ATLAS 550

User Manual

Part Number 1200305L1

61200305L1-1B
May 2000

TRADEMARKS

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

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

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

1. This equipment complies with Part 68 of the FCC rules. The required label is affixed to the bottom of the chassis.
2. An FCC-compliant telephone cord with a modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68-compliant. See Chapter 2, *Installation*, for details.
3. If your telephone equipment (ATLAS 550) 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 550), please contact ADTRAN at (256) 963-8000 for repair / warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or until you are sure the equipment is not malfunctioning.
6. This unit contains no user-serviceable parts.
7. The following information may be required when applying to your local telephone company for leased line facilities.

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

Federal Communications Commission Radio Frequency Interference Statement

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

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

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

Affidavit Requirements for Connection to Digital Services

- An affidavit is required to be given to the telephone company whenever digital terminal equipment without encoded analog content and billing protection is used to transmit digital signals containing encoded analog content which are intended for eventual conversion into voiceband analog signals and transmitted on the network.
- The affidavit shall affirm that either no encoded analog content or billing information is being transmitted or that the output of the device meets Part 68 encoded analog content or billing protection specifications.
- End user / customer will be responsible for filing an affidavit with the local exchange carrier when connecting unprotected customer premise equipment (CPE) to 1.544 Mbps or subrate digital services.
- Until such time as subrate digital terminal equipment is registered for voice applications, the affidavit requirement for subrate services is waived.

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

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

State of _____

County of _____

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

_____ (telephone number) being duly sworn, state:

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

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

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

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

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

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

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

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

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

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

_____Signature

_____Title

_____ Date

Transcribed and sworn to before me

This _____ day of _____, _____

_____
Notary Public

My commission expires:

_____

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.

About this Manual

The ATLAS 550 system consists of the Base Unit, at least one network module, and one or more option modules. (Each network / option module includes its own user manual which contains specific information about installing, configuring, and testing the option module; insert the option module manuals into this binder.) The ATLAS 550 *User Manual* provides the information you need to install, configure, test, and troubleshoot the ATLAS 550 system; when applicable, this manual refers you to the individual network / option module user manual. The arrangement of this user manual allows you to quickly and easily find the information you need. An overview of the contents of this manual follows:

Introduction

- Chapter 1, *Introduction*, familiarizes you with the ATLAS 550 Base Unit and provides some sample ATLAS 550 applications.

Getting Started

- Chapter 2, *Installation*, describes unit installation and the rear panel design.
- Chapter 3, *Operation*, describes different ways to operate the ATLAS 550.

Reference Information

- Chapter 4, *Using the Front Panel*, describes how to use the front panel.
- Chapter 5, *Navigating the Terminal Menus*, describes how to navigate the terminal menus.
- Chapter 6, *System Control Terminal Menus*, describes the terminal menus used for system control.
- Chapter 7, *Module Terminal Menus*, describes the terminal menus used for network and option module control.
- Chapter 8, *Packet Manager*, describes the terminal menus used for defining packet endpoints.
- Chapter 9, *Router*, describes the terminal menus associated with the integral router.
- Chapter 10, *Dedicated Maps*, describes the terminal menus used for dedicated maps and provides some examples.
- Chapter 11, *Dial Plan*, describes the terminal menus used for dial plans.

Working with the ATLAS 550

- Chapter 12, *Updating Firmware*, provides step-by-step instruction on how to update the ATLAS 550 firmware.
- Chapter 13, *SNMP Management*, describes using SNMP to control the ATLAS 550.
- Chapter 14, *ADTRAN Utilities*, describes the SysLog, Telnet, VT-100, and TFTP Server programs delivered with the ATLAS 550.

Appendices

- Appendix A, *System Event Logging*, describes the system events monitored by the ATLAS 550.
- Appendix B, *OSI Model and Frame Relay Technology Overview*, presents a summary of frame relay technology.
- Appendix C, *Frame Relay Examples*, provides step-by-step instructions for setting up frame relay.
- Appendix D, *Router Examples*, provides step-by-step instructions for setting up the router.
- Appendix E, *Troubleshooting*, provides solutions to some problems you may experience.
- Appendix F, *Acronyms and Abbreviations*, lists acronyms and abbreviations used for the ATLAS 550 and its option modules.
- Appendix G, *Glossary*, defines terms used with ATLAS 550 and its option modules.

Notations and Conventions

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

Notes provide additional useful information.

Cautions signify information that could prevent service interruptions.

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

Menu Items

Terminal menus and options are distinguished from regular text by using a bold font and small, uppercase letters. For example, "Use the **SYSTEM UTILITY** menu to view and set system parameters."

Keyboard Commands

The keyboard keys used to carry out commands are highlighted in bold. Examples include **Enter**, **I** (insert), or **C** (copy).

Limited Product Warranty

ADTRAN warrants that for five (5) years from the date of shipment to Customer, all products manufactured by ADTRAN will be free from defects in materials and workmanship. ADTRAN also warrants that products will conform to the applicable specifications and drawings for such products, as contained in the Product Manual or in ADTRAN's internal specifications and drawings for such products (which may or may not be reflected in the Product Manual). This warranty only applies if Customer gives ADTRAN written notice of defects during the warranty period. Upon such notice, ADTRAN will, at its option, either repair or replace the defective item. If ADTRAN is unable, in a reasonable time, to repair or replace any equipment to a condition as warranted, Customer is entitled to a full refund of the purchase price upon return of the equipment to ADTRAN. This warranty applies only to the original purchaser and is not transferable without ADTRAN's express written permission. This warranty becomes null and void if Customer modifies or alters the equipment in any way, other than as specifically authorized by ADTRAN.

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

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

Additional Warranty Information

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. See the last page of this manual for information on contacting ADTRAN Technical Support.

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

PRODUCT OVERVIEW

The ATLAS 550 is a modular, highly scalable platform that provides robust solutions for the wide area communication needs of small-to-medium corporations and network access providers. ATLAS 550 is an Integrated Access System with the most extensive support of dedicated bandwidth management and access switching in the industry.

The ATLAS 550 is a lower bandwidth version of the ATLAS 800^{PLUS}. The ATLAS 550 contains a high-performance CPU and powerful communications drivers which allow the support of optional applications such as frame relay.

The ATLAS 550 architecture also includes a packet switching and a circuit switching bussing scheme. The result is a system capable of supporting bandwidth requirements up to four T1/E1 or Primary Rate ISDN (PRI) circuits. Designed for standalone, rackmount, or wallmount installations, the ATLAS 550 Base Unit provides two hot-swappable network interfaces and four expansion slots that accommodate hot-swappable modules for a variety of applications. A 10/100BaseT Ethernet connection for remote access and network management is standard with the ATLAS 550 Base Unit.

The ATLAS 550 modules include the following:

- Dual Nx 56/64 Option Module
- Dual T1/PRI Option Module
- Quad Basic Rate ISDN Option Module
- Octal/Quad FXS Option Module
- Octal/Quad FX0 Option Module
- Resource Host Module
- Voice Compress Resource Module
- T1 Network Interface Module

With the ATLAS 550, you can consolidate your voice, data, and video applications into a single platform while optimizing wide area bandwidth and reducing equipment costs. The ATLAS 550 architecture and the chassis' four 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 two main functions of the ATLAS 550 are to act as an *Access Router* and an *Access Switch*.

Access Router

As an Access Router, the ATLAS 550 combines the functions of a T1 CSU / DSU, an intelligent channel bank, a T1 Multiplexer, and DACS into a single platform. The ATLAS 550 is ideal for point-to-point configurations or access to public networks. For optimization of existing equipment and network resources, the ATLAS 550 can support a variety of data and analog voice applications (see Figure 1-1). The Access Router also supports a wide range of data applications including T1 “drop and insert,” channel grooming, and wide area data transport.

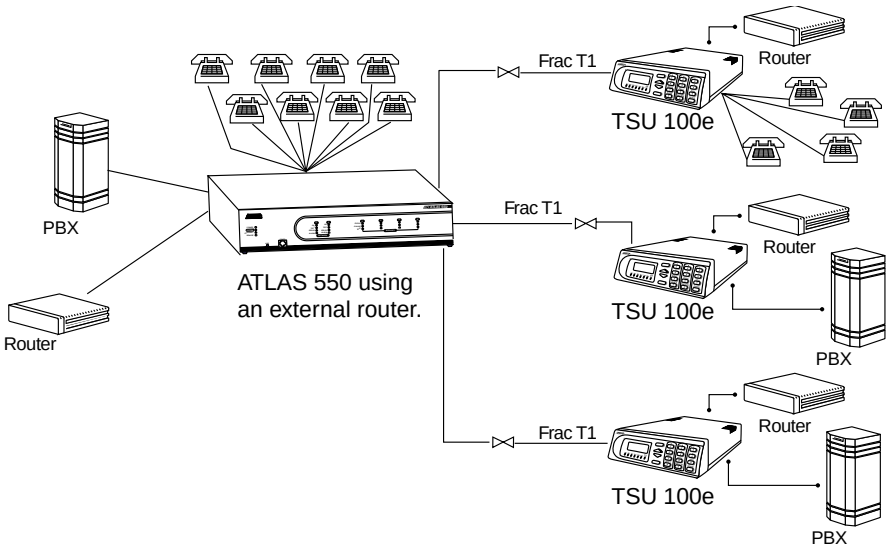


Figure 1-1. Point-to-Point Circuit with External Routers

Frame Relay/Router

The Frame Relay / Router features enable the Access Router to act as a voice / data FRAD, a frame relay switch, and an IP router in addition to acting as an available bandwidth manager and a switch application.

Frame Relay

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

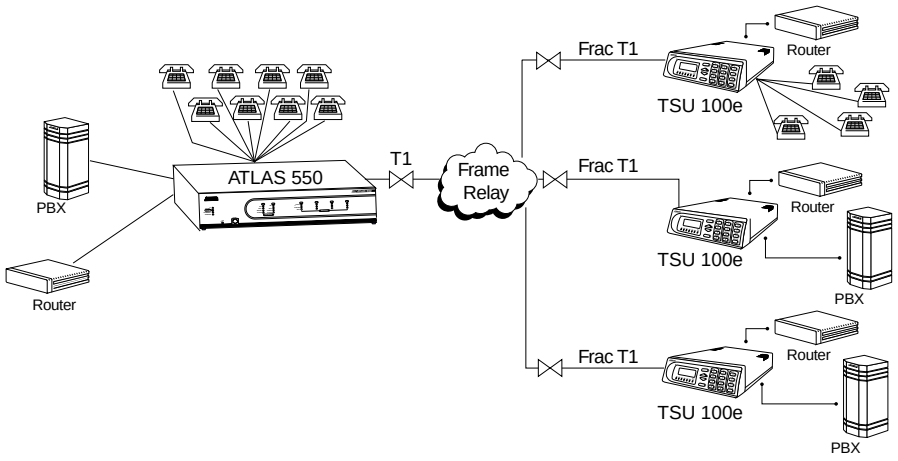


Figure 1-2. Frame Relay Circuit

Router

The ATLAS 550 router uses the Ethernet port to transmit local area network (LAN) traffic over the wide area network (WAN) to a remote LAN. By integrating the router into the network access device, you benefit from the cost savings of not requiring an external router. Figure 1-1 and Figure 1-3 illustrate a conversion from an application with external routers to one using integral routers within ADTRAN products.

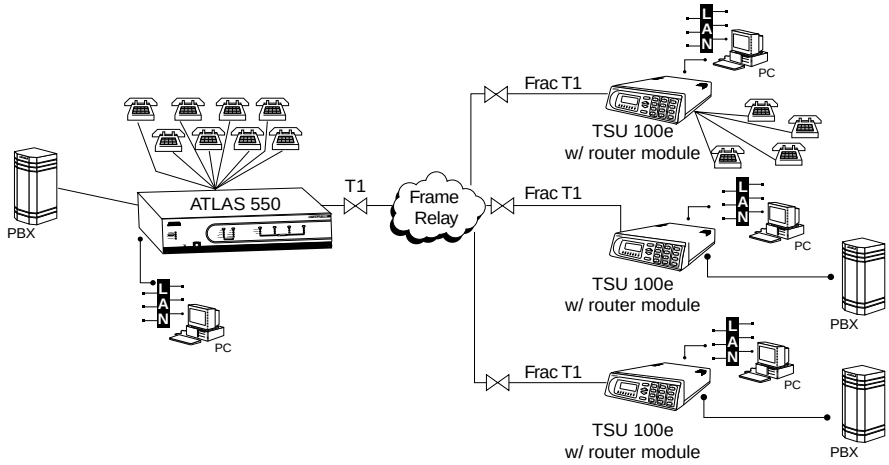


Figure 1-3. Frame Relay Circuit with Internal Routers

Access Switch

The ATLAS 550 includes an advanced access architecture for switching dialup calls to specific ports or DS0s. As an access switch functioning in user-to-user network and user-to-user mode, ATLAS 550 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. The ATLAS 550 also converts between ISDN D channel (PRI or

BRI) and T1 Robbed Bit Signaling (RBS) giving you the flexibility to get the speed and reliability of ISDN, while preserving your investment in non-ISDN equipment. AMI and B8ZS line coding provides interoperability with legacy equipment (see Figure 1-4). For network optimization, when bandwidth is not being used for switched applications such as video conferencing, switched connection mapping dynamically allocates bandwidth to the PBX for voice traffic. Call Filtering allows you to program the call types that will be answered and / or originated on a per-user basis.

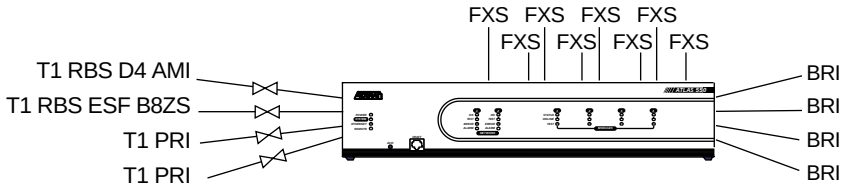


Figure 1-4. The Access Switch

Additional Applications

The following sections describe additional applications using the ATLAS 550.

Dedicated and Switched Connection Maps in a Single Platform

The ATLAS 550 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 four T1 circuits in the system. Dedicated connection maps can be manually invoked or automatically implemented based on the time of day and day of the week.

Additionally, the ATLAS 550 can be configured to switch dialup calls to specific ports or DS0s based on the number that is dialed. Switched connection mapping is supported for dialup calls placed over analog / digital voice basic rate ISDN (BRI) or primary rate ISDN (PRI).

WAN Overbooking

The WAN Overbooking feature of the ATLAS 550 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 required connectivity. Local subscriber-to-subscriber connections are made without accessing the network at all, resulting in even more efficient use of wide area bandwidth.

Digital Access Cross-Connect System (DACS)

Inherent in the ATLAS 550 architecture is the ability to cross connect, or DACS, 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 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.

Flexible Network Management and Maintainability

Several network management methods are available for the ATLAS 550, including SNMP support. VT-100 and Telnet are also offered, proving 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 by using either the control port, the CRAFT port, or the Ethernet interface. The Ethernet interface on the Base Unit provides a connection at 10 MBS or 100 MBS.

User configurations can be preserved in nonvolatile memory and duplicated for managing multiple ATLAS 550 implementations. ATLAS 550 also supports flash upgrades for future enhancements. You can remotely download software using TFTP or XMODEM.

The ATLAS 550 front panel contains an extensive array of LEDs for alarm and status information pertaining to the system and the individual modules.

Several test capabilities allow you to diagnose the health of your T1, PRI, or BRI circuits without additional test equipment. Tests include local, remote, and V.54 loopbacks using the 511, QRSS, all zeros, and all ones test patterns. Standard Bantam test jacks located on the ATLAS 550 network modules also allow you to use external test equipment to monitor traffic.

ATLAS 550 FEATURES

Configuration and Management

- VT-100 Emulation
- SNMP, per MIB II (RFC1213), DS1 MIB (RFC1406), and ADTRAN private MIBs
- Telnet
- Six levels of password protection and privileges

Software Upgrade

- Flash memory
- TFTP download
- XMODEM via control port

Signaling Support

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

ISDN Switch Types

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

Dedicated Connection Maps

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

Switched Connection Maps

- Inbound and outbound call filtering and blocking

Testing

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

Performance Monitoring

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

Frame Relay/Integral Router

- Routes Internet Protocol (IP) traffic between a public or private frame relay network and the Ethernet port.
- Concentrates IP traffic from a public or private frame relay network to one or more serial ports (V.35). The protocol passed over the serial port is frame relay.
- Passes Systems Network Architecture (SNA), Bisync, and other legacy protocols between a public or private frame relay network and an external DTE running frame relay to ATLAS.
- Performs voice compression / decompression (G.723.1) and interfaces to either a Private Branch Exchange (PBX) or the Public Switched Telephone Network (PSTN). (This feature requires an additional option module, the VCOM Module—P / N 1200312Lx.)

Chapter 2 Installation

This chapter discusses the installation process and the ATLAS 550 rear panel design.

INSPECTING THE ADTRAN SHIPMENT

Before installing the ATLAS 550, carefully inspect the ATLAS 550 Base Unit for shipping damage. If you suspect damage, file a claim immediately with the carrier and then contact ADTRAN Technical Support (see the last page of this manual). If possible, keep the original shipping container for returning the ATLAS 550 for repair or for verification of damage during shipment.

Contents of ADTRAN Shipments

Your ADTRAN shipment includes the following items:

- The ATLAS 550 Base Unit
- The ATLAS 550 *User Manual*
- AC Power cord - ADTRAN P/N 3127031
- Network cable (1) - ADTRAN P/N 3125M008
- Rackmount brackets and screws
- RJ-45—DB-25 adapter (1 for modem connection)
- RJ-45 control port cable (1) - ADTRAN P/N 3127004
- RJ-45—DB-9 adapter (1)
- ADTRAN Utilities diskettes (3)

Customers must supply the Ethernet cable.

GROUNDING INSTRUCTIONS

This section provides grounding instruction information from the Underwriters' Laboratory UL 1950 Standard for Safety of Information Technology Equipment Including Electrical Business Equipment, of July 28, 1995.

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

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

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

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

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

SUPPLYING POWER TO THE UNIT

The AC powered ATLAS 550 comes equipped with a detachable 8-foot power cord with a 3-prong plug for connecting to a grounded power receptacle. As shipped, the ATLAS 550 is set to factory default conditions. After installing the Base Unit and any option modules, the ATLAS 550 is ready for power-up. To power-up the unit, ensure that the unit is properly connected to an appropriate power source and turn on the unit using the on / off switch on the rear panel.

- *This unit shall be installed in accordance with Article 400 and 364.8 of the NEC NFPA 70 when installed outside of a Restricted Access Location (i.e., central office, behind a locked door, service personnel only area).*
- *Power to the ATLAS 550 must be from a grounded 90-240 VAC, 50/60 Hz source.*
- *The power receptacle uses double-pole, neutral fusing.*
- *Maximum recommended ambient operating temperature is 40°C.*

MOUNTING OPTIONS

The ATLAS 550 Base Unit may be installed for tabletop, 19-inch or 23-inch rackmount, or wall-mount configuration. ADTRAN includes 19-inch rackmount ears with the Base Unit (23-inch rackmount ears are sold separately). For a rackmount installation, the ATLAS 550 Base Unit allows flush-face mount, face-forward mount, center mount, and rear mount. The rackmount ears may also be turned face down for wall-mounting. When wall-mounted, the ATLAS 550 Base Unit may be installed with either side up and the front and rear panels facing sideways.

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

REVIEWING THE REAR PANEL DESIGN

The ATLAS 550 rear panel contains four slots for housing option modules which provide a variety of additional resources and data ports. All slots are functionally identical. The ATLAS 550 also contains two slots for housing network interface modules (see Figure 2-1 on page 2-4).

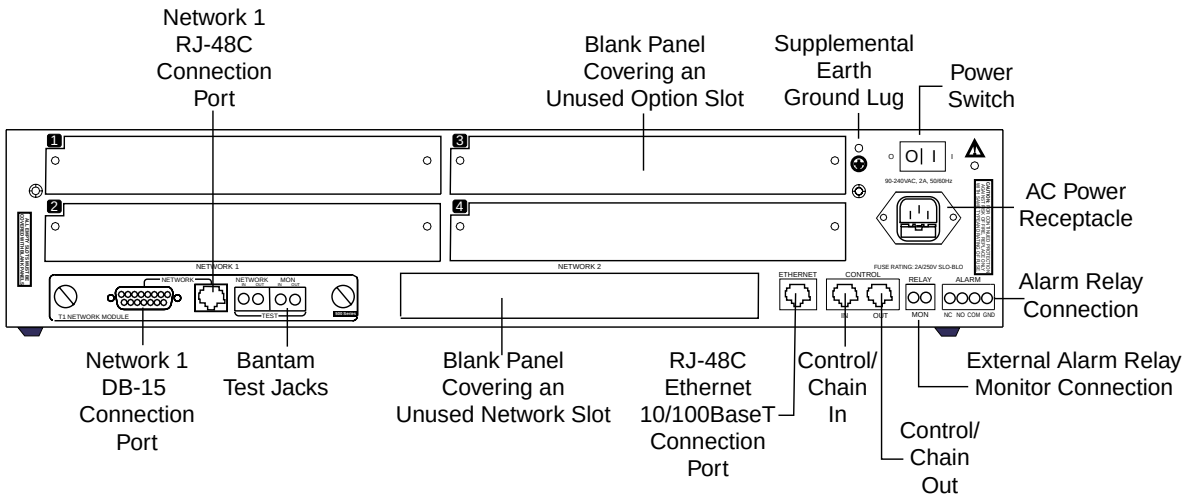


Figure 2-1. ATLAS 550 Rear Panel

Control/Chain In Port

The Control / Chain In port (EIA-232) connects to a computer or modem or to another ATLAS 550 Base Unit. The control port input provides the following functions:

- Accepts EIA-232 input from a PC or a modem for controlling the ATLAS 550.
- Operates at 2400, 9600, 19200, or 38400 bps.
- Acts as input for either PC control or a chained connection.
- Acts as an interface for flash memory software downloads using XMODEM.

The Control / Chain In connection follows, and Table 2-1 shows the pinout.

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

Table 2-1. Control/Chain In Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis
2	RTS	Request to send - flow control
3	RXDATA	Data received by the ATLAS 550
4	DTR	Data terminal ready
5	TXDATA	Data transmitted by the ATLAS 550
6	CD	Carrier detect
7	UNUSED	—
8	CTS	Clear to send - flow control

Control/Chain Out Port

The Control / Chain Out port (RJ-48C) connects to another ATLAS 550 Chain In connector. The Control / Chain Out port output provides the following:

- EIA-232 output to chain control to other ADTRAN equipment, such as a TSU 120.
- 2400, 9600, 19200, or 38400 bps operation
- Automatic setup; no user input required

The Control / Chain Out connection follows, and Table 2-2 shows the pinout.

