10-5
 - disconnect 10-2
 - display
 - event log 5-16
 - down arrow key 3-2
 - download
 - configuration file 5-20
 - firmware 5-18
 - DRAM 4-8, 5-22
 - installed 5-8
 - DS0
 - available 5-30, 5-44, 5-48
 - first 5-43, 5-48
 - number of 5-43, 5-48
 - selection 5-30
 - status 5-26
 - usage 5-26
 - DS0 signaling 5-26
 - DS0 status
 - * 5-26
 - A 5-26
 - D 5-26
 - M 5-26
 - N 5-26
 - O 5-26
 - R 5-26
 - DS0s, number of 5-41
 - DSP RAM 4-8, 5-22
 - DTE cable 2-1
 - DTR
 - chain port signal leads 5-11
 - chain port status 4-4
- ## E
- E&M
 - immediate 5-44, 5-48
 - wink 5-44, 5-48
 - edit
 - dedicated map 5-29
 - entry (Telnets utility) 10-2
 - empty module slot 5-25
 - enable
 - TFTP 10-5
 - enable day 5-33
 - enbl day 5-33
 - end of number timeout 5-39

- end point
 - configuration 5-41
- enter
 - dedicated map connections 5-29
- enter key 3-1, 3-2
- entry
 - edit (Telnet utility) 10-2
- erase
 - alarm history 4-9
 - event log 5-9
 - selftest log 5-22
 - test results 4-8
- error LED 3-4
- errored seconds 5-26
- errors
 - inject 5-28
- ES 5-26
- ESF 2-5
- ethernet
 - 10BaseT connection 2-6
 - configuration
 - config menu 4-5
 - connection 2-6
 - pinout 2-6
 - port 5-10, 5-13
 - configure 5-13
 - status
 - status menu 4-4
- ethernet configuration
 - config menu 4-5
- event
 - description 5-9
 - log A-1
 - logging 5-16
 - severity 5-9
 - slot of event 5-9
 - types 5-16
- event log 5-9
 - clear 5-9
 - view 4-9
- event logging 4-9
 - configure 5-16
- exit
 - menu 4-2
- F**
- failure messages 10-1
- fault
 - signaling 5-32
 - state 5-32
- filename
 - TFTP server 5-19, 5-21
- firmware
 - begin update 5-20
 - revision 5-8
 - update 5-18
 - begin 5-20
 - module slot 5-18
 - restart schedule 5-19
 - TFTP 5-19, 8-1, 8-4
 - XMODEM 5-19, 8-1
 - updating 8-1
- first DS0 5-41, 5-43, 5-46
- flash 5-22
- flash memory installed 5-8
- flashing red CSU LED 3-4
- flow control 4-5
 - configure 5-14
- forget password 4-8
- frame 5-27
- frame relay
 - description 1-2
- framing errors 5-12
- from
 - configuration 5-30
- from slot 5-30
- front panel
 - access active alarm display menus 3-3
 - activating 3-2
 - alarm 3-2
 - cancel key 3-2
 - clear data 3-3
 - clear key 3-2
 - CSU LED light
 - flashing red 3-4
 - green 3-4
 - red 3-4
 - yellow 3-4
 - CSU status LEDs 3-2
 - enter key 3-2
 - home key 3-2
 - layout 3-1, 3-2
 - LCD 3-2
 - LED description 3-3
 - main menu 4-3
 - module slot numbers 3-2
 - module status 3-2
 - module status LED 3-4
 - module status LED light
 - blinking green 3-4
 - blinking red 3-4
 - green 3-4
 - red 3-4
 - module status LEDs 3-2
 - navigating 4-2
 - navigation example 3-5
 - online 3-4
 - operation 4-1
 - operation keys 3-3
 - return to main menu 3-3
 - shift key 3-2
 - structure 4-1
 - system LED 3-2
 - system LED light
 - green (fast blink) 3-3
 - green (solid) 3-3
 - red (fast blink) 3-3
 - red (solid) 3-3
 - yellow 3-3
 - testing 3-4
 - up & down arrow keys 3-2
 - using 3-5
- G**
- general system information 5-1
- get
 - configuration file 5-20