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

Table 2-2. Control/Chain Out Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis. Connects to GND of next unit.
2	UNUSED	—
3	TX DATA	Data transmitted to chained units by the ATLAS 550. Connects to RX DATA of the next unit.
4	UNUSED	—
5	RX DATA	Data received from chained units by the ATLAS 550. Connects to TX DATA of the next unit.
6,7,8	UNUSED	—

Ethernet Connection

The Ethernet port (RJ-48C) provides a 10 / 100BaseT Ethernet LAN connection, which is used for TFTP, SNMP, and Telnet connection. The network connection follows, and Table 2-3 shows the pinout.

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

Table 2-3. Ethernet Pinout

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

Alarm Relay Connection

This connection alerts the user when a selected alarm condition exists. The four-pin, removable terminal block connects with external wiring. To make the appropriate connections, remove the block, connect wiring as needed, and return the terminal block to the connector socket. Clear the alarm condition by pressing the Alarm Cut-Off (ACO) switch located on the font panel of the ATLAS 550.

After the appropriate connections have been made, tighten the screws using a flathead screwdriver before reinserting the terminal block into the rear panel of the ATLAS 550.

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

Table 2-4. Alarm Relay Connector Pinout

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

External Alarm Relay Monitor Connection

This connection alerts the user when a selected external alarm condition exists. This connection could be used to monitor a UPS with dry contacts or another ATLAS 550. The two-pin, removable terminal block connects with external wiring. To make the appropriate connections, remove the block, connect wiring as needed, and return the terminal block to the connector socket. Clear the alarm condition by pressing the ACO switch located on the front panel of the ATLAS 550.

After the appropriate connections have been made, tighten the screws using a flathead screwdriver before reinserting the terminal block into the rear panel of the ATLAS 550.

Table 2-5 shows the pinout for the External Alarm Relay connector.

Table 2-5. External Relay Monitor Connector Pinout

Pin	Name	Description
1	Alarm Out	Outputs EIA-232 level signal for connection to external alarm contacts.
2	Alarm In	Monitors signal coming from external alarm contacts.

Network Connection

The ATLAS 550 provides two Network Interface Slots that allow different types of interfaces to be used. Currently only a T1 Network Interface is available. In the remainder of this manual, discussions about the Network Interface Module refer to the T1 Network Interface Module. The T1 Network Interface (NI) port complies with the applicable ANSI and AT&T® standards. The T1 Network Interface Module provides the following functions:

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

The network connections follow, with the pinouts shown in Table 2-6 and Table 2-7 on page 2-8.

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

Table 2-6. Network RJ-48C Pinout

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

Connector type 15-pin Male D-connector
Part number AMP# 74784-12

Table 2-7. Network Interface 15-pin Male D-connector Pinout

PIN	NAME		DESCRIPTION
1	T	TXDATA-TIP	Transmit data toward the network
2		UNUSED	
3	T1	RXDATA-TIP	Receive data from the network
4, 5, 6, 7		UNUSED	
8	FG	FRAME GROUND	Grounded to chassis
9	R	TXDATA-RING	Transmit data toward the network
10		UNUSED	
11	R1	RXDATA-RING	Receive data from the network
12, 13, 14		UNUSED	
15	FG	FRAME GROUND	Grounded to chassis

Test Interface

The **NETWORK IN** and **OUT** Bantam test jacks provide intrusive test capability for the incoming T1. By connecting test equipment to these jacks, the T1 connection breaks and the test equipment terminates the incoming T1. The **MON IN** and **OUT** Bantam test jacks provide a bridged access jack for nonintrusive monitoring of the incoming T1. When connected to this jack, configure the test equipment for bridged termination.

Frame Relay Specifications

- Packet throughput at 4000 pkts/sec
- Management signaling interfaces
  - UNI (user-to-network interface)
  - NNI (network-to-network interface)
- Management signaling types
  - ANSI T1.617-D (Annex D)
  - ITU-T Q.933-A (Annex A)
  - LMI (Group of four)
  - Auto
- Encapsulation - RFC 1490 for IP and LLC2
- PVC support - 300 PVCs

- Congestion control
  - FECN / BECN
  - Discard eligible (DE)
- Quality of service (QOS) - Prioritization on a per-PVC basis
- Testing (ADTRAN proprietary)
  - PVC loopback
  - Round trip delay measurement
- SNMP support - RFC 1315

IP Router Specifications

- Route discovery
  - RIP V1
  - RIP V2
  - ICMP
  - ARP
  - IARP
  - UDP Relay
- Virtual connections supported - 100 PVCs
- SNMP support - MIB II

Option Slots

Figure 2-2 shows the option slot numbering designation as viewed from the rear of the ATLAS 550. The functionally identical option slots only accept ATLAS 550 option modules.

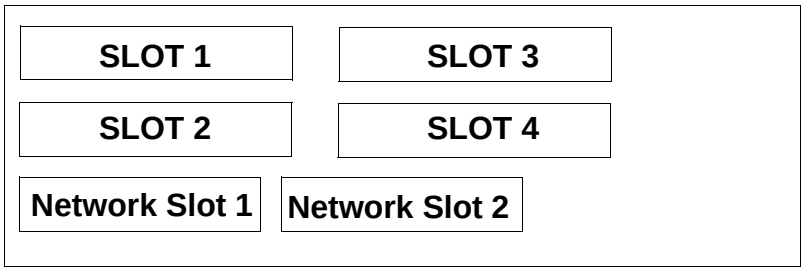


Figure 2-2. ATLAS 550 Slot Designation (Rear Panel)

INSTALLING OPTION MODULES

After installing the ATLAS 550 Base Unit and connecting the required cables, you can install your choice of option modules. Instructions for installing option modules are given in the user manuals for the chosen modules.

Chapter 3 Operation

OVERVIEW

To fully operate the ATLAS 550, you must connect to the terminal menus using VT-100 terminal emulation or a Telnet session. The following sections provide an overview of these methods of operating the ATLAS 550.

USING THE TERMINAL MENUS

The terminal menu provides the primary means of monitoring and configuring the ATLAS 550. The terminal menu interface uses the full capabilities of the VT-100 terminal to provide the quickest and most intuitive operation possible. (Access the terminal menu by using a VT-100 terminal or a computer running VT-100 terminal-emulation software.) To receive the full benefit of the terminal menu interface, you should use a fully VT-100 compatible client. The *ADTRAN Utilities* floppy disks (that you can install on a PC) contain both a VT-100 client and a customized Telnet program. See *ADTRAN Utilities* on page 14-1 for details on the available programs.

The three basic connection methods supported by the ATLAS 550 are a direct connection through the EIA-232 Control / Chain In port (located on the rear panel), a direct connection through the EIA-232 CRAFT port (located on the front panel), and a Telnet session. The following sections describe using VT-100 terminal emulation (for either of the two EIA-232 ports) and establishing a Telnet session.

Using VT-100 Terminal Emulation

You can access the ATLAS 550 terminal menu, using VT-100 terminal emulation, from either the Control / Chain In port on the rear panel or the CRAFT port on the front panel. Both of these ports provide an EIA-232 serial connection. The following Step / Action table provides instructions for setting up the ATLAS 550 for VT-100 terminal mode.

Instructions for Setting Up an ATLAS 550 for VT-100 Terminal Mode	
Step	**Action**
1	Set the baud rate on the VT-100 terminal to 9600 baud (8/N/1).
2	Use the ADTRAN-provided VT-100 terminal adapter to connect the **COM** port of a VT-100 compatible terminal, or equivalent, to the eight-pin modular jack labeled **CONTROL/CHAIN IN** on the rear panel **or** labeled **CRAFT** on the front panel. This connection provides both local and remote configuration.
3	Press **Enter** repeatedly on the keyboard until the **LOGIN** menu requiring a password appears.
4	Press **Ctrl-R** to refresh the display, if necessary.

When you begin the VT-100 session, you will be prompted for a password. The default password is *password* (which is a Level 0 superuser password). You can change this password using the **ACCESS PASSWORDS** option, which is only accessible through the terminal menu. See *Access Passwords* on page 6-15 for details. After your password is accepted, define the IP Address of the ATLAS 550 to which you want to connect. The following Step / Action chart describes this process.

Instructions for Defining the IP Address	
Step	**Action**
1	Obtain an IP address for the ATLAS 550 from your LAN administrator.
2	Use the ADTRAN-provided VT-100 terminal adapter to connect the **COM** port of a VT-100 compatible terminal, or equivalent, to the eight-pin modular jack labeled **CONTROL/CHAIN IN** on the rear panel or labeled **CRAFT** on the front panel. This connection provides both local and remote configuration.
3	Press **Enter** repeatedly on the keyboard until the **LOGIN** menu appears. Enter your password.
4	When the terminal menu opens, navigate the following path: ATLAS 550 **/ SYSTEM CONFIG / ETHERNET PORT / IP ADDRESS**
5	Key in the entire IP address, and then press **Enter**.

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

USING TELNET

To connect to the ATLAS 550 via Telnet, you must define the IP address, set the subnet mask, and, typically, set the default gateway IP address.

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

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

Starting a Telnet Session

When you begin the Telnet session, you will be prompted for a password. The default password is *password* (which is a Level 0 superuser password). You can change this password using the **ACCESS PASSWORDS** option, which is only accessible through the terminal menus. See *Access Passwords* on page 6-15 for details. The Telnet session will time out and display the Login prompt after a predefined time that is set in the **SESSION TIMEOUT** option (see *Session Timeout* on page 6-9 for details).

Use the **MAX TELNET SESSIONS** *option to define the number of Telnet sessions that can be active at one time (see Max Telnet Sessions on page 6-9 for details).*

Microsoft Telnet version 1.0 does not implement full VT-100 emulation. However, many commercial Telnet clients for Microsoft Windows exist which fully implement VT-100. In addition, a freeware client, recommended for optimum performance, comes with the ATLAS 550. See VT-100 Utility on page 14-8 for details.

Chapter 4 Using the Front Panel

OVERVIEW

The front panel contains the Alarm Cut-off (ACO) switch, the CRAFT port, and the controller and module status LEDs. The LEDs provide visual information about the ATLAS 550 Base Unit and any option module that may be installed. Figure 4-1 identifies the ACO switch, the CRAFT port, and the LEDs.

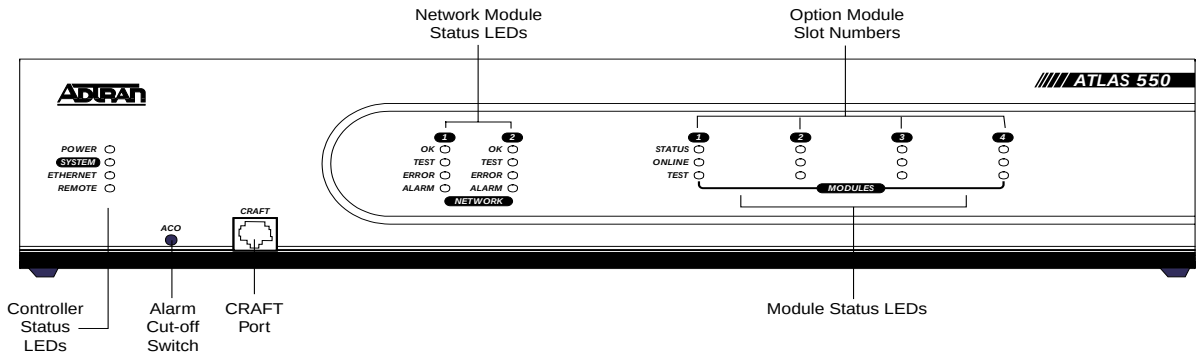


Figure 4-1. ATLAS 550 Front Panel Layout

ACO SWITCH

The ACO switch deactivates (clears) the Alarm Relay, located on the rear panel of the ATLAS 550, after an alarm condition has occurred. If an alarm condition is corrected and then reoccurs, the Alarm Relay will re-energize (see also *ACO Switch* in Table 4-2 on page 4-3).

CRAFT PORT

Use the CRAFT port to configure the system via an EIA-232 connection. The CRAFT port provides the same functions and operations as the Control In port located on the rear panel of the ATLAS 550. The connector type is shown below, and Table 4-1 gives the CRAFT port pinout (see also *CRAFT Port* on page 4-3 in Table 4-2).

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

Table 4-1. CRAFT Port Pinout

PIN	NAME	DESCRIPTION
1	GND	Ground - connected to unit chassis
2	RTS	Request to send - flow control
3	RXDATA	Data received by the ATLAS 550
4	DTR	Data terminal ready
5	TXDATA	Data transmitted by the ATLAS 550
6	CD	Carrier detect
7	UNUSED	—
8	CTS	Clear to send - flow control

FRONT PANEL LEDS

With the ATLAS 550 powered-up, the front panel LEDs provide visual information about the status of the ATLAS 550 and any option modules that may be installed. Table 4-2 on page 4-3 provides a brief description of the front panel features, and Table 4-3 on page 4-4 provides detailed information about the LEDs.

Table 4-2. ATLAS 550 Front Panel Description

Feature	Description
Controller Status LEDs	Displays the general status of the entire ATLAS 550. (See also Table 4-3 on page 4-4.)
Power	Indicates the unit is on or off.
System	Indicates the status of the system.
Ethernet	Indicates the status of the ethernet port.
Remote	Indicates whether a user is logged into the unit.
Network Module LEDs	Displays the status of the network interface. (See also Table 4-3.) All LEDs are off if no network module is installed.
OK	Indicates that the network interface is operating correctly.
Test	Indicates that the network interface is in a test mode.
Error	Blinks to indicate the occurrence of error events.
Alarm	Indicates an alarm condition on the network interface.
Option Module LEDs	Displays by row the operational condition of each module installed in the option slots. (See also Table 4-3 on page 4-4.) All LEDs will be off if no option module is installed.
Status	Indicates the operational condition of modules installed in the option slots.
Online	Indicates whether the module is available for use or is currently in use. If the module is manually taken offline, this LED is turned off.
Test	Indicates that one or more ports within a module are in test.
ACO Switch	Clears the Alarm Relay connection located on the rear panel of the ATLAS 550.
CRAFT Port	Allows the ATLAS 550 to connect to a computer or modem using the CRAFT port (an EIA-232 port).

Table 4-3. ATLAS 550 LEDs

For these LEDs...	This color light...	Indicates that...
Power	Green	The unit is on.
	Off	The unit is off.
Ethernet	Green (solid)	Physical link is up.
	Green (flashing)	Indicates activity on the LAN.
	Off	Physical link is down - no Ethernet connection.
Remote	Yellow	Indicates a user is logged in the system via Control/ Craft port or via Ethernet.
	Off	No one is logged into the system.
System	Green (solid)	No diagnosed system faults were found.
	Green (fast blink)	Flash download is in progress.
	Yellow (solid)	A fault was diagnosed, but the condition no longer exists. The condition will be recorded in the system log.
	Red (solid)	An error condition with either the power supply or the temperature is present.
	Red (fast blink)	A fatal error occurred during flash download.
	Off	Power is not currently supplied to the system.
Network Module Status	OK (green)	The network interface is operating normally with error-free operation. If the interface experiences alarms, the **OK** LED remains off.
	Test (yellow)	The interface 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 the module ports.
	Error (flashing red)	Indicates an error such as BPV (bipolar violation), OOF (out of frame), or CRC (cyclic redundancy check).
	Alarm (red)	An alarm condition has been detected. When the alarm condition is no longer valid, the **OK** LED illuminates. To view an alarm condition, select the active alarm menu item. If the alarm conditions have been corrected, you can view the alarm which caused the activation of the **ALARM** LED in the system log.

Table 4-3. ATLAS 550 LEDs (Continued)

For these LEDs...	This color light...	Indicates that...
Module Status	Green (solid)	One or both modules (in the case of a Resource Module) are OK.
	Green (fast blink)	• One or both modules (in the case of a Resource Module) have been set offline by the user. • One or both modules (in the case of a Resource Module) have invalid flash memory.
	Green (slow blink)	One module has been set offline or has invalid flash memory.
	Red (solid)	One module failed its selftest.
	Red (fast blink)	One module has no response, has been removed, or is not supported.
	Red (slow blink)	One module is not ready.
	Off	No module occupies the slot.
Module Online	Green (solid)	One or both modules (in the case of a Resource Module) have an active connection.
	Green (fast blink)	One module has invalid flash memory or is downloading firmware.
	Green (slow blink)	Only one module has an active connection.
Module Test	Yellow (solid)	One module is in a test mode.

Chapter 5 Navigating the Terminal Menus

TERMINAL MENUS WINDOW

The ATLAS 550 uses a multilevel menu structure that contains both menu items and data fields. All menu items and data fields display in the terminal menu window, through which you have complete control of the ATLAS 550 (see Figure 5-1).

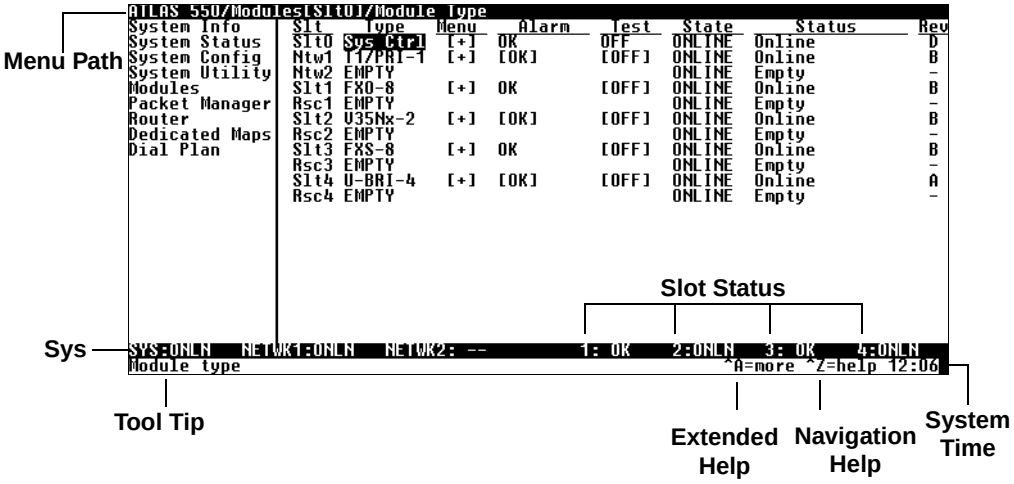


Figure 5-1. Top-level Terminal Menu Window

Viewing the Menus

You can view the terminal menu in two ways: with fields and submenus displaying horizontally across the right pane or with fields and submenus displaying vertically down the right pane. Viewing submenus vertically rather than horizontally allows you to see information at a glance rather than scrolling horizontally across the window. To change the view, move your cursor to an index number and press **Enter**. To view information about other modules, move the cursor up and down over the list of modules. Figure 5-2 on page 5-2 shows the two views for the **MODULES** menu.

Field and submenu names may vary slightly in the two views.

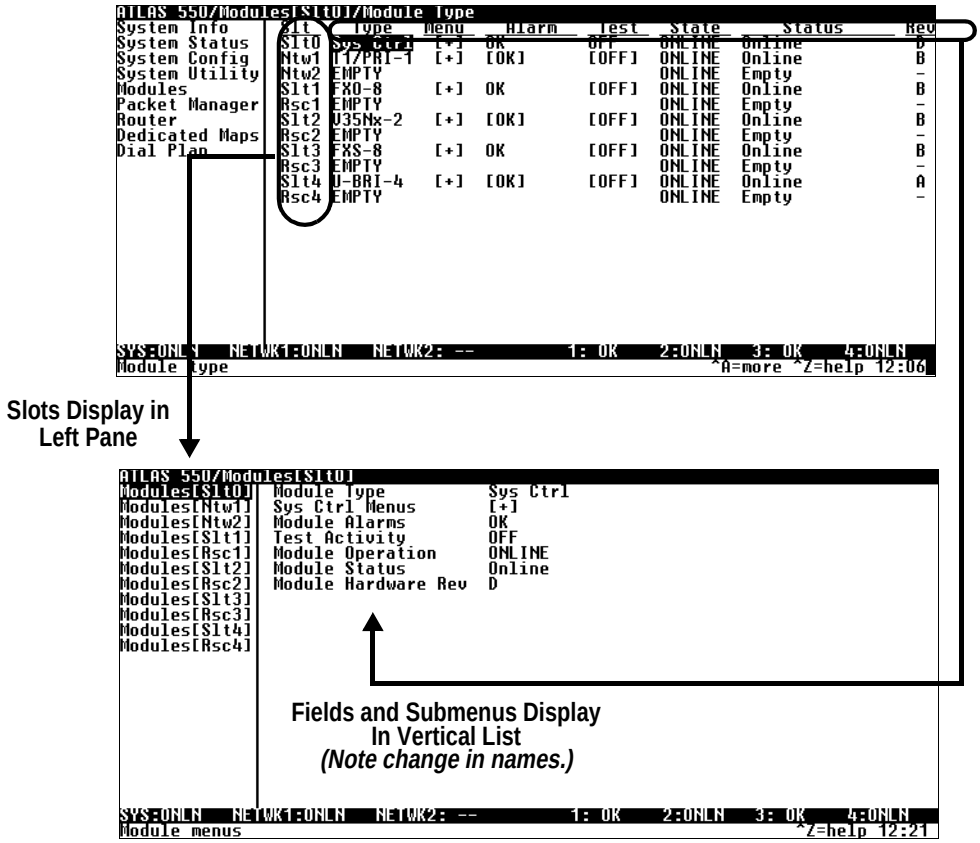


Figure 5-2. Two Views of the Same Menu

Menu Path

The top line of the terminal menu window, the menu path, shows the session's current position (path) in the menu structure. For example, in Figure 5-1 on page 5-1 the cursor is on the **SLOT 0 MODULE TYPE** field of the **MODULES** menu; therefore, the menu path reads **ATLAS 550/MODULES[SLOT0]/MODULE TYPE**.

Window Panes

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

Window Pane Navigation

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

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

Right Window Pane Notation

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

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

Additional Terminal Menu Window Features

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

Sys

Describes the status of the ATLAS 550 base unit.

Tool Tip

Provides a brief description of the currently selected (highlighted) field.

Slot Status

Displays status information, such as OK, WARN (warning), or ALRM (alarm), about slots 1 through 4.

Extended Help

(**Ctrl-A**) Displays information about selected commands (see Figure 5-3).

```
Help: QRSS/Remote Results
This field displays current status of T1 tests.  This includes
information regarding loopbacks and test patterns.

When displaying test pattern status, the display string is
composed of the following fields:
    Pattern sync status
        NONE -- No sync
        LOS  -- Sync has been lost
        SYNC -- Pattern sync'ed
    Errored second count
        ES   -- number of seconds with at least one bit error
```

Figure 5-3. Sample Extended Help Window

Navigation Help

(**Ctrl-Z**) Lists characters used for navigating the terminal menu (see Figure 5-4). See also the section, *Moving through the Menus* on page 5-5.

```
Help
      NAVIGATION                          SESSION MANAGEMENT
Return to home screen.......H       Logout.....................^L
Jump to alternate page......J       Secure.....................^S
Select..............Arrow Keys       Refresh display............^R
Edit/Descend.............Enter
Cancel Edit.............Escape             CONFIGURATION
Left/Right Pane...........Tab       Factory default selection..F
Page Up.....................A       Copy selected item.........C
Page Down...................Z       Paste from clipboard.......P
Ascend..............Backspace       Paste incremented value....>
                                    Paste decremented value....<
                                    Insert new list item.......I
                                    Delete list item...........D
```

Figure 5-4. Navigation Help Window

System Time

Displays the current time. See *Current Time/Date (24h)* on page 6-3 for details on editing the time.

NAVIGATING USING THE KEYBOARD KEYS

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

Moving through the Menus

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

Session Management Keystrokes

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

Configuration Keystrokes

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

Getting Help

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

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

Chapter 6 System Control Terminal Menus

OVERVIEW

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

To do this...	Go to this menu...
Review and monitor general system information for the ATLAS 550.	*System Info* on page 6-2.
Review and monitor system status for the ATLAS 550.	*System Status* on page 6-3.
Set up the operational configuration for the ATLAS 550.	*System Config* on page 6-8.
Update settings, transfer files, perform system diagnostics, and reboot the ATLAS 550.	*System Utility* on page 6-17.
Review and configure settings for each installed module, including the ATLAS 550 Base Unit.	*Modules* on page 7-1.
Define and configure all layer 2 connections including Frame Relay endpoints.	*Packet Manager* on page 8-1.
Define, configure, and monitor all ATLAS 550 Router functions.	*Router* on page 9-1.
Assign dedicated connections between any two ports in the ATLAS 550.	*Dedicated Maps* on page 10-1.
Set global ATLAS 550 switch parameters or set individual parameters for each port in ATLAS 550 that handles a switched call.	*Dial Plan* on page 11-1.

SECURITY LEVELS

To edit terminal menu items, you must have a password and the appropriate security level. Table 6-1 describes the six security levels. See *Access Passwords* on page 6-15 for additional information on working with passwords.

Table 6-1. Password Security Levels

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

SYSTEM INFO

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

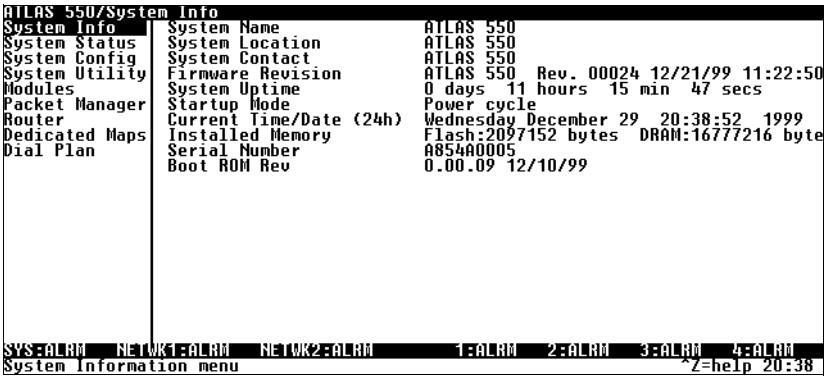


Figure 6-1. System Information Menu

SYSTEM NAME

Write security: 3; Read security: 5
Provides a user-configurable text string for the name of the ATLAS 550. 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 550. 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).

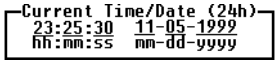
SYSTEM CONTACT Write security: 3; Read security: 5
Provides a user-configurable text string for a contact name. You can use this field to enter the name, phone number, or email address of a person responsible for the ATLAS 550 system. You can enter up to 40 alpha-numeric characters in this field, including spaces and special characters (such as an underbar).

FIRMWARE REVISION Read security: 5
Displays the current firmware revision level of the controller.

SYSTEM UPTIME Read security: 5
Displays the length of time the ATLAS 550 system has been running. Each time you reset the system, this value resets to 0 days, 0 hours, 0 minutes and 0 seconds.

STARTUP MODE Read security: 5
Displays details about the last system startup.

CURRENT TIME/DATE (24H) Write security: 3; Read security: 5
Displays the current date and time, including seconds. To edit this field, place the cursor on the field and press **Enter**. Then, enter the time in a 24-hour format (such as 23:25:30 for 11:00 pm, 25 minutes and 30 seconds), and the date in mm-dd-yyyy format (for example, 11-05-1999). Press **Enter** when you are finished.



INSTALLED MEMORY Read security: 5
Displays the type and amount of memory in use (including Flash memory and DRAM).

SERIAL NUMBER Read security: 5
Displays the serial number for the unit. The serial number of the ATLAS 550 will automatically display in this field.

BOOT ROM REV Read security: 5
Displays the boot ROM revision.

SYSTEM STATUS

The **SYSTEM STATUS** menu provides information on the status of the unit. Figure 6-2 on page 6-4 shows the submenu functions available in the **SYSTEM STATUS** menu.

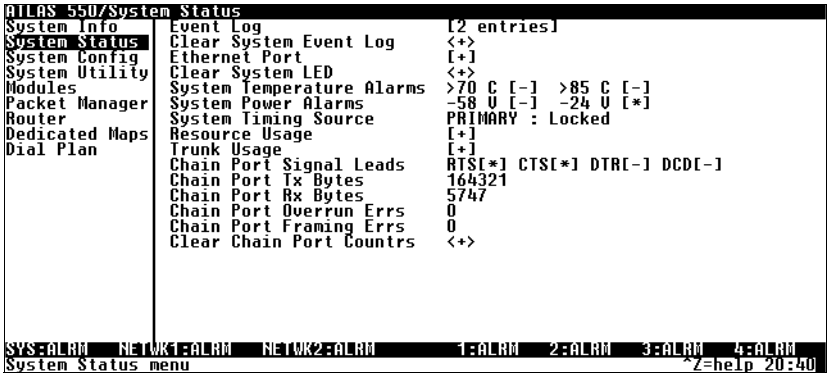


Figure 6-2. System Status Menu

EVENT LOG

Read security: 5

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

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

CAT Category (**CAT**) 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 **EVENT LOGGING** option. See *Event Logging* on page 6-14 for details.

SRC Displays the type of event.

SLOT Displays the slot number in which the event occurred. If this field displays a dash (-), the event occurred in the ATLA S550 base unit.

PORT Displays the port in which the event occurred.

EVENT DESCRIPTION Displays a description of the event.

CLEAR SYSTEM EVENT LOG

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

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

ETHERNET PORT

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

I/F STATUS	Indicates the current status of the Ethernet port.
TX FRAMES	Indicates the number of frames transmitted from the Ethernet port since system startup.
RX FRAMES	Indicates the number of frames received on the Ethernet port since system startup.
ETHERNET RATE	Indicates the data rate on the Ethernet port.

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 550 detects a major system failure. If the failure condition clears, the LED turns yellow and remains yellow to warn of the past failure.

SYSTEM TEMPERATURE ALARMS

Read security: 5
Indicates that the internal temperature of the unit has exceeded normal operating limits. The two thresholds indicate that the internal temperature is greater than 70° C and/or greater than 85° C. If one of these thresholds is exceeded, a warning will be placed in the Event Log but no other action will be taken.

```
>70 C [-]  >85 C [-]
```

SYSTEM POWER ALARMS

Read security: 5
Indicates that the -58 V and/or -24 V power supplies are not functional. These power supplies are continuously monitored to determine failures. If one of these supplies fails, a message will be placed in the **EVENT LOG** (see also *Event Log* on page 6-4).

```
-58 V [-]  -24 V [*]
```

SYSTEM TIMING SOURCE

Read security: 5
Indicates which timing source (primary or backup) is currently being used by ATLAS 550 and if ATLAS 550 is locked onto this source. If the display does not indicate locked, the ATLAS 550 does not have a valid source of timing and cannot reliably transfer data. Review the current setting for system timing source in the **SYSTEM CONFIG** menu. See *Primary Timing Source* on page 6-8 and *Backup Timing Source* on page 6-8 for details.

RESOURCE USAGE

Read security: 5
Indicates resource use (**ANALOG**, **NAILED DIGITAL**, **PACKET VOICE**, **SWITCHED DIGITAL**). Data displayed in this table is dependent on the Atlas 550 configuration.

One HDLC resource is used by each PRI or each Packet Endpoint.

DATA TABLES

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

RESOURCE TYPE
Displays the system resources list.

CURRENT
Shows the number of resources available (not in use) and the total number of resources. If a resource is taken offline, 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.

HOURLY DATA
Shows availability information by hour for a 24-hour period.

RESET
Write security: 4; Read security: 5
Activates the reset of all accumulated availability statistics.

CONFIGURATION

Configures the statistics displayed under data tables.

DISPLAY FORMT
Selects the statistics display format—**RAW DATA** or **%**.

RESET MODE
Write security: 4; Read security: 5
Selects the mode for resetting statistics—**MANUAL**, **DAILY**, or **WEEKLY**.

TRUNK USAGE

Read security: 5
Indicates trunk use:
(**NET TERM PRI, NET TERM RBS; USER TERM PRI, USER TERM RBS**).

DATA TABLES

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

TRUNK TYPE	Displays the system trunk list.
CURRENT	Shows the number of trunks available (not in use) and the total number of trunks. If a trunk is taken offline, it is not included in the total.
AVERAGE	Shows the average number of trunks available since the statistics were last reset.
MINIMUM	Shows the fewest number of trunks available since the last reset.
0 (ZERO) AVAILABLE	Provides a count of the number of times the quantity of available trunks reached 0.
SLT/PRT	Displays data tables for a specific port.
RESET	Write security: 4, Read security: 5 Resets all accumulated availability statistics.

CONFIGURATION

Configures the statistics displayed under data tables.

DISPLAY FORMT	Selects the statistics display format—**RAW DATA** or **%**.
RESET MODE	Write security: 4; Read security: 5 Selects the mode for resetting statistics—**MANUAL**, **DAILY**, or **WEEKLY**.

CHAIN PORT SIGNAL LEADS

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

RTS	Request to send.
CTS	Clear to send.
DTR	Data terminal ready.
DCD	Data carrier detect.

CHAIN PORT TX BYTES

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

CHAIN PORT RX BYTES
Read security: 5
Displays the number of received data bytes.

CHAIN PORT OVERRUN ERRS
Read security: 5
Displays the number of overrun errors.

CHAIN PORT FRAMING ERRS
Read security: 5
Displays the number of received framing errors.

CLEAR CHAIN PORT COUNTRS
Clears all chain port counters. Press **Y** to activate this command.

SYSTEM CONFIG

The **SYSTEM CONFIG** menu allows you to set up the ATLAS 550 operational configuration. Figure 6-3 shows the items included in this menu.

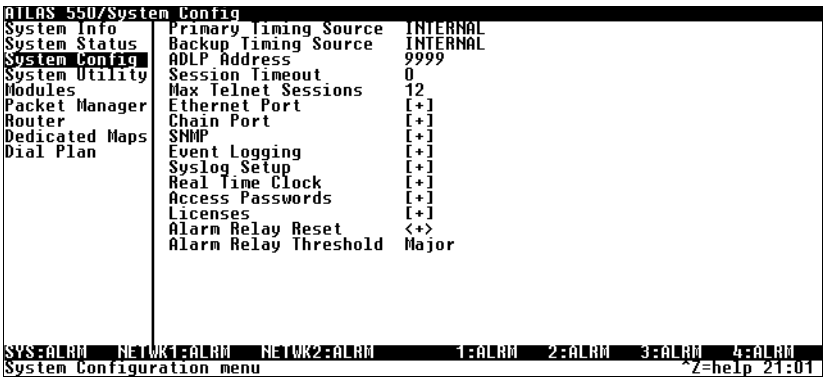
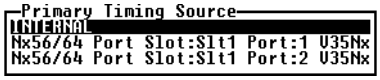


Figure 6-3. System Configuration Menu

PRIMARY TIMING SOURCE
Write security: 3; Read security: 5
Selects the primary timing source. 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 550 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. The allowable range is between 2 and 65520. Enter a value not used by any other ADTRAN 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 outTelnet 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 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 550 IP address to determine which nodes must be reached through the default IP gateway.

MAC ADDRESS

Displays the system Ethernet Media Access Control (MAC) address. This field is read-only.

ETHERNET SPEED — Write security: 3; Read security:5
Defines the data rate on the Ethernet interface. Choose from **10 MBPS** or **AUTO 10/100**. When the unit is set for **AUTO 10/100** the ATLAS 550 auto detects the data rate of the LAN and set itself to that rate, either **10 MBPS** or **100 MBPS**.

CHAIN PORT

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

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

PORT TYPE — Write security: 2; Read security: 5
Specifies whether you use **DIRECT** or **DIAL** mode.

PORT SPEED — Write security: 2; Read security: 5
Specifies the baud rate of the port. Select either 2400, 9600, 19200, or 38400. If you are using **DIAL** for **PORT TYPE**, ensure that the **PORT SPEED** setting matches the modem baud rate.

MODEM INITIALIZATION STRING — Write security: 2; Read security: 5
Specifies the initialization string for a modem. Refer to your modem documentation for acceptable initialization strings.

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

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

SNMP

Write security: 3; Read security: 5
Provides a way to configure SNMP access for the ATLAS 550. For detailed information on SNMP, refer to *SNMP Management* on page 13-1. The following options are available for review and editing:

SNMP ACCESS — Write security: 3; Read security: 5
Defines whether SNMP access to the ATLAS 550 is enabled or disabled. Select the appropriate option.

SNMP COMMUNITIES

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

IP ADDRESS
Specifies the IP address of the network manager.

PRIVILEGES
Defines **GET** (read-only) and **GET/SET** (read and write) privileges.

GET NAME
Defines the community name for **GET** access. This value must match the **GET** name defined on the network management station. **PUBLIC** is the default name.

SET NAME
Defines the community name for **SET** access. This value must match either the **GET** or **SET** name defined on the network management station. **PUBLIC** is the default name.

TRAP TRANSMISSION

Write security: 2; 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

Read security: 5
Defines the destination for SNMP traps as follows:

IP ADDRESS
Write security: 3; Read security: 5
Identifies the IP address to which the network manager sends traps.

COMMUNITY
Write security: 3; Read security: 5
Defines the community name for trap destinations. This name must match the community name defined at the network management station.

TRAP FILTERING
Write security: 2; Read security: 5
Sets the minimum severity level required for a system event to generate an SNMP trap. If a trap event occurs and if the trap's severity level is equal to or more severe than the trap type's current threshold setting, that event is sent as an SNMP trap. (Refer to the ATLAS 550 MIB for a listing of all traps and their severity levels.) You can set the following threshold levels for the available selections: **DISABLED, CRITICAL, MAJOR, MINOR, WARNING, NORMAL**, and **INFO**.

STATION TYPE
Write security: 3; Read security: 5
To deliver the SNMP trap packet with the **COMMUNITY NAME** unchanged, define the **STATION TYPE** as **NORMAL**. If you are using T-Watch PRO, define

the **STATION TYPE** as **T-WATCH MGMT** and append the **COMMUNITY NAME** with ".ADLP ADDRESS." Within the SNMP trap packet, this field is automatically updated before it is sent to the management station.

DS1 CURRENT PERF THRESHOLDS

Write security: 2; Read security: 5
Defines performance threshold values for DS1 Line and Path statistics recorded in a 15-minute interval. If a statistic value exceeds its threshold value, then the corresponding Alert Trap will be sent if the alert event is armed and Alert Traps are enabled. These thresholds apply to all DS1 interfaces in the system.

CURRENT ES THRSH

The DS1 performance monitor Threshold Value for the Current 15 minute Errored Seconds (ES) parameter. The default value is 65 for an approximate BER level of 10E-5.

CURRENT SES THRSH

The DS1 performance monitor Threshold Value for the Current 15 minute Severely Errored Seconds (SES) parameter. The default value is 10 for an approximate BER level of 10E-5.

CURRENT SEFS THRSH

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

CURRENT UAS THRSH

The DS1 performance monitor Threshold Value for the Current 15 minute Unavailable Seconds (UAS) parameter. The default value is 10 for an approximate BER level of 10E-5.

CURRENT CSS THRSH

The DS1 performance monitor Threshold Value for the Current 15 minute Controlled Slip Seconds (CSS) parameter. The default value is 1 for an approximate BER level of 10E-5.

CURRENT PCV THRSH (D4)

The DS1 performance monitor Threshold Value for the Current 15 minute Path Code Violation (PCV) parameter, when the Line Type is Super Frame (AT&T D4 format) DS1. The default value is 72 Framing errors for an approximate BER level of 10E-5.

CURRENT PCV THRSH (ESF)

The DS1 performance monitor Threshold Value for the Current 15 minute Path Code Violations (PCV) parameter, when the Line Type is Extended Super Frame (ESF) DS1. The default value is 13,296 CRC errors for an approximate BER level of 10E-5.

CURRENT LES THRSH

The DS1 performance monitor Threshold Value for the Current 15 minute Line Errored Seconds (LES) parameter. The default value is 65 for an approximate BER level of 10E-5.

CURRENT LCV THRSH

The DS1 performance monitor Threshold Value for the Current 15 minute Line Code Violations (LCV) parameter. The default value is 13,340 for an approximate BER level of 10E-5.

DS1 TOTAL CURRENT PERF THRESHOLD

Write security: 2; Read security: 5

Defines performance threshold values for DS1 Line and Path statistics. If a statistic value exceeds its threshold value, then the corresponding Alert Trap will be sent if the alert event is armed and Alert Taps are enabled. These threshold values apply to all DS1 interfaces in the system.

TOTAL ES THRSH

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

TOTAL SES THRSH

The DS1 performance monitor Threshold Value for the Total Severely Errored Seconds (SES) parameter. The default value is 100 for an approximate BER level of 10E-5.

TOTAL SEFS THRSH

The DS1 performance monitor Threshold Value for the Total Severely Errored Framing Seconds (SEFS) parameter. The default value is 17 for an approximate BER level of 10E-5.

TOTAL UAS THRSH

The DS1 performance monitor Threshold Value for the Total Unavailable Seconds (UAS) parameter. The default value is 10 for an approximate BER level of 10E-5.

TOTAL CSS THRSH

The DS1 performance monitor Threshold Value for the Total Controlled Slip Seconds (SES) parameter. The default value is 4 for an approximate BER level of 10E-5.

TOTAL PCV THRSH (D4)

The DS1 performance monitor Threshold Value for the Total Path Code Violations (PCV) parameter, when the Line Type is Super Frame (AT&T D4 format) DS1. The default value is 691 Framing Errors for an approximate BER level of 10E-5.

TOTAL PCV THRSH (ESF)

The DS1 performance monitor Threshold Value for the Total Path Code Violations (PCV) parameter, when the Line Type is Extended Super Frame (ESF) DS1. The default value is 132,960 CRC errors for an approximate BER level of 10E-5.

TOTAL LES THRSH

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

TOTAL LCV THRSH

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

EVENT LOGGING

Write security: 3; Read security: 5

Sets the system event severity level threshold for each of the ATLAS 550 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 550 Syslog client for use with a Syslog server (supplied on ADTRAN / Utility disk or available on most UNIX platforms).

TRANSMISSION

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

HOST IP ADDRESS

Lists the IP address of the external server that is running the Syslog host daemon.

HOST FACILITY

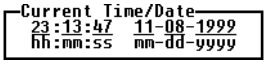
Specifies the facility destination of log events. Facilities are located on the host and are managed by the Syslog host daemon running on either a UNIX machine or a PC.

REAL TIME CLOCK

Write security: 3; Read security: 5

Provides access to the following two options that you can review and edit:

CURRENT TIME/ DATE



Displays the current date and time, including seconds. To edit this field, enter the time in 24-hour format (such as 23:13:47 for 11 pm, 13 minutes and 47 seconds), and enter the date in mm-dd-yyyy format (for example, 11-08-1999).

AUTO DAYLIGHT SAVINGS

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

ACCESS PASSWORDS

Write security: 0; Read security: 5
Provides a way to edit passwords and, also, to add new users and passwords. All menu items are protected by passwords of varying security levels. By assigning different passwords to different security levels, the ATLAS 550 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. Table 6-1 on page 6-2 describes each of the six password security levels.

Passwords are case-sensitive.

Instructions for Adding/Deleting Passwords

Figure 6-4 shows the menu for adding and deleting passwords. The instructions follow.

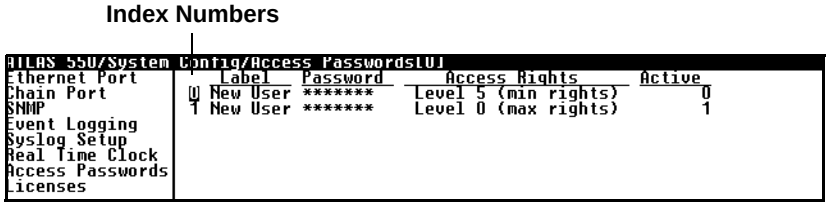
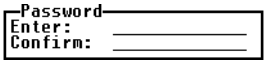


Figure 6-4. Menu for Adding/Deleting Passwords

Adding New Passwords

1. To add a new password, position the cursor over the index number 0 and press I.
2. Enter and confirm the new password.



3. Assign access rights (see also Table 6-1 on page 6-2).

Deleting Passwords

To delete a password, position the cursor over the index number of the password to be deleted and press **D**.

> **NOTE** *If you lose or forget the ATLAS 550 system administrator password, contact ADTRAN technical support (see last page of this manual) for help in resetting the password.*

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

PASSWORD Write security: 0; Read security: 5
Allows you to change the password (the default password is **password**). The current password displays as a series of asterisks (********). The password can contain up to 12 alphanumeric characters. You can also use spaces and special characters in the password. Remember, passwords are case-sensitive.

Instructions for Changing Passwords

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.

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

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

LICENSES

Write security: 0; Read security: 0
Provides menus to enable the optional ATLAS 550 feature upgrades.

FEATURE Names the ATLAS 550 feature upgrade.

LICENSE KEY Displays the license key of the feature upgrade.

SERIAL NUMBER Displays the serial number of the feature upgrade.

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

STATUS Reflects the status, Permanent or Temporary, of the feature upgrade license key.

ALARM RELAY RESET Write security: 3; Read security: 5
Clears the Alarm Relay located on the rear panel of the ATLAS 550.

ALARM RELAY THRESHOLD Write security: 3; Read security: 5
Defines which threshold sets the Alarm Relay. If an alarm occurs that is greater than or equal to the threshold selected, the Alarm Relay will set. These thresholds include, in descending order of importance, **CRITICAL**, **MAJOR**, **MINOR**, **WARNING**, and **NORMAL**. As an example, if the threshold is set for **MAJOR**, then ALL Major alarms and ALL critical alarms will set the Alarm Relay. However, setting the threshold to **NORMAL** will not set the Alarm Relay for Normal events. No Normal events set the Alarm Relay.

SYSTEM UTILITY

Use the **SYSTEM UTILITY** menu to view and set the system parameters shown in Figure 6-5 .