- configuration from TFTP server 10-7
- global parameters 5-39
- global switch parameters 5-33
- green CSU LED 3-4
- green module status LED 3-4
- ground start 5-48
- grounding 2-1
- grounding instructions 2-2

H

- hardware revision 5-25
- help 5-7, C-1
- history
 - clear 4-9
 - view 4-9
- home 3-2
- home key 3-3

I

- I/F status 5-10
- ID number 5-43, 5-47
- ID presentation 5-43, 5-47
- identification number 4-6
- implement dedicated map 6-3
- in#accept 5-37
- incrementing fields 5-6
- information
 - controller 5-25
- init modem 4-6
- initialization 2-7
- initialize
 - modem 5-14
- initialize modem 4-6
- inject
 - errors 5-28
- insert
 - dedicated map connection 5-30
- insert password 5-17
- Installation 2-1
- installed memory 5-8
- installing
 - ATLAS 800 PLUS 2-1
 - modules 2-7
- interface
 - configuration 5-41
 - Nx 56/64 5-49
 - Octal BRI 5-50
 - Quad T1/PRI 5-41
- interface configuration 5-36, 5-39
- Introduction 1-1
- IP
 - status (Telnet utility) 10-3
- IP address
 - configure 5-13
 - TFTP server 5-19, 5-21
- IP adress
 - SNMP 5-15
- ISDN access switch
 - description 1-5

K

- keyboard keys 5-5
- keypad 3-1

L

- label
 - password 5-17
- LAN
 - connection 2-6
- layout
 - front panel 3-1, 3-2
- LB accept 5-27
- LBO
 - line build out 5-27
- LCD 3-1, 3-2
- LCV 5-26
- LED
 - clear system LED 5-10
 - CSU status 3-2
 - descriptions 3-3
 - error 3-4
 - module status 3-2, 3-4
 - OK 3-4
 - online 3-4
 - system 3-2, 3-3
 - test 3-4
- LED alarm 3-4
- LES 5-26
- levels
 - password 5-17
- line build out 5-27
- line code 5-27
- line code violaions 5-26
- line errored seconds 5-26
- LNK
 - ethernet status 4-4
- load configuration 5-21
- Loc LB 5-28
- local echo 10-3, 10-4
- local loopback 5-28
 - modules 5-28
- LOFC 5-26
- log
 - clear events 5-9
 - clear selftest 5-22
 - failure messages 5-9
 - field (Telnet utility) 10-6
 - system events 5-16
 - view selftest 5-22
 - warnings 5-9
- log out of a session 5-6
- loop start 5-48
- loopback
 - local 5-28
 - modules 5-28
 - remote 5-28
- loopback accept 5-27
- LOS 5-25
- loss of frame count 5-26
- loss of signal 5-25
- Lucent 5E 5-41
 - Octal BRI 5-50, 5-51
 - Quad T1/PRI 5-46