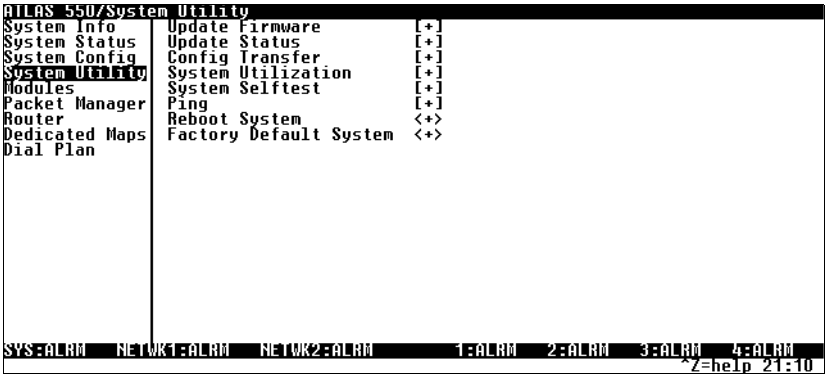


Figure 6-5. System Utility Menu

UPDATE FIRMWARE Write security: 1; Read security: 5
Updates firmware when ATLAS 550 enhancements are released. Two transfer methods are available for use in updating any modules that contain Flash memory—including the ATLAS 550 system controller.

The first transfer method uses the ATLA S550 serial Control / Chain In port of the system controller and XMODEM protocol. For detailed information on how to update firmware using this method, see *XMODEM Firmware Updates* on page 12-1.

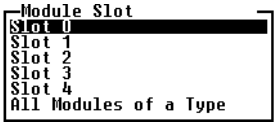
The second transfer method uses the ATLAS 550 built-in Ethernet port of the system controller and TFTP (Trivial File Transfer Protocol). For detailed information on how to update firmware using this method, see *TFTP Firmware Updates* on page 12-3.

> **NOTE** *The available update options vary depending on whether you select* **SLOT 0**, **SLOTS 1** *through* **4**, **RESOURCE 1***through* **4** *or* **ALL MODULES OF A TYPE**.

MODULE SLOT

Write security: 1; Read security: 5

Displays the slot you select for firmware updating. When this option first appears, **None Selected** displays. When you move the cursor to this field and press **Enter**, a dialog box opens, allowing you to select **SLOT 0** through **SLOT 4**, **RESOURCE 1** through **4** or **ALL MODULES OF A TYPE.**



ALL MODULES OF A TYPE is useful if several identical modules are installed in the ATLAS 550.

MODULE TYPE

Write security: 1; Read security: 5

Reflects the module type selected in **MODULE SLOT**. This is normally a read-only field; however, if you selected **ALL MODULES OF A TYPE**, you must select a particular module type to update all modules of that type. The selections only include upgradable modules.

TRANSFER METHOD

Write security: 1; Read security: 5

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

TFTP SERVER IP ADDRESS

Write security: 1; Read security: 5

Configures the IP address of the TFTP Server on which the update file resides. ATLAS 550 uses this field to locate the network server on which the update file resides.

TFTP SERVER FILENAME

Write security: 1; Read security: 5

Identifies the name of the update file to retrieve from the TFTP Server. Enter the full path name and filename for the file.

RESTART SCHEDULE

Write security: 1; Read security: 5

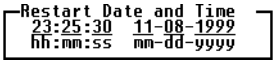
Indicates when to restart the updated module to invoke the new code, after selecting a module slot. The two options include **RESTART IMMEDIATELY AFTER UPDATE** and **RESTART AT SPECIFIED DATE AND TIME**.

RESTART IMMEDIATELY AFTER UPDATE

Automatically restarts the module immediately after the update is complete.

RESTART AT SPECIFIED DATE AND TIME
Lets you specify a date and time to automatically restart the updated module. (When you select this option, a new field called **RESTART DATE AND TIME** displays below the current field.)

RESTART DATE AND TIME
Write security: 1; Read security: 5



Defines the date and time to restart the system. Enter the time using a 24-hour format (i.e., 23:25:30 for 11 PM, 25 minutes, 30 seconds). Enter the date in mm-dd-yyyy format (i.e., 11-08-1999).

> **NOTE** **RESTART AT SPECIFIED DATE AND TIME** *is only available for the System Controller— not for modules residing in expansion slots, since they are unable to maintain normal operation during the update process.*

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

If you are updating several modules at the same time (if **MODULE SLOT** is set to **ALL MODULES OF A TYPE**), this option displays **[+]**, indicating this field contains submenu items. The following submenus display:

SLT	Indicates the slot number.
TYPE	Defines the type of module for each slot.
CURRENT STATUS	Indicates the status of the current update.
PREVIOUS STATUS	Indicates the status of the previous update.
PREVIOUS TIME	Indicates the time of the previous update.

During the TFTP upload process, various status messages are provided in **CURRENT UPDATE STATUS** (see Table 12-1 on page 12-5).

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

BEGIN FIRMWARE UPDATE

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

UPDATE STATUS

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

CONFIG TRANSFER

Write security: 3; Read security: 5
Used only with TFTP transfers. Sends a file containing the ATLAS 550 configuration to a file on a TFTP Server using the TFTP protocol through the Ethernet port. **CONFIG TRANSFER** also lets you save the ATLAS 550 configuration as a backup file, so you can use the same configuration with multiple ATLAS 550 units. In addition, **CONFIG TRANSFER** can retrieve a configuration file from a TFTP Server.

To support these transfers, ADTRAN delivers a TFTP program with ATLAS 550 called *TFTP Server*. You can configure any PC running Microsoft Windows with this software, and store a configuration file. See *TFTP Server Utility* on page 14-10 for details on how to use *TFTP Server*.

Before using **CONFIG TRANSFER**, *the ATLAS 550 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 550 unit's transferred configuration; this way, identical configurations can be sent to multiple units.

TRANSFER METHOD

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

TFTP SERVER IP ADDRESS

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

TFTP SERVER FILENAME

Write security: 3; Read security: 5
Defines the name of the configuration file that you transfer to or retrieve from the TFTP Server. The default name is **Atlas550.cfg**, but you can edit this name.

CURRENT TRANSFER STATUS

Read security: 5
Indicates the current status of the update.

PREVIOUS TRANSFER STATUS

Read security: 5
Indicates the status of the previous update.

LOAD AND USE CONFIG

Write security: 3; Read security: 5
Retrieves the configuration file specified in the **TFTP Server Filename** field from the server. To start this command, enter **Y** to begin or enter **N** to cancel.

If you execute **LOAD AND USE CONFIG**, *the ATLAS 550 retrieves the configuration file, reboots, then restarts using the new configuration.*

SAVE CONFIG REMOTELY

Write security: 3; Read security: 5
Saves the configuration file specified in **TFTP SERVER FILENAME** to the server identified in **TFTP SERVER IP ADDRESS**. To start this command, enter **Y** to begin or enter **N** to cancel.

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

SYSTEM UTILIZATION

Write security: 0; Read security: 0
Displays statistics related to the ATLAS 550 internal operating system. Please check with ADTRAN Technical Support before attempting to use this menu.

SYSTEM SELFTEST

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

Self-tests disrupt data flow.

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

SELECTED TESTS Write security: 3; Read security: 5
Allows the user to select a system-wide test or an individual card test. Choose from **ALL TESTS**, **SLOT:SLT0 SYS CTRL**, or any other installed option / network module.

CURRENT TEST STATUS Read security: 5
Displays which part of **SELFTEST** is currently being run. See *View Selftest Log* on page 6-22 for details on individual tests.

CURRENT SLOT/ PORT Read security: 5
Displays slot and port of the subsystem currently being tested.

VIEW SELFTEST LOG Read security: 5
Displays time-stamped log of the tests conducted and the Pass / Fail results. Self-tests verify data integrity and processor control to each port. Each port is looped back and a data pattern is sent and tested. The result of the self-test on each installed port is listed with Pass / Fail results. Figure 6-6 shows a typical test log.

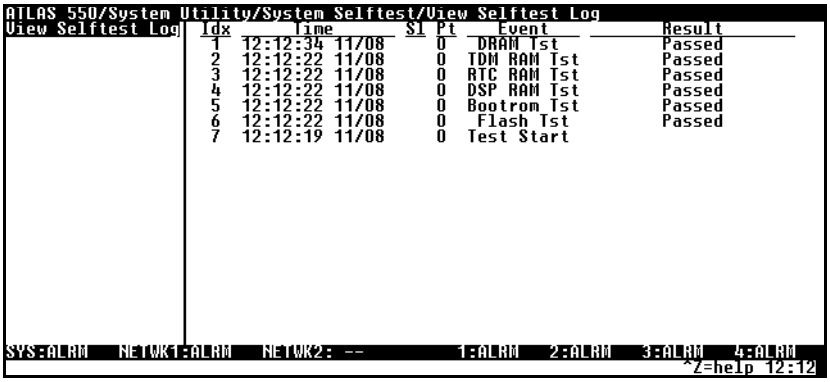


Figure 6-6. View Self-test Log

The self-test log includes the following fields.:

IDX	Index number of the log.
TIME	Time and date of the log entry.
SL	ATLAS 550 slot number.
PT	ATLAS 550 port number.
EVENT	Event description.
RESULT	Shows Pass / Fail results.

Table 6-2 lists the tests associated with the system controller.

Table 6-2. System Controller Tests

This event...	Logs this result...
FLASH	Verifies flash memory checksum.
BOOTROM	Verifies boot ROM checksum.
DSP RAM	Verifies memory associated with the DSP.
RTC RAM	Verifies memory associated with the real time clock.
TDM RAM	Verifies memory associated with mapping TDM bandwidth.
DRAM	Verifies dynamic RAM used for program execution.
HDLC	Verifies each HDLC controller used for frame relay or PRI.

CLEAR SELF-TEST LOG

Write security: 3; Read security: 5
Clears the self-test log.

PING

Write security: 5; Read security: 5
Allows you to send pings (Internet Control Message Protocol (ICMP) requests) to devices accessible via the network.

Only one ping session can be active at a time.

IP ADDRESS

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

COUNT

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

SIZE

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

TIMEOUT

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

ROUND TRIP MIN Read security: 5
Displays the minimum round trip time of the ping request/reply of the current set of pings.

ROUND TRIP AVG Read security: 5
Displays the average round trip time of the ping request/reply of the current set of pings.

ROUND TRIP MAX Read security: 5
Displays the maximum round trip time of the ping request/reply of the current set of pings.

TX STATS Read security: 5
Displays the number of ping requests transmitted (***n*** **TXED**), the number of ping replies received (***n*** **RXED**) and the number of ping requests that were lost (***n*** **LOST**).

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

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

REBOOT SYSTEM Write security: 0; Read security: 0
Reboots the ATLAS 550. When you select this command, the following message displays: ***WARNING** ** *This will reboot the entire system!* Press **Y** to reboot the system, or **N** to exit the command.

FACTORY DEFAULT SYSTEM Write security: 0; Read security: 0
Resets the entire system to the factory default settings.To reset the system, press **Y**; to cancel this command, press **N**.

Chapter 7 Module Terminal Menus

OVERVIEW

The controller board (slot 0) has two network interface slots. This chapter only describes the module options available for the T1/PRI network interface module. Individual option module menus are described in the applicable module manuals.

The ATLAS 550 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 **MODULES** menu and press **Enter**. If you prefer to view these options in a vertical mode, move the cursor to a slot number and press **Enter** on the keyboard.

MODULES

The **MODULES** main menu (see Figure 7-1) provides status information and menu options that allow you to configure and control the installed option modules, as well as the network ports.

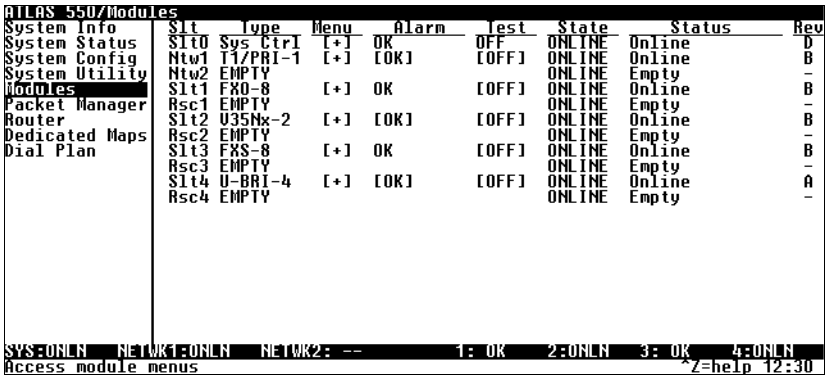


Figure 7-1. Modules Menu

SLT

Read security: 5
Identifies the slot number. Slot 0 refers to the ATLAS 550 Base Unit.

The ATLAS 550 has three types of slots: network slots, option module slots, and resource module slots. The two network slots are designated **NTW1** and **NTW2**. The four option module slots are designated **SLT1** through **4**, and the four resource module slots are designated **RSC1** through **4**.

Resource modules are installed onto any option module, but not onto network modules.

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 550 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 preconfigure 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**.

TYPE *automatically displays the name of an installed module. If you want to preconfigure the slot for a different type of module, you must set this field to* **EMPTY** *before selecting another module type.*

MENU

Displays additional status and configuration menus for the ATLAS 550 or selected module. To access the submenus for this item, use the arrow keys to scroll to the **MENU** column for the module you want to edit, and press **Enter**. For detailed information on each submenu item, see *Modules Menu (T1Network Interface Module)* on page 7-3.

ALARM

Read security: 5
Displays an alarm condition on the ATLAS 550 or selected module. To access this menu, use the arrow keys and move to the **ALARM** menu and then press **Enter**.

TEST

Read security: 5
Displays the type of test the ATLAS 550 or selected module is executing. To initiate a test, select the **MENU/TEST** option and then press **Enter**. You now have access to the screen that allows you to set up and initiate tests. See *Test* on page 7-7 for details.

STATE

Read security: 5
Displays whether the ATLAS 550 or selected 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 field allows an installed mod-

ule to be marked **OFFLINE**, which may be useful in system troubleshooting. If you choose **OFFLINE**, the module will not be in alarm condition, but will display **OFFLINE**.

Once a module is installed, **STATE** *must be set to* **ONLINE** *for the ATLAS 550 to use the module for any data bandwidth.* **ONLINE** *is the default setting.*

STATUS

Read security: 5
Displays status information on the ATLAS 550 ports and other installed modules as follows:

ONLINE	The module is enabled and is responding to the system controller's status polls. This is the normal response of the system.
NO RESPONSE	The module is enabled but is not responding to the system controller's status polls. This response indicates a problem in the system or that the module is not installed.
EMPTY	The system controller has not detected the presence of a module in the system, nor has a module been manually enabled for this option slot.
OFFLINE	The module is installed but has been taken offline by a user. The module is still responding to controller polls.
OFFLINE/NO RESPONSE	The module is installed but has been taken offline by a user. The module is not responding to polls.
NOT SUPPORTED	The module is not supported by the current system configuration.

REV

Read security: 5
Displays the hardware revision of the ATLAS 550 and other installed modules.

Modules Menu (T1Network Interface Module)

This section provides detailed information on the **MODULES** / **MENU** submenus. **MENU** provides access to commands that allow you to review the status of various options, change the configuration for general parameters, and initiate tests. This section *only* describes the menu options for the T1 Network Interface Module. For details on menu options for other modules, refer to the appropriate module manuals.

To configure the T1 Network Interface Module in the Dial Plan, use the descriptions provided for the Dual T1 / PRI Module (see page 11-10).

INFO Read security: 5
Displays general information about the T1/PRI network interface module as follows:

PART NUMBER	Displays the part number of the T1/PRI network interface.
SERIAL NUMBER	Displays the module's serial number.
ASSEMBLY REVISION	Displays the assembly revision.

ALARM STATUS Read security: 5
Displays any active alarms as follows:

PRT	Displays the port number. The T1/PRI Network Interface Module is a single-port device.
ALARMS	Displays the alarm type. Table 7-1 describes each alarm type.

Table 7-1. Alarm Types

LOS	(Loss of Signal) No signal detected on port interface.
RED	(Red Alarm) Not able to frame data received on the port. Alternately referred to as Out of Frame (OOF).
YELLOW	(Yellow Alarm) Remote alarm indicator (RAI) being received on port.
BLUE	(Blue Alarm) Receiving unframed all ones from the port alarm indicator signal (AIS).
DS0 ALARM	At least one DS0 channel is in alarm.
RX LEVEL	(Receive Level) Indicates the strength of the signal received on the port.

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

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

DS0 ALARMS Read security: 5
Indicates DS0 alarm as follows:

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

SIG STATUS Read security: 5
Displays the A/B signaling bits for Rx and Tx DS0s.

PERFORMANCE: CURR Write security: 3; 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 the T1/PRI port as follows:

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

PERFORMANCE: 15 MIN Write security: 3; Read security: 5
In the **PERFORMANCE 15 MIN** menu, the performance data for the previous 15 minute window is stored. Refer to *Performance: Curr* on page 7-5 for a detailed description.

PERFORMANCE: 24 HR Write security: 3; Read security: 5
Stores the performance data for the previous 24-hour window. Refer to *Performance: Curr* on page 7-5 for a detailed description.

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

PRT
Read security: 5
Identifies the port number.

PORT NAME
Write security: 3; Read security: 5
Accepts any alphanumeric name up to 16 characters long to uniquely identify each port.

FRAME
Write security: 2; Read security: 5
Matches the frame format of the circuit to which it is connected (available from the network supplier).

CODE
Write security: 2; Read security: 5
Matches the line code of the circuit to which it is connected (available from the network supplier).

TX YELLOW
Write security: 3; Read security: 5
Enables and disables yellow alarm transmissions.

TX PRMS
Write security: 3; Read security: 5
Enables and disables PRM data transmissions on the facility data link (FDL). The PRM data continues to be collected even if **TX PRMS** is disabled (possible only with ESF format).

LBO
Write security: 2; Read security: 5
Depends on whether the circuit is provisioned for DS1 by the telephone company.

LB 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.

PULSE DENSITY
Write security: 3; Read security: 5
When **ON**, the ATLAS 550 monitors for ones (1s) density violations and inserts a one (1) when needed to maintain ones at 12.5%.

TEST Initiates different types of tests and displays test results.

These **TEST** *commands temporarily disrupt service.*

PRT
Identifies the port number.

LOC LB
Write security: 4; Read security: 5
Causes loopback on near-end port. (Local Loopback)

LINE	Metallic loopback.
PAYLD	Payload loopback framing and clocking are regenerated.

REMOTE LB
Write security: 4; Read security: 5
Sends a loopback code to a remote CSU.

ANSI FDL LINE	Sends ANSI line loopback code. Requires ESF mode.
ANSI FDL PYLD	Sends ANSI payload loopback code. Requires ESF mode.
ATT INBAND LINE	Sends line loopback using inband code.

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	Pseudorandom pattern with suppression of excess zeros

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

CLR
Write security: 3; Read security: 5
(Test Pattern Results Clear) Clears current error counters on test pattern results menu.

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

Chapter 8 Packet Manager

OVERVIEW

The **PACKET MANAGER** menu contains submenus that define packet endpoints. A packet endpoint is a *virtual* port within the ATLAS 550 into which a specified *physical* port (a T1 or an Nx56/64) terminates its data for further routing by the system. All packet services, including the ATLAS 550 frame relay, must have defined packet endpoints.

Your frame relay provider furnishes specific information on defining the packet endpoint. This information includes signaling type (Annex A, Annex D, or LMI) and definitions for all active PVCs. The **PACKET CNCTS** submenu map connects protocols from packet endpoint to packet endpoint.

In addition to defining packet endpoints, you must also configure the physical port before it can run frame relay (see also Chapter 10, *Dedicated Maps* and Chapter 11, *Dial Plan*).

PACKET MANAGER MENUS

The **PACKET MANAGER** menus (see Figure 8-1) define and configure all layer 2 connections, including frame relay endpoints. These submenus, discussed in this chapter, include **PACKET ENDPNTS**, **PACKET CNCTS**, **CNCTS SORT**, and **FRAME RELAY IQ**. See also, the menu tree in Figure 8-2 on page 8-2.

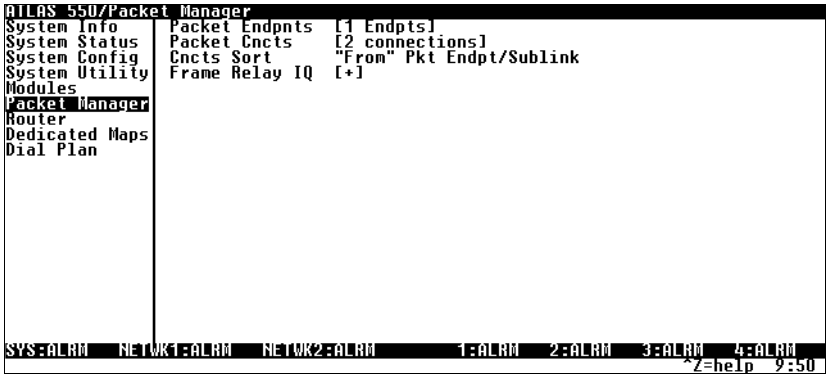


Figure 8-1. Packet Manager Menu

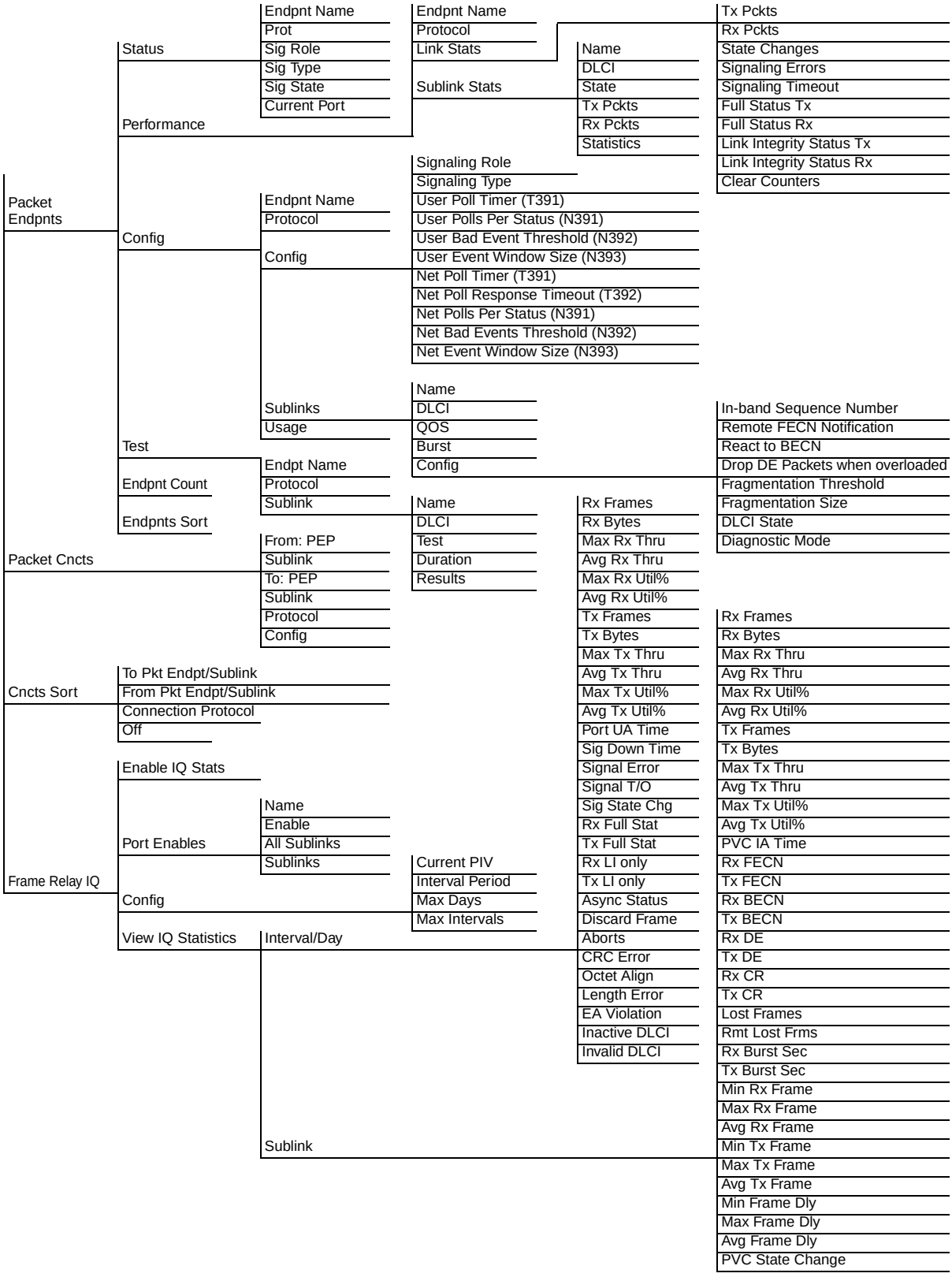


Figure 8-2. Packet Manager Menu Tree

PACKET ENDPNTS

The **PACKET ENDPNTS** menu defines, monitors, and tests a packet endpoint. Submenus include **STATUS**, **PERFORMANCE**, **CONFIG**, **TEST**, **ENDPNT COUNT**, and **ENDPNTS SORT**.