M

- main menu
 - diagram 4-3
- management via PC 3-8

- map
 - user map complete 7-7
 - map name 5-29
 - maps
 - dedicated 5-28
 - nailed 5-28
 - max telnet session 5-13
 - memory
 - installed 5-8
 - menu
 - alarm 4-9
 - configuration 4-5
 - item
 - activate 4-2
 - module 5-24
 - modules 5-23
 - path 5-4
 - session 10-1
 - status 4-4
 - submenu 5-25
 - system status 5-9
 - system utility 5-18
 - util 4-6
 - menu tree 4-3
 - menus
 - dedicated maps 5-28
 - dial plan 5-33
 - modules 5-23
 - system config 5-12
 - system info 5-7
 - system utility 5-18
 - method
 - signaling 5-44
 - MIB 10-1
 - modem
 - initialize 5-14
 - modem initialization 4-6
 - modem initialization string 5-14
 - module
 - configuration 5-27
 - menu 5-24
 - slot 5-23
 - slot number 3-2
 - state 5-24
 - status LED 3-2
 - type 5-23
 - update firmware 5-19
 - module settings 5-1
 - module slot
 - update firmware 5-18
 - module slots
 - preconfigure 5-23
 - module status 3-2
 - module submenu 5-25
 - modules
 - alarms 5-24
 - installing 2-7
 - menu options 5-23
 - online 5-24
 - status 5-24
 - test 5-24
 - test pattern 5-28
 - modules menu 5-23
 - MON 2-2, 2-6
 - MON test jack 2-6
 - Monitor 2-2
 - monitor 2-6
 - most significant digits (MSD) 5-42, 5-45, 5-46, 5-49
 - MSD 5-42, 5-45, 5-46, 5-49
- ## N
- nailed
 - maps 5-28
 - nailed map
 - activate 5-29
 - create/edit 5-29
 - current 5-29
 - name 5-29
 - name
 - TFTP server 5-19
 - National ISDN 5-41
 - Octal BRI 5-50, 5-51
 - navigating
 - terminal menus 5-2
 - navigating front panel 4-2
 - navigating the terminal menu 5-2
 - network
 - connection 2-5
 - management methods 1-4
 - map
 - complete 7-6
 - pinouts 2-6
 - specific facility data 5-42, 5-46
 - specific facility voice 5-42, 5-46
 - termination
 - configuration settings 5-41
 - Octal BRI 5-50
 - Quad T1/PRI 5-43
 - Quad T1/PRI configuration 5-41
 - terminations 5-33
 - new password 5-17
 - no response 5-24, 5-25
 - Northern DMS 100 5-41
 - Octal BRI 5-50, 5-51
 - Quad T1/PRI 5-46
 - NTWK1 2-2, 2-5
 - NTWK2 2-2, 2-5
 - number
 - complete template 5-40
 - of DS0s 5-48
 - of ports 5-50
 - number of DS0s 5-41, 5-43, 5-46
 - number of users currently logged into system 5-18
 - number type template 5-40
 - numbers
 - accept 5-35, 5-38
 - reject 5-36, 5-39
 - numeric keypad 3-1
 - NVRAM 4-8
 - Nx 56/64
 - interface configuration 5-49
 - user termination 5-50
- ## O
- Octal BRI
 - interface configuration 5-50
 - network termination 5-50

- switch type 5-51
- user termination 5-51
- offline 5-25
- offline/no response 5-25
- OK LED 3-4
- online 5-24
- online help 5-7
- online LED 3-4
- operating
 - front panel 4-1
 - terminal menu 3-5, 5-1
 - VT 100 3-7
- operating ATLAS 800 PLUS 3-5
- operation 3-1
- operation keys 3-3
- option slot
 - arrangement 2-7
 - numbering 2-7
- option slots
 - arrangement 2-7
- out#rej 5-36, 5-39
- outgoing caller ID 5-42, 5-47
- outgoing number conversion 5-41
- outgoing#accept 5-34
- overrun errors 5-12
- overview
 - product 1-1
- P**
- packing list 2-1
- panel
 - rear 2-2
- parameters
 - global 5-39
- part num 5-25
- passcode
 - set 4-8
- password
 - access 5-16, 5-17
 - add new 5-17
 - change 5-17
 - default 5-17
 - define 5-16
 - front panel 4-8
 - label 5-17
 - levels 5-17
 - new 5-17
 - reset 4-8
- path code 5-26
- pattern
 - clear 5-28
 - module test
 - test
 - pattern (modules) 5-28
- pattern clear 5-28
- PC management 3-8
- performance
 - 15 minutes 5-27
 - 24 hour 5-27
 - current 5-26
- performance data
 - clear 5-26
- performance monitoring 2-5
- pinout
 - 10-BaseT 2-6
 - chain in 2-4
 - chain out 2-5
 - control in 2-4
 - control in / chain in 2-4
 - control out / chain out 2-5
 - ethernet 2-6
 - Ethernet 10BaseT 2-6
 - network 2-6
 - PLL status 5-25
 - polls
 - no response 5-25
 - port 5-9
 - 10-Base-T 2-2
 - 10-BaseT 2-6
 - chain in 2-2, 2-3
 - chain out 2-4
 - control in 2-3
 - control out 2-4
 - dial plan 5-34
 - ethernet 2-6
 - ethernet status 5-10
 - menu (Telnet utility) 10-3
 - name 5-27
 - configure chain port 5-13
 - configure ethernet port 5-13
 - speed 5-14
 - port name 5-27
 - port type
 - configure chain port 5-13
 - ports
 - available
 - Nx 56/64 5-50
 - number of 5-50
 - power connection 2-1
 - power up testing 2-7
 - preconfigure
 - module slots 5-23
 - pre-sales support C-1
 - previous transfer status 5-21
 - previous update status 5-20
 - PRI
 - Quad T1/PRI 5-46
 - Quad T1/PRI configuration 5-41
 - PRI switch 5-41
 - primary search 5-35, 5-38
 - primary timing sources 5-12
 - print log 10-5
 - privileges
 - SNMP 5-15
 - PRMs
 - transmit 5-27
 - product
 - overview 1-1
 - provision network 7-3
 - Prt 5-26
 - prt 5-25
 - PS1 fail 5-10
 - PS2 fail 5-10
 - Q**
 - QRSS 5-28
 - QRSS generation 2-5
 - QRSS/RLB results 5-28

- Quad T1/PRI
 - interface configuration 5-41
 - network termination/PRI 5-41
 - network termination/RBS 5-43
 - user termination/PRI 5-46
 - user termination/RBS 5-48
- R**
- RBS 5-32
 - Quad T1/PRI 5-43, 5-48
- RCV 5-26
- real time clock 5-16
- rear panel 2-2
- reboot system 5-22
- receive level 5-26
- red alarm 5-25
- red CSU LED 3-4
- red module status LED 3-4
- refresh screen 10-4
- reject numbers 5-36, 5-39
- remote access
 - setup with dial plan 7-2
- remote LB 5-28
- remote loopback 5-28
- repair C-1
- reset password 4-8
- response # 4-8
- restart
 - date and time 5-19
 - schedule 5-19
 - schedule after update 5-19
 - system 5-22
- restore factory default settings 5-6
- results
 - clear 4-8, 5-28
 - module test 5-28
- retrieve
 - configuration from TFTP server 10-7
- return C-1
- return material authorization C-1
- rev 5-25
- revision
 - boot ROM 5-8
 - controller 5-8
 - firmware 5-8
 - hardware 5-25
 - software 4-7
- RMA C-1
- RMA requests C-1
- robbed bit signaling 5-32
- routback rejection 5-40
- RTC RAM 4-8, 5-22
- RTS
 - chain port signal leads 5-11
 - chain port status 4-4
- RX
 - ethernet status 4-4
- Rx
 - level 5-26
- Rx frames 5-10
- S**
- S0 system
 - config menu 4-5
 - status menu 4-4
- S1-S8
 - config menu 4-6
 - status menu 4-4
- save
 - configuration file 5-21
- saving
 - configuration to TFTP server 10-6
- schedule
 - restart system 5-19
- secondary search 5-35, 5-38
- security
 - TFTP server 10-7
- security levels 5-17
- SEFS 5-26
- select
 - front panel items 4-2
- selftest 2-7, 4-7
 - clear log 5-22
 - clear results 4-8
 - failure messages 10-1
 - run 4-7, 5-21
 - show results 4-8
 - system 5-21
 - view log 5-22
- send
 - configuration file 5-20
- serial number 5-8
- service C-1
- SES 5-26
- session
 - menu 10-1
- session timeout 5-12
- set
 - data field 4-2
 - date 4-6, 5-8, 5-16
 - time 4-6, 5-8, 5-16
- set passcode 4-8
- set up passwords 5-16
- setting default gateway 3-6
- setting subnet mask 3-6
- setup
 - remote access 7-2
 - video conferencing 7-2
- severely errored frame seconds 5-26
- severely errored seconds 5-26
- severity level threshold 5-16
- severity of event 5-9
- shift 3-2
- shift key 3-2
- show results 4-8
- sig
 - dial plan 5-34
- sig status 5-26
- signaling
 - dial plan 5-34
 - status 5-26
 - user termination 5-37
- signaling conversion
 - description 1-3
- signaling method 5-44, 5-48
- slot 5-9
 - dial plan 5-34
 - update firmware 5-18