STATUS

STATUS submenus display the status of each packet endpoint including the packet endpoint name (**ENDPNT NAME**), the protocol type (**PROT**), the signaling role (**SIG ROLE**), the signaling type (**SIG TYPE**), the signaling state (**SIG STATE**), and the connections (**CURRENT PORT**). The following sections discuss each of these fields.

ENDPNT NAME

Read Security: 5
Displays the packet endpoint name as defined in the **PACKET ENDPNTS/ CONFIG MENU** (also see *Config* on page 8-6).

PROT

Read Security: 5
Displays the layer 2 protocol that this packet endpoint terminates. **FR** indicates that this packet endpoint is configured for frame relay. **TBOP** indicates that this packet endpoint is configured for Transparent Bit Oriented Protocol (TBOP).

SIG ROLE

Read Security: 5

Displays the frame relay signaling role for this packet endpoint. The selections include **OFF**, **UNKNOWN**, **NETWORK**, **USER**, and **BOTH**.

OFF
Indicates that the endpoint is configured so that it does not use signaling.

UNKNOWN
Indicates that the endpoint is configured to auto-detect the role, but has not yet done so.

NETWORK
Indicates that the endpoint is acting as the network end of a UNI link.

USER
Indicates that the endpoint is acting as one end of a UNI link.

BOTH
Indicates that the endpoint is acting as one end of an NNI link.

SIG TYPE

Read Security: 5
Displays the frame relay signaling type used on this packet endpoint. Selections include **UNKNOWN**, **ANNEX A**, **ANNEX D**, and **LMI**.

UNKNOWN
Indicates that the endpoint is configured to auto-detect the signaling standard to use, but has not yet done so.

ANNEX A
The endpoint is signaling using ITU-T Q.933-A.

ANNEX D
The endpoint is signaling using ANSI T1.617-D.

LMI
The endpoint is signaling using Group of Four LMI specification.

SIG STATE Read Security: 5
Indicates the current condition (i.e., active frame relay signaling) of this packet endpoint, as defined by the frame relay configuration settings. This field is either **ACTIVE** or **INACTIVE**.

CURRENT PORT Read Security: 5
Displays the connections for the packet endpoint. The letter **U** in this field indicates that this packet endpoint is used in the **PACKET CNCTS** map (also see *Packet Cncts* on page 8-13). The remainder of the field indicates the physical port to which this packet endpoint is connected, as defined in the **DEDICATED MAP** (also see *Dedicated Maps* on page 10-1). If the port is a channelized interface such as a T1, the DS0 assignment is also provided.

PERFORMANCE Displays performance information for each packet endpoint including **ENDPNT NAME** (endpoint name), **PROTOCOL**, **LINK STATS**, and **SUBLINK STATS**.

ENDPNT NAME Read Security: 5
Displays the packet endpoint name as defined in **PACKET ENDPNTS/CONFIG** (also see *Config* on page 8-6).

PROTOCOL Read Security: 5
Displays the layer 2 protocol that this packet endpoint terminates as defined in **PACKET ENDPNTS/CONFIG** (also see *Config* on page 8-6).

LINK STATS Read Security: 5
Displays layer 2 performance statistics. This field is dependent on the type of protocol (Frame Relay or TBOP) selected in **PACKET ENDPNTS/CONFIG** (also see *Config* on page 8-6).

Frame Relay Statistics
These fields reflect the total count since last cleared:

TX PACKETS
Total number of frame relay packets transmitted through this packet endpoint, including both user data (on all PVCs) and signaling.

RX PACKETS
Total number of frame relay packets received through this packet endpoint (on all PVCs).

STATE CHANGES
Total number of times that frame relay signaling has gone active or inactive.

SIGNALING ERRORS
Total number of signaling frames received with PVC signaling protocol violations.

SIGNALING TIMEOUTS
Number of times signaling polls were not received in the time specified in T391 in the **PACKET ENDPNTS/CONFIG** menu (also see *Config* on page 8-6).

FULL STATUS TX
Number of full status polls transmitted by this packet endpoint.

FULL STATUS RX
Number of full status polls received by this packet endpoint.

LINK INTEGRITY STATUS TX
Number of link integrity polls transmitted by this packet endpoint.

LINK INTEGRITY STATUS RX
Number of link integrity polls received by this packet endpoint.

CLEAR COUNTERS
Clears all values in this submenu.

TBOP Statistics
These statistics reflect the total count since last cleared:

TX PACKETS
Displays the total number of HDLC packets transmitted through this packet endpoint.

RX PACKETS
Displays the total number of HDLC packets received through this packet endpoint.

CLEAR COUNTERS
Clears all values in this submenu.

SUBLINK STATS Read Security: 5
Displays frame relay performance statistics for supported packet endpoint sublinks. These statistics fields reflect the total count since last cleared.

NAME
User-defined name of a sublink (PVC).

DLCI
DLCI for sublink as defined in **PACKET ENDPNTS/CONFIG** (also see *Config* on page 8-6).

STATE
Indicates if this particular sublink (PVC) has been defined as active by a full status poll.

UP
PVC is up (active).

DOWN
PVC is down (inactive).

TX PCKTS
Total number of frame relay user data packets transmitted over this PVC.

RX PCKTS
Total number of frame relay user data packets received over this PVC.

STATISTICS
Provides additional information, as follows, on the individual sublink:

BECN COUNT
Total number of BECN bits received on this PVC.

DE DISCARD COUNT
Total number of Discard Eligible bits that have been received on this PVC.

FECN COUNT
Total number of FECN bits received on this PVC.

RESET COUNTERS
Resets all sublink counters.

CONFIG

Creates and configures packet endpoints.

One HDLC resource is used by each PRI or each Packet Endpoint.

ENDPNT NAME
Write Security: 3; Read Security: 5
Simplifies configuration with user-definable names such as the name of the frame relay provider or the circuit ID.

PROTOCOL
Write Security: 3; Read Security: 5
Defines the protocol operating on this port. **FRAME RELAY** configures this packet endpoint to frame relay. **TBOP** configures this packet endpoint as transparent bit oriented protocol.

CONFIG
Write Security: 3; Read Security: 5
Displays the configuration for this packet endpoint. This menu is protocol-dependent. TBOP requires no configuration.

SIGNALING ROLE
Defines whether this packet endpoint acts as the network or user side of the UNI or as an NNI.

OFF
Use when the remote device does not support frame relay signaling.

AUTO
Detects the role of the device on the other end of the circuit and automatically sets this packet endpoint to the appropriate value.

BOTH
Operates in NNI mode.

NETWORK
Acts as the network side of the UNI interface.

USER
Acts as the user side of the UNI interface.

SIGNALING TYPE
Controls the frame relay signaling type that operates on this packet endpoint.

AUTO
Detects the signaling type of the device on the other end of the circuit and sets this packet endpoint to the same signaling type.

ANNEX A
Transmits and responds to ITU-T Q.933-A standards.

ANNEX D
Transmits and responds to ANSI T1.617-D standards.

LMI
Transmits and responds to Group of Four specifications.

USER POLL TIMER (T391)
Sets the polling interval to the network in seconds.

USER POLLS PER STATUS (N391)
Controls how many link integrity polls occur between full status polls.

USER BAD EVENT THRESHOLD (N392)
Sets the number of bad polling events that will cause the link to be declared down in N393 Polls.

USER EVENT WINDOW SIZE (N393)
Defines the number of poll events in each monitored window.

If the number of polls reaches N392 in any N393 period, the link will be declared down. When N393 good polls are received, the link will be declared active again.

NET POLL RESPONSE TIMEOUT (T392)
Determines how long this packet endpoint will wait without receiving a poll before declaring the poll bad.

Ensure that this timer is greater than the T391 on the user side of the UNI; otherwise, erratic behavior will result.

NET POLLS PER STATUS (N391)
Sets the number of link integrity polls before a full status is transmitted.

NET BAD EVENTS THRESHOLD (N392)
Sets the number of bad polling events that will cause the link to be declared down in N393 Polls.

NET EVENT WINDOW SIZE (N393)
Defines the number of poll events in each monitored window.

If the number of bad polls reaches N392 in any N393 period, the link will be declared down. When N393 good polls are received, the link will be declared active again.

SUBLINKS

Write Security: 3; Read Security: 5
Allows PVC creation and configuration within a frame relay link that uses sublink DLCIs. Sublinks are not supported in TBOP.

NAME
User-defined name for the DLCI.

DLCI
Local address for each PVC as assigned by the carrier.

QOS
Quality of service. These values can be used to assign a guaranteed amount of bandwidth available for this connection. The sum of all QOS values for the sublink should not exceed the Committed Information Rate (CIR).

BURST
Sets the burst to be used by this virtual circuit for data traffic. A value of zero means that the burst rate is not limited. The value is in kilobits/second (kbps). The **BURST** rate defines by what amount this virtual circuit is allowed to exceed the CIR.

If voice traffic is flowing on *any* sublink on the port carrying *this* sublink, you should enter a value for this setting. Otherwise, leave this as zero. If the service provider has supplied a “Be” value, use that value for this setting. If the service provider has not supplied an excess burst rate, enter the wire speed in this field.

CONFIG
Allows configuration of parameters for each DLCI.

IN-BAND SEQUENCE NUMBER

All packets on this PVC will get a numbered tag so that ADTRAN IQ products can detect lost packets in the frame relay network. Turn this option **ON** only if there is an ADTRAN IQ-capable product on the other end of the PVC.

REMOTE FECN NOTIFICATION

If FECN is received on the interface, a notification is sent to frame relay equipment on other end of the PVC.

REACT TO BECN

If BECN is received, traffic to the frame relay network is flowed off.

DROP DE PACKETS WHEN OVERLOADED

If traffic congestion occurs, discard eligible (DE) packets drop.

FRAGMENTATION THRESHOLD

Defines the maximum data packet size that will be transmitted without fragmenting the data to support voice. Table 8-1 on page 8-9 provides suggested values based on the PVC CIR.

FRAGMENTATION SIZE

Defines packet size when fragmentation is active.

Table 8-1. Suggested Fragmentation Values Based on the PVC CIR

PVC CIR	Frag Size	Frag Threshold	PVC CIR	Frag Size	Frag Threshold
64	56	112	832	1016	2032
128	136	272	896	1096	2192
192	216	432	960	1176	2352
256	296	592	1024	1256	2512
320	376	752	1088	1336	2672
384	456	912	1152	1416	2832
448	536	1072	1216	1496	2992
512	616	1232	1280	1576	3152
576	696	1392	1344	1656	3312
640	776	1552	1408	1736	3472
704	856	1712	1472	1816	3632
768	936	1872	1536	1896	3792

DLCI STATE

Controls how the state of this DLCI is reported to any packet connections within the ATLAS 550 attempting to send or receive data on this DLCI.

AUTO
Passes the state as reported by the frame relay switch. Set **DLCI STATE** to **AUTO** for normal operation.

FORCE UP
This DLCI disregards the status as reported from the switch and reports **ACTIVE** to all packet endpoints within the ATLAS 550.

FORCE DOWN
Reports status as **DOWN** to all packet endpoints within the ATLAS 550.

DIAGNOSTIC MODE
Controls operation of PVC testing options. To allow the far end to measure delay, select **ECHO FAR-END LOOPBACKS**. To continuously measure in-band delay, select **IN-BAND DELAY MEASUREMENT**. To turn off continuous diagnostic functions, select **PASS-THROUGH DIAGNOSTIC PACKETS**.

ECHO FAR-END LOOPBACKS
Generates and transmits a response on this DLCI to the remote equipment if an ADTRAN proprietary diagnostic message is received on this DLCI.

IN-BAND DELAY MEASUREMENT
Generates a diagnostic packet to measure delay through the frame relay network. This process requires that the equipment at the remote site be ADTRAN IQ compatible.

PASS-THROUGH DIAGNOSTIC PACKETS
Used when the ATLAS 550 is acting as a frame relay switch. Transmits a diagnostic packet out the packet endpoint connected to this DLCI, if a diagnostic packet is received on this packet endpoint.

Sublinks Example

Assume the following sublink packet endpoint is connected to the frame relay network via a full T1:

Name	DLCI	QOS
Atlanta	903	768
New York	805	384
San Francisco	615	384

If the PVC to San Francisco needs to transmit data, it will be able to access the network at full T1 rates. If, at the same time, data needs to be transmitted to the PVC to New York, the San Francisco and New York PVCs would equally share the T1 to the frame relay provider because they have the same QOS value. If, also at the same time, data needed to be transmitted to the Atlanta PVC, the T1 would be divided three ways: traffic to Atlanta gets half of the T1, and the New York and San Francisco PVCs equally share the remaining half of the T1, since they share the same QOS value.

USAGE Read Security: 5
This field displays a 7-character summary of the references to this link. Each character can be a dash (-), or it can be a character indicating the resource represented by the character position (see Table 8-2 on page 8-11).

Table 8-2. Usage Characters

Character	Description
1	Packet connection in the first dedicated connections map.
2	Packet connection in the second dedicated connections map.
3	Packet connection in the third dedicated connections map.
4	Packet connection in the fourth dedicated connections map.
5	Packet connection in the fifth dedicated connections map.
s	Switched packet connection in the dial plan.
u	Used by one or more packet switch connections or packet voice entries.

*Packet voice entries are in either the **DEDICATED MAPS** or the **DIAL PLAN**.*

TEST

Provides menus for controlling test options for packet endpoints.

ENDPNT NAME Read Security: 5
Displays the name of the packet endpoint.

PROTOCOL Read Security: 5
Displays the protocol running on this packet endpoint.

SUBLINK Write Security: 3; Read Security: 5
Displays test menus for the packet endpoint sublinks. The menus vary depending on the protocol. Testing is not supported on TBOP.

NAME
User-defined name for the DLCI.

DLCI
Local address for each PVC as assigned by the carrier.

TEST
Shows the test mode for this PVC.

START
The fixed duration that **TEST** is not running and the DLCI is not configured for continuous in-band delay measurement. To change this option, set **DIAGNOSTIC MODE** to **IN-BAND DELAY MEASUREMENT** (also see *In-Band Delay Measurement* on page 8-10).

CONTDLY
The fixed duration **TEST** is not running and the DLCI is configured for continuous in-band delay measurement. The following **RESULTS** menu accumulates these measurements.

STOPTST
The fixed duration **TEST** is running. The following **DURATION** field shows the time remaining in the current test.

DURATION
Shows the duration in seconds for the fixed-duration test.

RESULTS [MN/AV/MX DLY]
Displays the minimum, average, and maximum delay for the delay-measurement test.To display the additional test results, place the cursor over this field and press **Enter** on the keyboard. These times are in milliseconds.

ECHO PKT TX
Displays the total number of test packets that have been transmitted.

ECHO PKT RX
Displays the total number of test packets that have been received.

ECHO PKT DROPPED
Displays the total number of packets lost in the receiving direction (traveling from the remote ADTRAN frame relay device to the ATLAS 550).

RMT PKT DROPPED
Displays the total number of packets lost in the transmit direction (traveling from the ATLAS 550 to the remote ADTRAN frame relay device).

MIN DELAY
Displays the minimum round trip delay for the current test period.

MAX DELAY
Displays the maximum round trip delay for the current test period.

AVG DELAY
Displays the average round trip delay for the current test.

RESET COUNTERS
Resets the counters.

ENDPNT COUNT

Read Security: 5
Displays the total number of packet endpoints configured.

ENDPNTS SORT

Write Security: 3; Read Security: 5
Provides sorting options. **SORTING BY NAME** sorts packet endpoints alphabetically by name. If you do not want to sort packet endpoints, set this option to **OFF**.

PACKET CNCTS

After packet endpoints are defined, they are connected in the packet connects (**PACKET CNCTS**) map. **PACKET CNCTS** connects upper layer protocols from packet endpoint to packet endpoint. You can think of it as a dedicated map for virtual ports rather than physical ports.

FROM: PEP

Write Security: 3; Read Security: 5
Selects one packet endpoint for the packet connection. Packet endpoints created in the packet endpoint configuration are visible on a pull-down menu which includes the **ROUTER** option. Additionally, a router option is available in this pull-down menu. The router is the internal the ATLAS 550 router and can be used multiple times within the **PACKET CNCTS** menu.

SUBLINK

Write Security: 3; Read Security: 5
If the packet endpoint selected in **FROM: PEP** supports sublinks, they are available in this menu. In frame relay, this is the PVC from which you are selecting to groom data.

TO: PEP

Write Security: 3; Read Security: 5
Selects the other packet endpoint for the packet connection. Refer to **FROM: PEP** for more detail.

SUBLINK

Write Security: 3; Read Security: 5
If the **TO: PEP** packet endpoint supports sublinks, the available sublinks are shown within this menu, which includes the **ROUTER** option.

PROTOCOL

Write Security: 3; Read Security: 5
Selects the protocols for this packet connection. Selecting the protocols on each individual connection allows the mixing of data from multiple sources onto a single PVC. Available protocols include the following: **ALL**, **IP**, **PACKET VOICE**, **SNA - LLC2**, **SNAP**, and **TRANSPARENT PROTOCOLS** (**TBOP** and **TASYNC**).

Keep in mind the following:

1. If **ALL** is selected, additional connections from that PVC are not allowed.
2. If **ROUTER** is selected as one packet endpoint, **IP** is automatically set as the **PROTOCOL**.
3. If a **TBOP** packet endpoint is selected as one packet endpoint, **TRANSPARENT** is automatically set as the **PROTOCOL**.

CONFIG Write Security: 3; Read Security: 5
Determines data source and destination. The available options depend on the protocol selected.

CONFLICT Indicates DLCI mismatch.

FROM Indicates data source.

TO Indicates data destination.

CNCTS SORT

Determines the order in which connections are displayed within **PACKET CNCTS**. Options include **FROM PKT ENDPT/SUBLINK**, **TO PKT ENDPT/SUBLINK**, **CONNECTION PROTOCOL**, and **OFF**.

FRAME RELAY IQ

Use this menu to gather and store statistical information in the submenus **ENABLE IQ STATS**, **PORT ENABLES**, **CONFIG**, and **VIEW IQ STATISTICS**.

FRAME RELAY IQ provides information about frame relay activity. Statistical information for ports and PVCs is collected in day and interval (5, 10, 15, 20, or 30 minutes) statistics tables. Users can adjust the number of days and number of intervals for which statistics are gathered; however, interval collections are limited to 5, 10, 15, 20, or 30 minutes.

ENABLE IQ STATS Write security: 2; Read security: 5
Globally enables and disables IQ statistics gathering. IQ statistics are only gathered when this option is enabled. This field defaults to the original setting of **[15 MIN, 7 DAYS, 96 INTS]** when re-enabled.

PORT ENABLES Enables and disables IQ statistics gathering for each port. Use the submenus **NAME**, **ENABLE**, **ALL SUBLINKS**, and **SUBLINKS** to configure the individual ports.

NAME Read security: 5
Displays the port number and name.

ENABLE PORT Write security: 2; Read security: 5
Enables and disables IQ statistics gathering for the port identified in **NAME**.

ALL SUBLINKS Write security: 2; Read security: 5
Provides an easy way to enable or disable IQ statistics gathering on all sublinks. When this activator reads **DISABLE**, pressing **Enter** disables IQ statis-

tics gathering on all sublinks. When it reads **ENABLE**, pressing **Enter** enables IQ statistics gathering on all sublinks.

SUBLINKS Write security: 2; Read security: 5
Identifies the PVC to be polled.

ALL PVCS ENABLED
Indicates the number of sublinks that the ATLAS 550 will collect IQ data for within the given link.

NAME
Read security: 5
Displays the user-designated name of the sublink (up to 15 characters).

DLCI
Read security: 5
Displays the Data Link Connection Identifier (circuit number).

ENABLE
Write security: 2; Read security: 5
Indicates collection of IQ data for the target DLCI.

CONFIG

Sets the parameters for IQ statistics gathering.

CURRENT PIVS Read security: 5
Identifies resources used by IQ statistics storage. A PIV is a port or PVC per interval. The ATLAS 550 can track up to 10,000 PIVs. Think of it as a resource meter. The PIV number is derived from the **MAX DAYS** and **MAX INTERVALS** selected by the user. Changing one affects the other.

INTERVAL PERIOD Write security: 2; Read security: 5
Sets the period for IQ statistics gathering. Options are **5**, **10**, **15**, **20**, and **30 MINUTES**.

MAX DAYS Write security: 2; Read security: 5
Defines the number of history day intervals to keep. Maximum entry is dependent on the **MAX INTERVALS** setting.

MAX INTERVALS Write security: 2; Read security: 5
Defines the number of history intervals to keep. Maximum entry is dependent on the **MAX DAYS** setting.

VIEW IQ STATISTICS

Displays statistical information gathered for intervals and days on a port and for intervals and days on sublinks (PVCs or DLCIs).

INTERVAL / DAY (LINK)

Read security: 5

Descriptions of the statistics available in the **INTERVAL** or **DAY** submenus follow:

RX FRAMES
The number of frames the port received for the interval or day.

RX BYTES
The number of bytes the port received for the interval or day.

MAX RX THRU
The maximum throughput the port received for the interval or day.