- slot/port
 - user termination 5-37
 - slt 5-23
 - SNMP 5-14
 - access 5-14
 - communities 5-14
 - IP address 5-15
 - privileges 5-15
 - software rev 4-7
 - solid green system LED 3-3
 - solid red system LED 3-3
 - sort to/from 5-29
 - source ID 5-34, 5-37, 5-43, 5-45, 5-47, 5-49
 - speech
 - accept 5-35, 5-38
 - reject 5-36, 5-39
 - SPID list 5-50
 - Octal BRI 5-51
 - start
 - ground 5-48
 - loop 5-48
 - start telnet session 3-6
 - startup mode
 - mode
 - startup 5-8
 - state
 - module 5-24
 - status
 - 10-BaseT 5-10
 - alarm 5-25
 - current configuration transfer 5-21
 - current firmware update 5-20
 - current update 5-19
 - DS0 5-26
 - ethernet port 5-10
 - field 4-2
 - field (Telnet utility) 10-6
 - I/F 5-10
 - menu 4-4
 - modules 5-24
 - PLL 5-25
 - previous update 5-20
 - previous updates 5-21
 - status menu
 - chain port status 4-4
 - ethernet status 4-4
 - S1-S8 4-4
 - storing
 - configuration on TFTP server 10-6
 - strip MSD 5-42, 5-45, 5-46, 5-49
 - structure
 - front panel 4-1
 - terminal menu 5-1
 - submenu
 - menu 5-25
 - modules 5-25
 - subnet mask
 - config menu 4-5
 - configure 5-13
 - support C-1
 - post-sales C-1
 - pre-sales C-1
 - SW56 5-44
 - swap ANI/DNIS 5-43, 5-47
 - switch parameters 5-33
 - switch type 5-41
 - Octal BRI 5-50, 5-51
 - Quad T1/PRI 5-46
 - switched call parameters 5-2
 - Syslog
 - host facility 5-16
 - IP address 5-16
 - setup 5-16
 - transmission 5-16
 - system
 - alarm 5-10
 - config 5-12
 - configuration menu 5-12
 - contact 5-8
 - event log
 - clear 5-9
 - event logging 5-16, A-1
 - info menu 5-7
 - information 5-7
 - LED 3-2, 3-3
 - clear 5-10
 - location 5-8
 - name 5-7
 - resource usage 5-10
 - restart 5-22
 - selftest 5-21
 - status 5-1, 5-9
 - status menu 5-9
 - timing sources 5-10
 - uptime 5-8
 - utility 5-18
 - utility menu 5-18
- T**
- T1 bandwidth management
 - description 1-5
 - T1/PRI interface ports 5-23
 - TDM MAP 4-8
 - TDM RAM 5-22
 - technical support C-1
 - Telnet
 - delivered utility 10-1
 - telnet 3-6
 - define IP address 3-6
 - maximum sessions 5-13
 - set default gateway 3-6
 - set subnet mask 3-6
 - start session 3-6
 - temp fail 5-10
 - template
 - number complete 5-40
 - number type 5-40
 - terminal emulation 3-7
 - terminal menu 5-6
 - copy items to clipboard 5-6
 - decrementing fields 5-6
 - delete list item 5-7
 - extended help 5-4
 - graphic layout 5-4
 - help 5-7
 - insert new list item 5-7
 - invalidate the password entry 5-6
 - left pane 5-4