AVG RX THRU
The average throughput the port received for the interval or day.

MAX RX UTIL%
The maximum utilization the port received for the interval or day.

AVG RX UTIL%
The average utilization the port received for the interval or day.

TX FRAMES
The number of frames the port transmitted for the interval or day.

TX BYTES
The number of bytes the port transmitted for the interval or day.

MAX TX THRU
The maximum throughput the port transmitted for the interval or day.

AVG TX THRU
The average throughput the port transmitted for the interval or day.

MAX TX UTIL%
The maximum utilization the port transmitted for the interval or day.

AVG TX UTIL%
The average utilization the port transmitted for the interval or day.

PORT UA TIME
Time, in seconds, the port is unavailable due to physical or frame relay outage.

SIG DOWN TIME
Time, in seconds, the signaling state has been down.

SIGNAL ERROR
The number of PVC signaling frames received with protocol violations.

SIGNAL T/O
The number of PVC signal time-outs. Either T391 seconds elapsed without receiving a response to a poll or T392 seconds elapsed without receiving a poll.

SIG STATE CHG
The number of state changes for the PVC signaling protocol. This number includes transitions from down state to up state and vice-versa.

RX FULL STAT
The number of PVC-signaling, full-status frames received.

TX FULL STAT
The number of PVC-signaling, full-status frames transmitted.

RX LI ONLY
The number of PVC-signaling, link integrity only frames received.

TX LI ONLY
The number of PVC-signaling, link integrity only frames transmitted.

ASYNC STATUS
The number of single PVC status frames received.

DISCARD FRAME
The number of frames discarded by the IQ unit.

ABORTS
The number of frames received without proper flag termination.

CRC ERROR
The number of frames received with CRC errors.

OCTET ALIGN
The number of frames received with a bit count not divisible by eight.

LENGTH ERROR
The number of frames received that are less than 5 bytes or greater than 4500 bytes.

EA VIOLATION
The number of frames received with errors in the EA field of the frame relay header.

INACTIVE DLCI
The number of frames received while the PVC is in the inactive state.

INVALID DLCI
The number of frames received with a DLCI value less than 16 or greater than 1007, not including PVC signaling frames.

SUBLINK

Provides statistics for a particular DLCI or PVC by interval or day. Descriptions of the statistics available from the **INTERVAL** or **DAY** submenus of **SUBLINK** follow:

RX FRAMES
The number of frames the PVC received for the interval or day.

RX BYTES
The number of bytes the PVC received for the interval or day.

MAX RX THRU
The maximum throughput the PVC received for the interval or day.

AVG RX THRU
The average throughput the PVC received for the interval or day.

MAX RX UTIL%
The maximum utilization the PVC received for the interval or day.

AVG RX UTIL%
The average utilization the PVC received for the interval or day.

TX FRAMES
The number of frames the PVC transmitted for the interval or day.

TX BYTES
The number of bytes the PVC transmitted for the interval or day.

MAX TX THRU
The maximum throughput the PVC transmitted for the interval or day.

AVG TX THRU
The average throughput the PVC transmitted for the interval or day.

MAX TX UTIL%
The maximum utilization the PVC transmitted for the interval or day.

AVG TX UTIL%
The average utilization the PVC transmitted for the interval or day.

PVC IA TIME
Time, in seconds, the PVC has been in the inactive state for the interval or day.

RX FECN
The number of FECNs the PVC has received for the interval or day.

TX FECN
The number of FECNs the PVC has transmitted for the interval or day.

RX BECN
The number of BECNs the PVC has received for the interval or day.

TX BECN
The number of BECNs the PVC has transmitted for the interval or day.

RX DE
The number of DEs the PVC has received for the interval or day.

TX DE
The number of DEs the PVC has transmitted for the interval or day.

RX CR
The number of CRs the PVC has received for the interval or day.

TX CR
The number of CRs the PVC has transmitted for the interval or day.

LOST FRAMES
The number of lost frames on the PVC for the interval or day.

RMT LOST FRMS
The number of remote lost frames on the PVC for the interval. Applies only if **IN-BAND SEQUENCE NUMBER** is **ENABLED** (see page 8-9) on the PVC.

RX BURST SEC
The number of bursty seconds the PVC received for the interval or day.

TX BURST SEC
The number of bursty seconds the PVC transmitted for the interval or day.

MIN RX FRAME
The minimum frame size the PVC received for the interval or day.

MAX RX FRAME
The maximum frame size the PVC received for the interval or day.

AVG RX FRAME
The average frame size the PVC received for the interval or day.

MIN TX FRAME
The minimum frame size the PVC transmitted for the interval or day.

MAX TX FRAME
The maximum frame size the PVC transmitted for the interval or day.

AVG TX FRAME
The average frame size the PVC transmitted for the interval or day.

MIN FRAME DLY
The minimum **IN-BAND DELAY MEASUREMENT** is **ENABLED** (see page 8-10) for the PVC or if PVC diagnostics are being performed.

MAX FRAME DLY
The maximum delay in milliseconds on the PVC for the interval or day. Applies only if **IN-BAND DELAY MEASUREMENT** is **ENABLED** (see page 8-10) for the PVC or if PVC diagnostics are being performed.

AVG FRAME DLY
The average delay in milliseconds on the PVC for the interval or day. Applies only if **IN-BAND DELAY MEASUREMENT** is **ENABLED** (see page 8-10) for the PVC or if PVC diagnostics are being performed.

PVC STATE CHANGE
The number of state changes for this PVC for the interval or day.

Chapter 9 Router

OVERVIEW

The ATLAS 550 router provides remote connectivity of LANs within an ATLAS 550—from LAN-to-WAN connection or from WAN-to-WAN connection.

Internet Protocol (IP) routing is performed at layer 3 of the Open System Interconnection (OSI) model. (See Appendix B, *OSI Model and Frame Relay Technology Overview*, for a discussion of the OSI model.) The routing process determines the optimal path for data packets to travel and then moves the data packets along that path. Routers exchange information about paths or routes that reach additional LAN segments. This exchange of routing information allows a router to build a detailed knowledge of the network topology. Criteria for selecting the best path can include such items as distance, number of hops (servers or routers), and cost of the transportation media.

The ATLAS 550 supports Routing Information Protocol (RIP), a protocol based on hops. Each route has a set number of hops (routers or servers) that it must travel through to reach a final destination. If a new route to a host address that has a fewer number of hops is learned, it becomes the preferred route. When a new route is learned, the router increments the hop count by one and immediately broadcasts the new route over the other interfaces. To prevent routing loops, RIP defines a hop count of 16 as an infinite or unreachable route.

The **ROUTER MENU** defines, configures, and monitors all ATLAS 550 **ROUTER** options. Figure 9-1 on page 9-2 displays the IP Router menu tree.

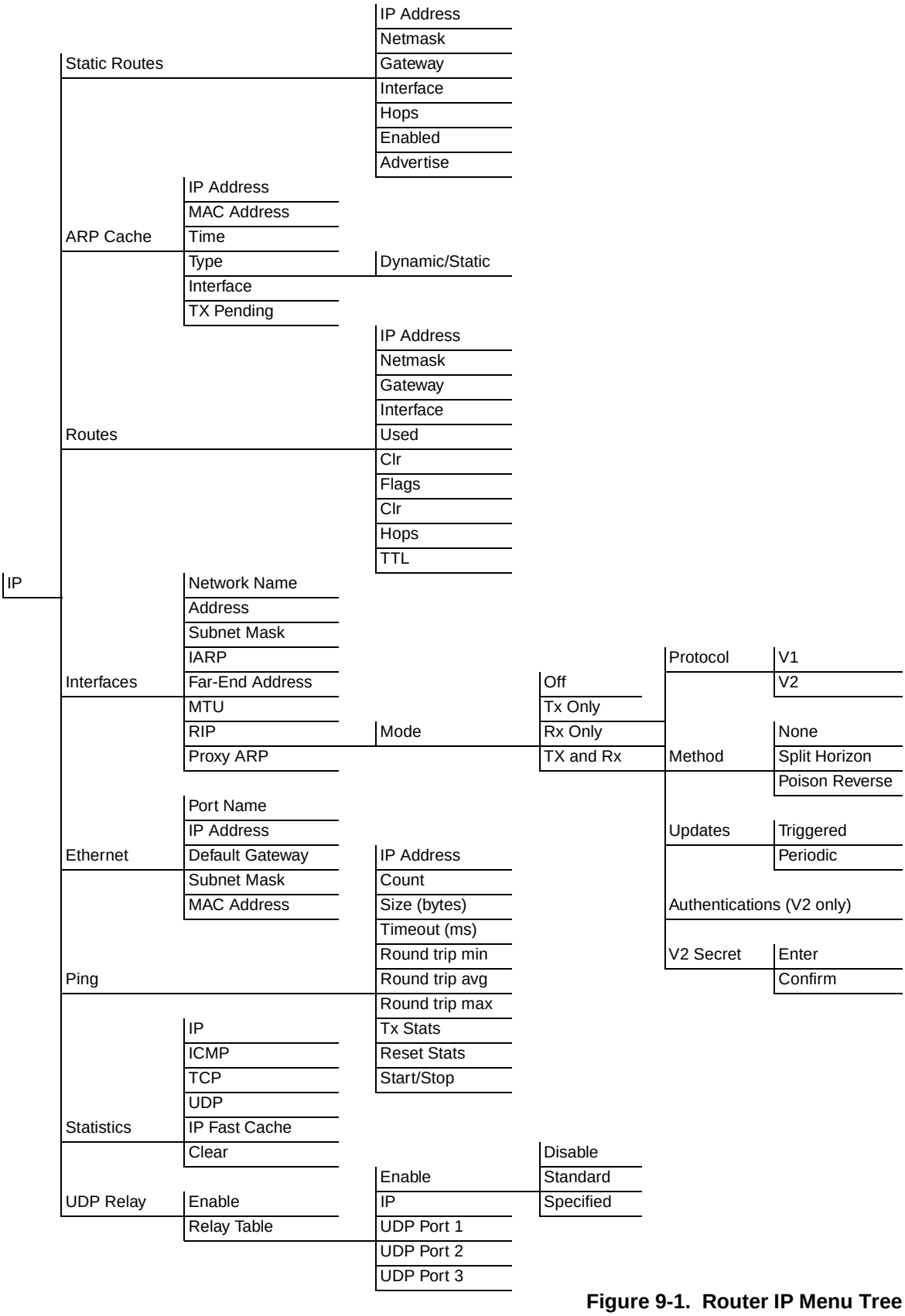


Figure 9-1. Router IP Menu Tree

IP MENUS

The **IP MENU** defines and monitors IP routes (see Figure 9-2).

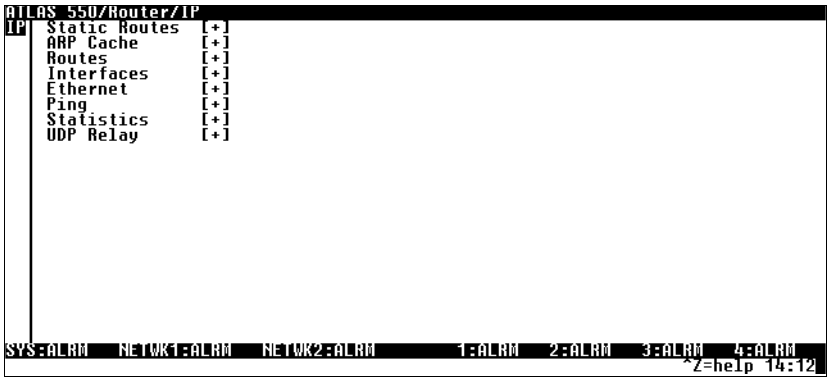


Figure 9-2. IP Routes Menu

STATIC ROUTES

The **STATIC ROUTES MENU** manages static IP routes. You can create, modify, and delete routes using this menu.

IP ADDRESS

Write security: 2; Read security: 5
Defines the IP address of the host or network device being routed to.

NETMASK

Write security: 2; Read security: 5
Determines for routing the number of bits used in the above-defined IP address. If a host address is desired for the IP address, this field must be set to 255.255.255.255.

GATEWAY

Write security: 2; Read security: 5
Defines the IP address of the router to receive the forwarded IP packet.

INTERFACE

Write security: 2; Read security: 5
Defines the interface to which IP packets with this address will be routed. These are either Ethernet or frame relay DLCIs.

HOPS

Write security: 2; Read security: 5
Defines the number of router hops required to get to the network or host. Maximum distance is 15 hops.

ENABLED

Write security: 2; Read security: 5
Enables or disables this static route.

ADVERTISE

Write security: 2; Read security: 5
When set to **YES**, this static route is advertised over all interfaces on which a route advertisement protocol (e.g. RIP) is enabled. When set to **NO**, this is a private route.

ARP CACHE

The **ARP CACHE MENU** displays the contents of the ATLAS 550 Address Resolution Protocol (ARP) cache. All resolved cache entries time out after 20 minutes. Unresolved entries time out in 3 minutes.

IP ADDRESS

Read security: 5
Displays the IP address used for resolving MAC address.

MAC ADDRESS

Read security: 5
Resolves Ethernet address. If set to all zeros, there is no resolution for that address.

TIME

Read security: 5
Displays the minutes since the entry was last referenced.

TYPE

Write security: 2; Read security: 5
Defines this entry as dynamic or static.

INTERFACE

Read security: 5
Displays the interface upon which this entry was found.

TX PENDING

Read security: 5
Displays the number of transmit packets pending a reply.

ROUTES

The **ROUTES MENU** displays the contents of the ATLAS 550 route table. All static and discovered routes are displayed from this menu.

IP ADDRESS

Read security: 5
Displays the IP address of the network or host destination address.

NETMASK

Read security: 5
Displays the netmask applied to the destination address.

GATEWAY

Read security: 55
Displays the IP address of the host or router receiving the forwarded IP packet.

INTERFACE

Read security: 5
Displays the interface to which IP packets with this address will be routed.

LOCAL

Sent directly to the ATLAS 550 router.

EN0 IP

The ATLAS 550 Ethernet port.

ENDPOINT NAME

The DLCI number.

USED

Read Security: 5
Displays the number of times the router has referenced this route.

CLR

Write security: 2; Read security: 5
Clears the **USED** count field for this route.

FLAGS

Read security: 5
Indicates the properties of this routing table entry, composed of the following letters:

- **H** - route is a host route
- **G** - route is a gateway route
- **D** - route learned dynamically from RIP
- **I** - route learned from an ICMP redirect
- **P** - route is private and is not advertised with RIP
- **T** - route is to a triggered port (updated only when table changes)

HOPS

Read security: 5
Displays the number of router hops required to get to the network or host. Ranges from 0 to 16. If set to 16, it is defined as infinite and cannot be routed.

TTL

Read security: 5
Displays the number of seconds until the address is removed from table. Value of 999 means the route is static.

INTERFACES

The **INTERFACES MENU** configures and monitors all interfaces connected to the ATLAS 550 router. These include the Ethernet and frame relay DLCIs connected in the **PACKET MANAGER/ PACKET CNCTS**.

NETWORK NAME

Read security: 5
Displays the name of the interface connected to the ATLAS 550 router. The options are listed below:

EN0 IP The ATLAS 550 Ethernet port.

ENDPOINT NAME The DLCI number.

ADDRESS

Write security: 2; Read security: 5
Defines the individual interface IP address. If this field is left as 0.0.0.0, it is treated as an unnumbered interface.

SUBNET MASK

Write security: 2; Read security: 5
Defines the subnet mask applied to the address defined for this link. If the subnet mask is unnumbered, leave as 0.0.0.0.

IARP

Write security: 2; Read security: 5
The Inverse ARP (IARP) field is only present when this is a frame-relay network interface. The ATLAS 550 always responds to Inverse ARP requests with its IP address for the requested DLCI.

ENABLE

The ATLAS 550 sends Inverse ARP packets in order to determine the IP address on the other end of the virtual circuit. If the Inverse ARP packet is responded to, a route is placed in the IP route table. When this field is set to **ENABLE**, the ATLAS 550 dynamically sends Inverse ARP packets to determine the IP address on the other end of the virtual circuit. When an Inverse ARP packet is not responded to, a route is placed in the IP route table.

DISABLE

The ATLAS 550 responds to Inverse ARP requests with its IP address for the requested DLCI. If set to **DISABLE**, the ATLAS 550 does not generate Inverse ARP request packets. In this case, the **FAR-END ADDRESS** parameter may be used to statically assign a route address (see the following section, *Far-End Address*).

FAR-END ADDRESS

Write security: 2; Read security: 5
The Far-End IP Address field is only present for frame-relay network interfaces, and it is only selectable when Inverse ARP is disabled. The IP address of the device on the other end of the virtual circuit may be specified. A static route to the far-end network will be added using the interface *Subnet-Mask* if nonzero. If 0.0.0.0 has been specified for the *Subnet-Mask*, a default subnet mask is used based on the class of the Far-End Address. (See also the previous section, *Subnet Mask*.)

MTU

Read security: 5
Defines maximum number of bytes in a datagram transmitted over this interface. (Maximum Transmit Unit)

RIP

Configures routing information protocol (RIP) on this interface.

MODE

Write security: 2; Read security: 5
Allows RIP to be enabled or disabled on a per-interface basis.Turn off (**OFF**) if you do not want to enable this feature.

TX ONLY
RIP advertisements are periodically transmitted, but are not listened to on this virtual circuit.

RX ONLY
RIP advertisements are not transmitted on this virtual circuit, but they are listened to.

TX AND RX
RIP advertisements are periodically transmitted and are listened to on this virtual circuit.

If **MODE** *is* **OFF**, *the following menus (*PROTOCOL, METHOD, *and* **UPDATES**) *will* ***not*** *be visible.*

PROTOCOL
Write security: 2; Read security: 5
Sets the version of RIP being used on this interface. The options are **RIP V1** (version 1) and **RIP V2** (version 2).

If RIP V2 is selected, a user-defined secret must be created (see V2 Secret on page 9-8).

METHOD
Write security: 2; Read security: 5
Defines the method used to send RIP route advertisements. The options are listed below:

NONE
All routes in the router table are advertised through this interface with no modification of the routing metric.

SPLIT HORIZON
Only advertises routes not learned through this interface.

POISON REVERSE
All routes are advertised, but the routes learned through this interface are “poisoned” with an infinite route metric.

UPDATES
Write security: 2; Read security: 5
Defines when RIP advertisements are transmitted.

PERIODIC
RIP advertisements are periodically transmitted.

TRIGGERED
RIP advertisements are transmitted only when new routes are learned, and learned routes do not age.

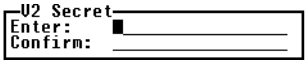
AUTHENTICATION

Write security: 2; Read security: 5
Enables the V2 Secret to be advertised when using RIP V2. **AUTHENTICATION** is visible only if **RIP V2** is **ENABLED** (see the previous section, *Protocol on page 9-7).* When enabled, requires all received RIP V2 packets to be authenticated against the configured V2 secret. All transmitted RIP V2 packets will include the secret.

> **NOTE** *This parameter is global throughout the ATLAS 550. Changes here affect all router interfaces.*

V2 SECRET

Write security: 2; Read security: 5
Defines the secret used to advertise routes when using **RIP V2**. To create the secret, enter the new secret, and press **Enter** on the keyboard. Then re-enter the secret and press **Enter** again to confirm it. **V2 SECRET** is only visible if **AUTHENTICATION** is set to **ENABLED**.



PROXY ARP

Write security: 2; Read security: 5
Enables or disables proxy ARP on this interface.

ETHERNET

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 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 550 IP address to determine which nodes must be reached through the default IP gateway.

MAC ADDRESS Displays the system Ethernet Media Access Control (MAC) address. This field is read-only.

PING

Write security: 5; Read security: 5
Allows you to send pings (Internet Control Message Protocol (ICMP) requests) to devices accessible via the network.

Only one ping session can be active at a time.

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

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

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

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

ROUND TRIP MIN Read security: 5
Displays the minimum round trip time of the ping request / reply of the current set of pings.

ROUND TRIP AVG Read security: 5
Displays the average round trip time of the ping request / reply of the current set of pings.

ROUND TRIP MAX Read security: 5
Displays the maximum round trip time of the ping request / reply of the current set of pings.

TX STATS

Read security: 5
Displays the number of ping requests transmitted (***n*** **TXED**), the number of ping replies received (***n*** **RXED**) and the number of ping requests that were lost (***n*** **LOST**).

RESET STATS

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

START/STOP

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

STATISTICS

This section describes the statistics submenus **IP**, **ICMP**, **TCP**, **UDP**, and **IP FAST CACHE**. All of these statistics are taken from the MIB-2 variables in RFC 1156.

IP

Table 9-1 describes the **IP** statistics.

Table 9-1. IP Statistics

Name	Description
Forwarding	The indication of whether thisATLAS 550 is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this ATLAS 550. IP gateways forward datagrams; hosts do not (except those Source-Routed via the host).
Default TTL	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this ATLAS 550, whenever a TTL value is not supplied by the transport layer protocol.
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
InAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this ATLAS 550. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Table 9-1. IP Statistics (Continued)

Name	Description
ForwDatagrams	The number of input datagrams for which thisATLAS 550 was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this ATLAS 550, and the Source-Route option processing was successful.
InUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g. for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this “no-route” criterion
ReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this ATLAS 550.
ReasmReqds	The number of IP fragments received which needed to be reassembled at this ATLAS 550.
ReasmOKs	The number of IP datagrams successfully re-assembled.
ReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably RFC 815’s) can lose track of the number of fragments by combining them as they are received.
FragOKs	The number of IP datagrams that have been successfully fragmented at this ATLAS 550.
FragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this ATLAS 550 but could not be, e.g., because their “Don't Fragment” flag was set.

Table 9-1. IP Statistics (Continued)

Name	Description
FragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this ATLAS 550.
Clear	Clears the accumulated statistics.

ICMP

Table 9-2 describes the **ICMP** statistics.

Table 9-2. ICMP Statistics

Name	Description
InMsgs	The total number of ICMP messages which the ATLAS 550 received. Note that this counter includes all those counted by icmpInErrors.
InErrors	The number of ICMP messages which the ATLAS 550 received but determined as having errors (bad ICMP checksums, bad length, etc.).
InDestUnreachs	The number of ICMP Destination Unreachable messages received.
InTimeExcds	The number of ICMP Time Exceeded messages received.
InParmProbs	The number of ICMP Parameter Problem messages received.
InSrcQuenchs	The number of ICMP Source Quench messages received.
InRedirects	The number of ICMP Redirect messages received.
InEchos	The number of ICMP Echo (request) messages received.
InEchoReps	The number of ICMP Echo Reply messages received.
InTimestamps	The number of ICMP Timestamp (request) messages received.
InTimestampReps	The number of ICMP Timestamp Reply messages received.
InAddrMasks	The number of ICMP Address Mask Request messages received.
InAddrMaskReps	The number of ICMP Address Mask Reply messages received.
OutMsgs	The total number of ICMP messages which this ATLAS 550 attempted to send. Note that this counter includes all those counted by icmpOutErrors.
OutErrors	The number of ICMP messages which this ATLAS 550 did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
OutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
OutTimeExcds	The number of ICMP Time Exceeded messages sent.
OutParmProbs	The number of ICMP Parameter Problem messages sent.
OutSrcQuenchs	The number of ICMP Source Quench messages sent.

Table 9-2. ICMP Statistics (Continued)

Name	Description
OutRedirects	The number of ICMP Redirect messages sent.
OutEchos	The number of ICMP Echo (request) messages sent.
OutEchoReps	The number of ICMP Echo Reply messages sent.
OutTimestamps	The number of ICMP Timestamp (request) messages sent.
OutTimestampReps	The number of ICMP Timestamp Reply messages sent.
OutAddrMasks	The number of ICMP Address Mask Request messages sent.
OutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.
Clear	Clears the accumulated statistics.

TCP

Table 9-3 describes the **TCP** statistics.

Table 9-3. TCP Statistics

Name	Description
RtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
RtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
RtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
MaxConn	The limit on the total number of TCP connections the ATLAS 550 can support. In entities where the maximum number of connections is dynamic, this object should contain the value “-1.”
ActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
PassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
AttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

Table 9-3. TCP Statistics (Continued)

Name	Description
EstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
CurrEstab	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
InSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
RetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Clear	Clears the accumulated statistics.

UDP

Table 9-4 describes the **UDP** statistics.

Table 9-4. UDP Statistics

Name	Description
InDatagrams	The total number of UDP datagrams delivered to UDP users.
NoPorts	The total number of received UDP datagrams for which there was no application at the destination port.
InErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
OutDatagrams	The total number of UDP datagrams sent from this ATLAS 550.
Clear	Clears the accumulated statistics.

IP FAST CACHE

Table 9-5 describes the **IP FAST CACHE** statistics.

Table 9-5. IP Fast Cache Statistics

Name	Description
Hits	Total number of times the ATLAS 550 went into the Fast Cache and successfully retrieved an IP address.
Misses	Total number of times the ATLAS 550 went into the FastCache and failed to retrieve an IP address.
Clear	Clears the accumulated statistics.

UDP RELAY

Write security: 2; Read security:5
Configures the ATLAS 550 as a UDP (User Datagram Protocol) relay agent to relay UDP broadcasts to a specified server IP address. UDP broadcasts received on a given port may be relayed to, at most, one server.

ENABLED

Enables / disables UDP Relay. An entry in the UDP relay table can configure the ATLAS 550 to relay either **STANDARD** ports or up to three **SPECIFIED** ports.

STANDARD

Relays the following UDP protocols: DHCP, TFTP, DNS, NTP, NBNS (NetBIOS Name Server), NBDG (NetBIOS DataGram), and BootP.

SPECIFIED

Relays datagrams received on any of the specified ports.

RELAY TABLE

Sets server IP addresses and UDP relay ports.

ENABLE

Enables the **RELAY TABLE**. This option can also be set to **DISABLE**.

IP

Defines IP addresses that will receive the relay packet.

UDP PORT 1

Specifies the UDP port to be relayed. Set to zero (0) to disable.

UDP PORT 2

Specifies the UDP port to be relayed. Set to zero (0) to disable.

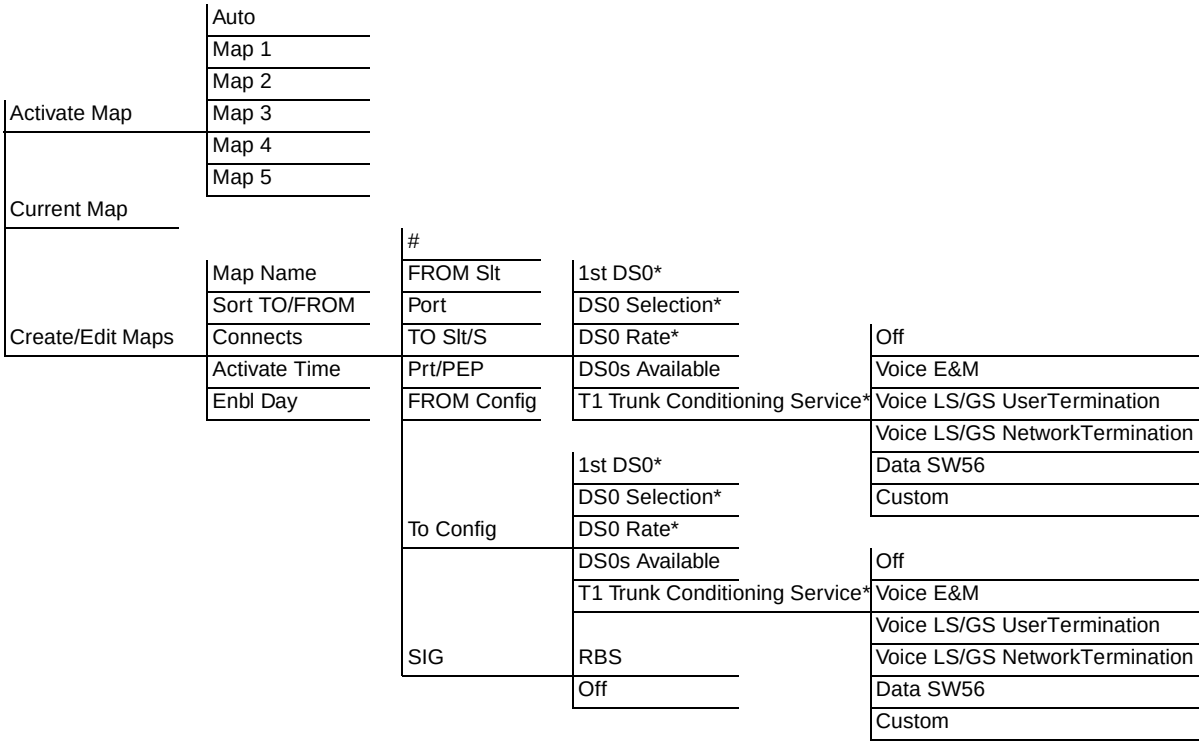
UDP PORT 3

Specifies the UDP port to be relayed. Set to zero (0) to disable.

Chapter 10 Dedicated Maps

OVERVIEW

The **DEDICATED MAPS** options assign dedicated connections between any two ports in the ATLAS 550 Base Unit. This chapter describes the **DEDICATED MAPS** menu (see Figure 10-1). These options are module-dependent; that is, the menu items available depend on the module selected. In addition, step-by-step instructions are provided for setting up a sample dedicated map (see *Creating A Dedicated Map* on page 10-7).



* Selection is module-dependent.

Figure 10-1. Dedicated Maps Menu Tree

USING DEDICATED MAPS WITH FRAME RELAY

After packet endpoints are created, they must be connected to a physical port. You can connect the endpoints using either the **DEDICATED MAP** or the **DIAL PLAN** (see also, Chapter 11, *Dial Plan*). **DEDICATED MAPS** "nail" the endpoints to a service, and the **DIAL PLAN** associates a phone number with the endpoint.

For packet links created within the **PACKET MANAGER MENU,** use **DEDICATED MAPS** (see Figure 10-2) to connect packet endpoints to a physical port. Nail the endpoint to a service by selecting **DEDICATED MAPS** and picking a physical slot (**FROM SLT**) and a port (**PORT/PEP**) for the data. Assign the DS0s (**FROM CONFIG**), and then set the service (**TO SLT/S**) to **PKT ENDPT** or **PKT VOICE**.

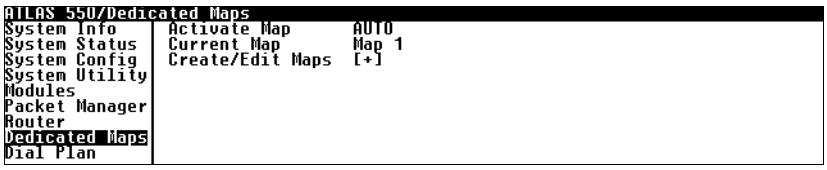


Figure 10-2. Dedicated Maps - Frame Relay

ACTIVATE MAP

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

AUTO

Automatically activates a particular dedicated map at the time and day specified in **ACTIVATE TIME** (see *Activate Time* on page 10-6).

MAPS 1 THROUGH 5

Allows you to manually activate a specific dedicated map.

Instructions for Manually Activating a Dedicated Map

Step	Action
1	Move the arrow keys to highlight the **ACTIVATE MAP** field and press **ENTER**.
2	Move the arrow key to highlight the map of choice from the pop-up menu list and press **ENTER**.

CURRENT MAP

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

CREATE / EDIT MAPS

Creates new maps and defines settings, as well as edits existing maps. To add a new map, position the cursor in the index column and press **I**. ATLAS 550 automatically names the maps in the sequence in which they are created; however, this sequence can be sorted (see the subsequent discussion of *Sort TO/FROM*). You can change the names with **MAP NAME**.

MAP NAME

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

SORT TO/FROM

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

CONNECTS

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

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

#

Displays the index number of the dedicated map connection. To add another dedicated map connection, press the **I** key on your keyboard. New map connections are numbered consecutively. To delete a connection, press **D**.

FROM SLT

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

PORT

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

The ATLAS 550 does not support frame relay at a DS0 rate of 56K.

TO SLT/S

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

PRT/PEP

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

The ATLAS 550 does not support frame relay at a DS0 rate of 56K.

FROM CONFIG

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

1ST DS0

Write security: 3; Read security: 5
Defines the first DS0 for this endpoint. The ATLAS 550 uses DS0s, starting with this selection, to send and receive calls to and from the network. This option is module-dependent.

DS0 SELECTION

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

DSO RATE

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

DS0s Available

Read security: 5

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

- **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.

T1 Trouble Code Service

Write security: 3; Read security: 5

Sets known values in the data field for outgoing DS0s which are cross-connected to a T1 port experiencing alarms. Choose from **Off**, **Voice**, **Data**, and **Custom**, depending on the type of traffic on the T1.

T1 Trouble Code Service only applies to non-RBS T1s in the **Dedicated Map**.

T1 Trunk Conditioning Service

Write security: 3; Read security: 5

Sets known values in the signaling bits and the data field for outgoing DS0s which are cross-connected to a T1 port experiencing alarms. The trunk conditioning process consists of a 2.5-second transmission (indicating call termination), followed by a continuous transmission signaling the final condition as chosen by the user. See the trunk conditioning example on page 10-7.

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

Choose from **Off**, **Voice E&M**, **Voice LS/GS User Termination**, **Voice LS/GS Network Termination**, **Data SW56**, and **Custom**—depending on the type of traffic or configuration of the T1.

Table 10-1 describes the options for **T1 TRUNK CONDITIONING SERVICE**.

Table 10-1. T1 Trunk Conditioning Service Options

Option	Description
T1 Trunk Conditioning State	Defines the final fault signaling state as follows: **IDLE** is used for one-way trunks; that is, for outgoing or incoming calls, but not both. **SEIZED** is used for two-way trunks. It prevents the PBX from attempting to use a failed trunk for an outgoing call. This option is not included for **CUSTOM**.
T1 Fault Signaling (AB/AB)	Defines to the ATLAS 550 the signaling bits being used on the trunk. *Fault signaling is only visible when RBS is turned on.*
T1 Trouble Code Value	Defines to the ATLAS 550 the value to set in the data field for outgoing DS0s when a trouble condition exists.

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. See *From Config* on page 10-4 for a description of these settings.

SIG Write security: 3; Read security: 5
(Signaling) Defines whether the connection has active RBS. Where RBS is not an option, the ATLAS 550 automatically assigns the correct setting. For example, a T1-to-Nx connection is set to **Off**.

RBS Preserves the signaling bits between the connections.

OFF Ignores signaling bits.

ACTIVATE TIME Write security: 3; Read security: 5
Sets the time when the map becomes active if you have selected **AUTO** in the **ACTIVATE MAP** field (see *Activate Map* on page 10-2). Enter this time in hh:mm:ss 24-hour format.

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

Example 1 Setting Trunk Conditioning

The trunk conditioning process (see also, *T1 Trunk Conditioning Service* on page 10-5) sets known values in the signaling bits and the data bits for outgoing DS0s which are cross-connected to a T1 port experiencing alarms. The trunk conditioning process consists of a 2.5-second transmission (indicating call termination), followed by a continuous transmission (signaling the final condition as chosen by the user).

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

For this example, assume voice traffic is received on T1-A, and T1-B is groomed onto T1-C to the PBX (see Figure 10-3). If T1-A fails, the DS0s which were cross-connected to T1-C will receive trunk conditioning.

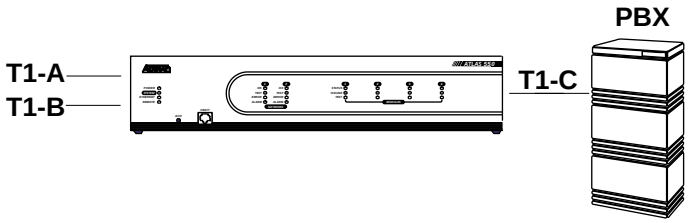


Figure 10-3. Trunk Conditioning

Example 2 Creating A Dedicated Map

Any ATLAS 550 port supporting dedicated bandwidth can be mapped to any other port supporting dedicated bandwidth. A dedicated map defines connections for dedicated bandwidth between ports and also grooms and cross-connects bandwidth between T1 ports. For this example, the central ATLAS 550 is equipped as shown in Figure 10-4.

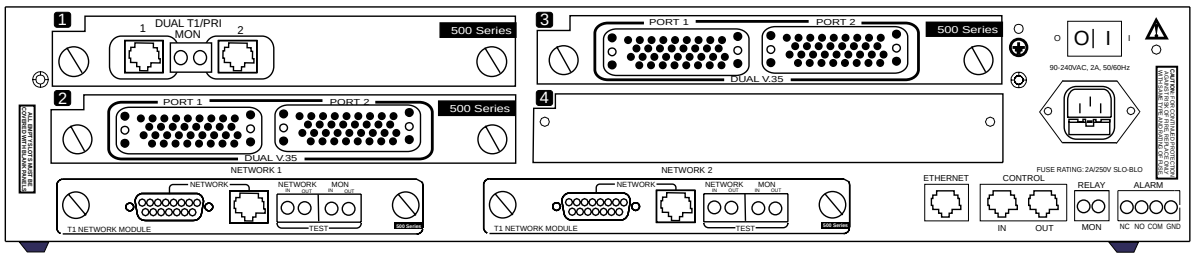


Figure 10-4. ATLAS 550 with Modules Installed for Example 2

Example 2 (see Figure 10-5) contains three T1s (T1-A, T1-B, T1-C) that support dedicated bandwidth from three remote sites. Each remote T1 includes DS0s for voice (1-8) and data (9-24). At the central site (the ATLAS 550), each

incoming DS0 carrying data is mapped to a separate V.35 port and connected to the router. DS0s carrying voice are collected together (groomed) and sent to the PBX over a single T1 (T1-D).

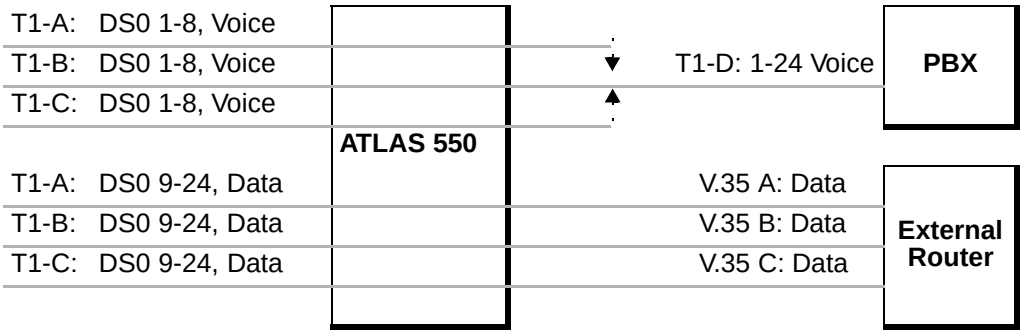


Figure 10-5. Overview of Dedicated Map Example

Designing the Dedicated Map for Example 2

In designing a dedicated map, follow the general procedure listed below:

1. Determine which connections to make and which ports to involve. For T1 ports, you must also decide which DS0s to use.
2. Configure the ports.
3. Define the appropriate connections.

The remainder of this chapter provides the step-by-step procedures for creating a dedicated map based on example 2 and the connections and ports listed in Table 10-2 on page 10-8.

Table 10-2. Connections And Ports for the Dedicated Map in Example 2

Name	ATLAS 550 Port	DS0s	Name	ATLAS 550 Port	DS0s
T1-A Voice	T1/PRI Network Interface: Network Slot 1	1-8; RBS On	T1-D	Dual T1/PRI DSX: Slot 1/Port 2	1-8; RBS On
T1-B Voice	T1/PRI Network Interface: Network Slot 2	1-8; RBS On	T1-D	Dual T1/PRI DSX: Slot 1/Port 2	9-16; RBS On
T1-C Voice	Dual T1/PRI: Slot 1/Port 1	1-8; RBS On	T1-D	Dual/T1/PRI DSX: Slot 1/Port 2	17-24; RBS On
T1-A Data	T1/PRI Network Interface: Network Slot 1	9-24; RBS Off	V.35 A	Dual V.35: Slot 2/Port 1	N/A
T1-B Data	T1/PRI Network Interface: Network Slot 2	9-24; RBS Off	V.35 B	Dual V.35: Slot 2/Port 2	N/A
T1-C Data	Dual T1/PRI: Slot 1/Port 1	9-24; RBS Off	V.35 C	Dual V.35: Slot 3/Port 1	N/A

Configuring the Ports for Example 2

Complete the steps outlined in the following Step / Action table to configure the various ports to match the framing parameters of the T1 line provided by the telco. (Also see Table 10-2.)

Instructions for Configuring the Ports	
Step	**Action**
1	Navigate to **MODULES**.
2	Select **NTW1** (a T1/PRI network interface).
3	Set the line framing parameters by selecting the corresponding **MENU / CONFIGURATION / FRAME / ESF**.
4	Navigate to **PRT** and press **C** to copy this configuration information for use with additional ports.
5	Navigate back to **NTW2** and move to its corresponding **MENU / CONFIGURATION / PRT**. Paste the information copied in step 3 here by pressing **P**. Press **Y** to confirm paste.
6	Assign a T1/PRI card to Slot 1. Paste the information copied in step 3 by moving to the corresponding **MENU / CONFIGURATION / PRT** and pressing **P**. Press **Y** to confirm paste (see Figure 10-6 on page 10-9).
7	Assign Dual Nx 56/64 cards (V35Nx-2) to Slots 2 and 3.

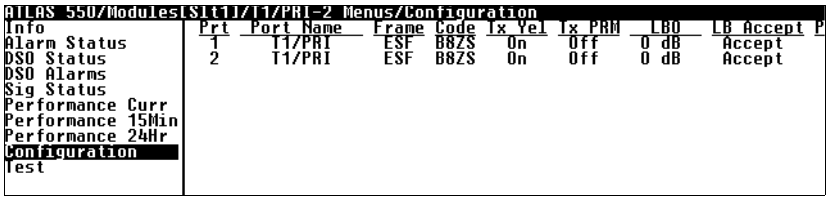


Figure 10-6. T1/PRI Configuration Menu for Example 2

Defining the Connections for Example 2

Define the connections by completing the following Step / Action tables. Make the data connections first and then make the voice connections. Refer to Table 10-2 on page 10-8 and Figure 10-7 as you define the connections.

Instructions for Defining the Data Connections (DS0s 9-24)	
Step	**Action**
1	Name your map by navigating to **DEDICATED MAPS / CREATE/EDIT MAPS** and entering a name.
2	Navigate to the **CREATE/EDIT MAPS** field, **CONNECTS**. This field defines the connections necessary to route the required bandwidth.
3	For T1-A Data, select and define **FROM SLOT** as **N1) T1/PRI-1**.
4	Select and define the "from" **PORT** as **1)T1/PRI**.
5	Select and define **TO SLT/S** as **S2) V35Nx**; S2) represents Slot 2.
6	Select and define **PRT/PEP** as **1) Nx56/64**; 1) represents Port 1 of Slot 2.
7	Select and define **FROM CONFIG** DS0s as **9-24**.
8	Set the V.35 to operate at 64k per DS0 in **TO CONFIG**, **[RATE=64K]**.
9	Repeat these steps for the remaining data connections (i.e., T1-B and T1-C) as follows:
9a	Copy the current connection by positioning the cursor on the index # and pressing **C**.
9b	Insert new connection lines by positioning the cursor over the index # of the current connection and pressing **I** on the keyboard.
9c	Paste this information onto a new connection line by positioning the cursor over the index number of the new connection, and pressing **P**.
10	Modify these connection lines to complete the connections for data (see Figure 10-7).

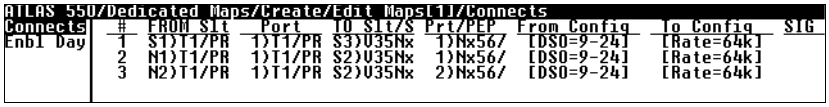


Figure 10-7. Data Connections

Instructions for Defining Voice Connections (DS0s 1-8)	
Step	**Action**
1	Set the **FROM SLOT** and **PORT** for the first voice connection, A, as **N1) T1/PRI** and **1) T1/PRI**, respectively.
2	Set the **FROM CONFIG** voice DS0s as **[DS0=1-8]**.
3	Set **TO SLT/S** and **PRT/PEP** for the PBX connection as **S1) T1/PRI** and **1) T1/PRI**, respectively. This action selects the Dual T1/PRI in Slot 1/Port 2.
4	Set the **FIRST DS0S** for this connection in **TO CONFIG**. For Voice A, the first DS0 is 1; for Voice B, it is 9; and for Voice C it is 17. (This action sets the DACSing between the T1s.)
5	Set **SIG** to **RBS**.
6	(Optional) From **TO CONFIG**, set the trunk conditioning (Signaling and Data code) for T1 failure.
7	Repeat for the remaining voice connections.

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

ATLAS 550/Dedicated Maps/Create/Edit Maps[1]/Connects[6]/To Config

Connects Enbl Day	#	FROM Slt	Port	TO Slt/S	Prt/PEP	From Config	To Config	SIG
	1	N1)T1/PR	1)T1/PR	S2)U35Nx	1)Nx56/	[DS0=9-24]	[Rate=64k]	
	2	N2)T1/PR	1)T1/PR	S2)U35Nx	2)Nx56/	[DS0=9-24]	[Rate=64k]	
	3	S1)T1/PR	1)T1/PR	S3)U35Nx	1)Nx56/	[DS0=9-24]	[Rate=64k]	
	4	N1)T1/PR	1)T1/PR	S1)T1/PR	2)T1/PR	[DS0=1-8]	[1st DS0=1]	Off
	5	N2)T1/PR	1)T1/PR	S1)T1/PR	2)T1/PR	[DS0=1-8]	[1st DS0=9]	Off
	6	S1)T1/PR	1)T1/PR	S1)T1/PR	2)T1/PR	[DS0=1-8]	[1st DS0=17]	Off

Figure 10-8. Completed Dedicated Map for Example 2

Chapter 11 Dial Plan

OVERVIEW

This chapter provides information on the **DIAL PLAN**, including discussions on interface configurations for the following modules:

- Dual T1 / PRI (network and user terminations, for PRI and RBS)
- Dual Nx 56 / 64 (user termination)
- Quad BRI / U (network and user terminations)

In addition, a section is included on using the **DIAL PLAN** with Frame Relay (see *Connecting Packet Endpoints in Frame Relay* on page 11-28).