- log out of a session 5-6
 - menu path 5-2, 5-4
 - moving around in 5-2
 - navigating 5-2
 - navigating with the keyboard keys 5-5
 - navigation help 5-4
 - operating 3-5
 - operation 5-1
 - paste items from clipboard 5-6
 - port status 5-4
 - refresh the screen 5-6
 - restore factory default settings 5-6
 - right pane 5-4
 - right pane notation 5-5
 - structure 5-1
 - Sys 5-4
 - system time 5-4
 - tool tip 5-4
 - window panes 5-2
 - terminal menu structure 5-1
 - termination
 - network
 - Octal BRI 5-50
 - user
 - Octal BRI 5-51
 - terminations
 - user 5-36
 - test 5-28
 - inject errors 5-28
 - modules 5-24
 - self 2-7
 - test jack 2-6
 - MON 2-6
 - test LED 3-4
 - test pattern 5-28
 - error inject 5-28
 - test results
 - clear 4-8
 - testing
 - power up 2-7
 - TFTP
 - delivered utility 10-1, 10-4
 - save configuration file 5-21
 - security 10-7
 - server filename 5-19, 5-21
 - server IP address 5-19, 5-21
 - update firmware 5-18, 5-19, 8-1, 8-4
 - time
 - current 5-16
 - restart schedule 5-19
 - restart system 5-19
 - set 5-8
 - time event log/time 5-9
 - time/date 4-6
 - timeout
 - end of number 5-39
 - terminal session 5-12
 - timing source
 - backup 5-12
 - primary 5-12
 - timing sources 5-10
 - tips for troubleshooting B-1
 - to clipboard 10-5
 - To Config 5-32
 - to printer 10-5
 - TO slot 5-32
 - transfer
 - configuration file 5-20
 - current status 5-21
 - method 5-20
 - previous status 5-21
 - transfer method
 - update firmware 5-19
 - transmit PRMs 5-27
 - trap
 - destination 5-15
 - community 5-15
 - filtering 5-15
 - trap transmission 5-15
 - authenticate 5-15
 - treat call as
 - accept 5-35, 5-39
 - reject 5-36
 - troubleshooting B-1
 - trunk
 - number 5-45
 - trunk conditioning 5-31
 - defining 5-32
 - trunk type 5-44
 - T-Watch PRO 3-8
 - TX
 - ethernet status 4-4
 - Tx frames 5-10
 - Tx PRMs 5-27
 - Tx yellow alarm
 - enable/disable 5-27
 - type
 - module 5-23
- ## U
- UAS 5-26
 - unavailable seconds 5-26
 - unit ID 4-6
 - up and down arrows 3-1, 3-2
 - up arrow key 3-2
 - update
 - current status 5-19
 - firmware 5-18
 - module slot 5-18
 - restart schedule 5-19
 - TFTP 8-1, 8-4
 - XMODEM 8-1
 - previous status 5-20
 - update status 5-20
 - updating
 - firmware 8-1
 - upload
 - configuration file 5-20
 - uptime
 - system 5-8
 - usage
 - DS0 5-26
 - use configuration 5-21
 - user
 - map completed 7-7
 - termination
 - configuration settings 5-41
 - Nx 56/64 5-50

- Octal BRI 5-51
- Quad T1/PRI 5-46, 5-48
- terminations 5-36
- users logged into system, number of 5-18
- using
 - terminal menu 5-2
- using front panel 3-5
- util menu 4-6
- utilities 10-1
- utility
 - Telnet 10-1
 - TFTP 10-1
 - TFTP server 10-4
 - VT 100 10-1, 10-3
- utility menu 4-6

V

- video conferencing
 - setup with dial plan 7-2
- view
 - event log 5-16
 - selftest log 5-22
- view error log 5-9
- view history 4-9
- voice/SW56 5-44
- VT 100

- delivered utility 10-1, 10-3
- operation 3-7

W

- WAN overbooking
 - description 1-5
- warnings
 - view log 5-9
- warranty C-1
- window
 - LCD 3-1, 3-2
- writing
 - configuration to TFTP server 10-6

X

- XMODEM
 - update firmware 5-18, 5-19, 8-1

Y

- yellow alarm 5-25
 - auto TX 5-27
 - enable/disable 5-27
- yellow CSU LED 3-4
- yellow system LED 3-3

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 # _____