The **DIAL PLAN** submenus (see Figure 11-1) set global ATLAS 550 switch parameters as well as individual parameters for each ATLAS 550 port handling a switched call. The individual ports are separated into two port types: network and user. Network ports terminate a connection from the Network. User ports terminate incoming calls and, in turn may be connected to user equipment. *Network Term* on page 11-3 and *User Term* on page 11-6 provide clarification for these two port types. (See also Figure 11-2 on page 11-2 for the menu structure.)

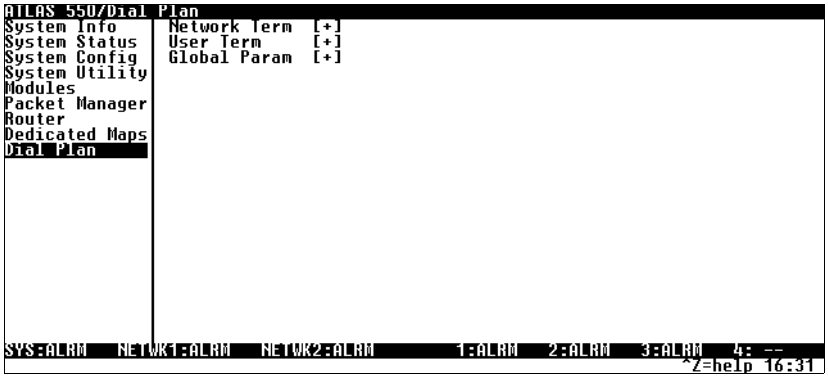


Figure 11-1. Dial Plan Menu

In the following sections, **INCOMING CALLS** *refers to calls coming to ATLAS 550 from the Network (PSTN) and* **OUTGOING CALLS** *refers to calls directed toward the Network (PSTN).*

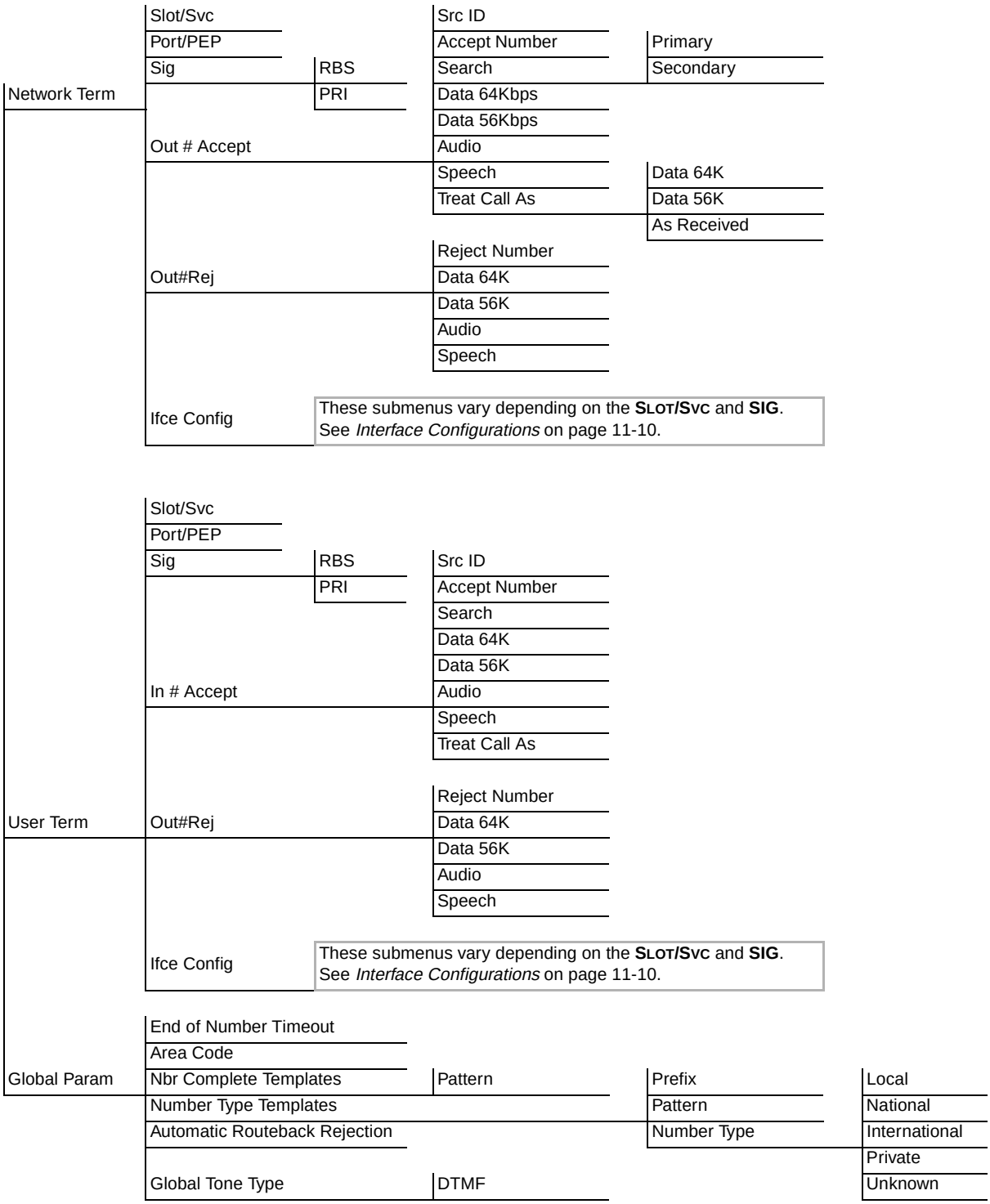


Figure 11-2. Dial Plan Menu Tree

NETWORK TERM

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

> **NOTE** *In applications where two ATLAS 550 units are used in a point-to-point configuration, a port in the ATLAS 550 at one end would act as the Network (User termination), while the ATLAS 550 at the opposite end would be terminating a "Network" connection (Network Termination).*

SLOT/SVC

Write security: 3; Read security: 5
Selects the ATLAS 550 slot that terminates a Network connection.

PORT/PEP

Write security: 3; Read security: 5
Selects the ATLAS 550 port that terminates a Network connection.

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

SIG

Write security: 3; Read security: 5
Defines the type of signaling being used for this connection (endpoint). Select **RBS** for a T1 using Robbed Bit Signaling or **PRI** for a Primary Rate ISDN interface. This selection is only necessary if a T1 / PRI is selected as the **SLOT/PORT** type.

> **NOTE** *One HDLC resource is used by each PRI or each Packet Endpoint.*

OUT#ACCEPT

Write security: 3; Read security: 5
Defines the parameters for the outgoing calls that ATLAS 550 sends to the Network.

SRC ID

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

X = Any digit 0 through 9
[1,3,5] = Any of these digits
0 = Default value

The default ID for all source endpoints all accept numbers is 0. This results in all calls being routed based on the dialed number.

ACCEPT NUMBER

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

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

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

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

SEARCH

Write security: 3 Read security: 5
Instructs ATLAS 550 in which order to search for an accept number match. Normally, all searches are set to primary. The secondary search selection forces ATLAS 550 to only accept a call at this endpoint if all primary endpoints are unavailable.

PRIMARY SEARCH

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

SECONDARY SEARCH

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

DATA 64K, DATA 56K, AUDIO, SPEECH Reflects the bearer capability the Network has provisioned for this line. If the ISDN lines were purchased with different services provisioned, then ATLAS 550 would send the call out of the port which supports the type of service the call requires.

For example, the Network termination is on a pair of BRIs (with the same phone number) with one provisioned for data and the other for voice. By enabling data in one and not the other, ATLAS 550 ensures that calls bearing data will be sent out the right BRI interface.

TREAT CALL AS Allows the incoming call to be treated as the selected call type, regardless of the actual incoming call type. The default selection, **AS RECEIVED,** effectively disables the feature by using the actual call type. Other options include **DATA 64K** and **DATA 56K**.

OUT#REJ

Write security: 3; Read security: 5
Defines the parameters for the outgoing calls that ATLAS 550 will not send to the Network.

REJECT NUMBER Identifies which numbers this endpoint will not pass on toward the Network (PSTN). The reject list may consist of multiple entries. The reject list may be used to more easily specify the call filtering desired. The wild cards are identical as in **OUT#ACCEPT** (see *Out#Accept* on page 11-3).

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

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

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

IFCE CONFIG

Sets configuration parameters for the endpoint. These parameters vary by the type of port selected. For detailed information on the interface configuration, refer to *Interface Configurations* on page 11-10.

USER TERM

This menu allows you to define option parameters for ports which terminate a connection from user equipment. In this case, ATLAS 550 is acting as the Network.

In applications where two ATLAS 550 units are used in a point-to-point configuration, a port in the ATLAS 550 at one end acts as the Network (set up as a User termination), while the ATLAS 550 at the opposite end terminates a Network connection (Network Termination).

SLOT/SVC

Write security: 3; Read security: 5
Selects the ATLAS 550 slot and port that terminate a User connection. (The user selects from a list of option modules / ports.)

PORT/PEP

Write security: 3; Read security: 5
Selects the ATLAS 550 slot that terminates a User connection.

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

SIG

Write security: 3; Read security: 5
Defines the type of signaling being used for this connection (endpoint). Select **RBS** for a T1 using Robbed Bit Signaling or **PRI** for a Primary Rate ISDN interface. You only need to set signaling if a T1 / PRI is selected as the Slot / Port type.

One HDLC resource is used by each PRI or each Packet Endpoint.

IN#ACCEPT

Write security: 3; Read security: 5
Defines the parameters for incoming calls that ATLAS 550 accepts from the Network.

SRC ID

Write security: 3 Read security: 5
Identifies the ID of the call sources from which this endpoint accepts calls. This field simplifies the creation of a **DIAL PLAN** in applications where the criterion for switching calls to a certain endpoint is a function of which end-

point originated the call. **SRC ID** may be entered with the usual wild card entries (except $).

X	=	Any digit 0 through 9
[1,3,5]	=	Any of these digits
0	=	Default value

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

ACCEPT NUMBER

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

X	=	Any single digit
N	=	Any single digit 2 through 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 endpoint. If this endpoint consisted of a T1 with multiple DS0s, a "hunt" group for 963-8000 would be formed. The entry **$** would accept any call.

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

SEARCH

Write security: 3; Read security: 5
Defines to ATLAS 550 the order in which to search for an accept number.

PRIMARY SEARCH

The **SEARCH** parameter instructs ATLAS 550 in 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 550 to only accept a call at this endpoint if all primary endpoints were unavailable.

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

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

DATA 64K, DATA 56K, AUDIO, SPEECH
Write security: 3; Read security: 5
Reflects the attached user equipment (typically a TA) bearer capability. If the attached TA can only handle digital calls, then a voice call sent to this endpoint would be rejected.

TREAT CALL AS
Allows the incoming call to be treated as the selected call type, regardless of the actual incoming call type. The default selection, **AS RECEIVED**, effectively disables the feature by using the actual call type. Other options include **DATA 64K** and **DATA 56K**.

OUT#REJ

Write security: 3; Read security: 5
Defines the parameters for outgoing calls that ATLAS 550 will not send to the Network.

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

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

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

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

IFCE CONFIG

Sets configuration parameters for the endpoint. These parameters vary by the type of port selected. For detailed information on the interface configuration, see *Interface Configurations* on page 11-10.

GLOBAL PARAM

Sets ATLAS 550 options which apply to all switched operations, both incoming and outgoing calls.

END OF NUMBER TIMEOUT

Write security: 3; Read security: 5
Sets the length of time ATLAS 550 waits before assuming the outgoing dialed number is complete. The default value is six seconds. This timeout will only be invoked if the dialed number does not match one of the patterns set in the Number Complete Template menu (see the section, *Nbr Complete Templates* on page 11-9).

AREA CODE

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

NBR COMPLETE TEMPLATES

Write security: 2; Read security: 5
Sets completed number patterns for outgoing calls so that ATLAS 550 recognizes when the phone number is complete. Fields include the index number (#) and **PATTERN**. For example, a local number will be 7 digits long while a long distance (1+ area code + number) will be 11 digits long. The ATLAS 550 defaults cover almost any installation, and these templates should not require any additional user input—except for unusual circumstances. The template allows the use of the following wild card inputs to define numbers:

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

NUMBER TYPE TEMPLATES

Write security: 2; Read security: 5
Sets call type patterns. ISDN interfaces require that a number type be sent over the D channel when a call is sent or received. A normal RBS trunk does not send a type designator, but uses prefixes instead. For example, "1 +" prefix is a national long distance call type while a "011 +" prefix is an international long distance call type. These templates form a table to permit ATLAS 550 to translate the RBS prefix into a call type for ISDN and vice-versa.

#

Denotes an entry number. The maximum number of entries is 50. Press **I** to insert a new entry and **D** to delete any entry.

The ATLAS 550 default templates should cover all applications and should not need to be added to by the user except for very rare circumstances.

PREFIX

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

PATTERN Modifies an entry when you press **Enter** (MAX 40). A pattern for a normal long distance call, for example, would be 1+(NXX) NXX - XXXX. Note that the symbols ( ), +, -, and space are not required and are only used to improve the readability of this example.

NUMBER TYPE Lists valid selections when you press **Enter**. Selections include **LOCAL**, **NATIONAL**, **INTERNATIONAL**, **PRIVATE**, and **UNKNOWN**.

AUTOMATIC ROUTEBACK REJECTION

Write security: 1; Read security: 5
When enabled, **AUTOMATIC ROUTEBACK REJECTION** prevents calls entering 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.

Use extreme caution when disabling **AUTOMATIC ROUTEBACK REJECTION**.

GLOBAL TONE TYPE

Write security: 1; Read security: 5
Specifies the dialing digit tone encoding to be used throughout the entire system. **DTMF** (dual-tone-multifrequency) is currently the only available option.

INTERFACE CONFIGURATIONS

This section describes Dial Plan **NETWORK TERMINATION** and **USER TERMINATION** configuration settings for the following modules.

- *Dual T1/PRI Module: Network Termination/PRI* on page 11-11
- *Dual T1/PRI Module: Network Termination/RBS* on page 11-14
- *Dual T1/PRI Module: User Termination/PRI* on page 11-17
- *Dual T1/PRI Module: User Termination/RBS* on page 11-20
- *Dual Nx56/64 Module: User Termination* on page 11-22
- *Quad BRI/U Module: Network Termination* on page 11-24
- *Quad BRI/U Module: User Termination* on page 11-25

Configuration descriptions for the Dual T1/PRI Module also apply to the T1 Network Interface.

DUAL T1/PRI MODULE: NETWORK TERMINATION/PRI

> **NOTE** *One HDLC resource is used by each PRI or each Packet Endpoint.*

When you are working in the network termination section of the **DIAL PLAN** menu, when **SLT** is defined as **T1/PRI-2**, and when **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 to which the port is connected. If connected to another ATLAS 550, both need to be set to the same switch type. The following options are available:

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

FIRST DS0

Write security: 3; Read security: 5
Defines to the ATLAS 550 the first DS0 for this endpoint.The ATLAS 550 uses DS0s, starting with this selection, to send and receive calls to and from the network (PSTN). The outgoing calls which are allowed or restricted over these DS0s are set by **OUT#ACCEPT** (see page 11-3) and **OUT#REJECT** (see page 11-5).

NUMBER OF DS0S

Write security: 3; Read security: 5
Specifies the number of DS0s ATLAS 550 uses for this endpoint.

OUTGOING NUMBER CONVERSION

Write security: 3; Read security: 5
Converts outgoing (towards the network) numbers to the selected numbering plan and type option.

AS DIALED Sends the digits provided as an unknown number type.

ISDN-NATIONAL PREFERRED Regardless of what type of number is received, the outgoing number is substituted with ISDN-National as the number plan and type. Ten digits are always sent to the network. Leading ones, if present, are stripped out and the area code (provisioned under **DIAL PLAN/GLOBAL PARAMETERS**) is added, if only seven digits are supplied. This action may be required in areas with ten-digit local dialing.

ISDN-SUBSCRIBER PREFERRED Examines the incoming number and if seven digits are received or if a ten-digit number is received with an area code that matches the area code provisioned in the global parameters, the number is forwarded to the network as a seven-digit number defined as ISDN-Subscriber number plan and type.

If the incoming number is ten digits, but with a different area code, it is forwarded to the network as ISDN-National preferred.

ISDN-NATIONAL DMS RESERVED PREFERRED Ignores the incoming numbering plan and type and substitutes the ISDN / Telephony numbering plan and National number type. Ten digits are sent to the network. Leading ones, if present, are stripped out and the area code set in global parameters is added if only seven digits are supplied. This action may be required in areas with ten-digit local dialing.

ISDN-NATIONAL AS DIALED Sends the digits provided as National number type.

When **SWITCH TYPE** *is set to* **4ESS**, *many installations require the National form where possible; this may also be the preferred form in 10-digit calling areas.*

STRIP MSD

Write security: 3; Read security: 5
Strips a selected quantity (choose from **NONE**, **1**, **2**, and **3**) of the Most Significant Digits (MSD) of a dialed number 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.

STRIP MSD *does not affect* **CALL ACCEPT** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criterion.*

NETWORK SPECIFIC FACILITY VOICE AND DATA

Write security: 3; Read security: 5
Enables the sending of appropriate information to the PSTN. The default for this option is **NORMAL**, and in this case no Network Specific Facility Information Element is sent. Unless one of the services listed below is subscribed to, the selection should remain set to **NORMAL**.

The list below indicates services that may be subscribed to from the PSTN. These services require that specific information (such as a Network Specific Facility Information Element) be sent to the network during call setup.

- AT&T SDN
- AT&T Megacom 800
  - AT&T Megacom
  - AT&T Accunet
- AT&T Long Distance
- AT&T International-800
- AT&T Dial-It 900 / Multiquest
- National ISDN INWATS
- Nortel Private Network
- Nortel InWats
- Nortel OutWats
- Nortel Foreign Exchange
- Nortel Tie Trunk

CALLED DIGITS TRANSFERRED

Write security: 3; Read security: 5
Some PRI switches may be provisioned to send only a portion of the called number (like DID). This menu item allows the ATLAS 550 to know how many digits to expect (choose from **NONE**, **THREE**, **FOUR**, **SEVEN**, and **ALL**). The default is **ALL** and would almost always be correct. If less than **ALL** digits are sent, then the **PREFIX** is defined as follows

PREFIX

Write security: 3; Read security: 5
Displays only if **CALLED DIGITS TRANSFERRED** is not set to **ALL**. Enter the prefix for the digits received.

Example:
If the number of digits is four and the number called is 963-8615, the telco's PRI switch sends only 8615 and the prefix is set to 963. This entire number is then used to determine which ATLAS 550 User port endpoint should receive the call.

OUTGOING CALLER ID

Write security: 3; Read security: 5
Defines the number for the ATLAS 550 to use to provide Caller ID to the Network for outgoing calls sent through this endpoint. Choose from **SEND AS PROVIDED**, **SUBSTITUTE IF NOT PRESENT**, or **SUBSTITUTE ALWAYS**.

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

SOURCE ID

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

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

Example:
An application requires that all calls that originate from Port 1 of the ATLAS 550 in Slot 1 be switched to Port 2 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 2 to only accept calls from that unique Source ID (7).

SWAP ANI/DNIS

Write security: 3; Read security: 5
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.

With this swap, the ATLAS 550 switchboard uses ANI to route the call. The accept number in the Dial Plan must use the ANI number, not the DNIS number.

DUAL T1/PRI MODULE: NETWORK TERMINATION/RBS

When you are working in the network termination section of the **DIAL PLAN** menu, when **SLT** is defined as **T1/PRI-2**, and when **SIG** is set to RBS, the following interface configuration options are available:

FIRST DS0

Write security: 3; Read security: 5
Defines to the ATLAS 550 the first DS0 for this endpoint.The ATLAS 550 uses DS0s, starting with this selection, to send and receive calls to and from the network (PSTN). The outgoing calls which are allowed or restricted over these DS0s are set by the **OUTGOING CALL ACCEPT** and **REJECT NUMBERS** (discussed in *First DS0* on page 11-11).

NUMBER OF DS0S

Write security: 3; Read security: 5
Specifies the number of DS0s the ATLAS 550 uses for this endpoint.

DS0s Available

Read security: 5
Indicates which DS0s of the T1 have been defined in this switched endpoint (indicated by "! "), in another switched endpoint (indicated by "s"), or in a **Dedicated Map** (indicated by "n"). This field is read-only. The following characters may display in this field:

- **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 **Dial Plan**.
- **S** This DS0 is in the switched dial plan 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 the ATLAS 550 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
- Loop Start
- Feature Group D
- E&M Wink
- Ground Start

The ATLAS 550 converts signaling types between network and user terminations.

FGD Tx Sequence

Write security: 3; Read security: 5
Defines to the ATLAS 550 the format in which to present the outgoing digits. Choices: **Normal** if no digits are to be sent; **ANI/DNIS** to send both ANI and DNIS; **DNIS** to send DNIS only; **ANI** to send ANI only.

FGD Rx Sequence

Write security: 3; Read security: 5
Defines to the ATLAS 550 the format in which to receive the incoming digits. Choices: **Normal** if no digits are to be received; **ANI/DNIS** to receive both ANI and DNIS; **DNIS** to receive DNIS only; **ANI** to receive ANI only.

Wink after ANI/DNIS

Write security: 3; Read security: 5
When enabled, the ATLAS 550 will transmit a wink after ANI/DNIS digits are transmitted.

DIGIT SUPPRESSION Write security 3; Read security: 5
When enabled, no digits will be sent toward the network / PBX after going off-hook on an outgoing call.

DIRECT INWARD DIALING Write security: 3; Read security: 5
Defines to the ATLAS 550 whether Direct Inward Dialing (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 550 from the network if **DID** is used. This option only displays if **DID** is set to **ENABLED**.

DID PREFIX Write security: 3; Read security: 5
Defines to the ATLAS 550 the prefix digits which are not received as a part of the DID number. The ATLAS 550 uses the combination of prefix and DID number to determine the user endpoint that should receive the incoming call. This option only displays if **DID** is set to **ENABLED**. If **DID** is **DISABLED**, then you must define the trunk number.

If Feature Group D is used, DID only refers to DNIS digits.

TRUNK NUMBER Write security: 3; Read security: 5
When the network connection does not provide DID digits, the ATLAS 550 must be given a number to use to determine which user endpoint should receive the incoming call. **TRUNK NUMBER** displays only when **DID** is set to **DISABLED**.

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

Example:
To connect an incoming DS0 (trunk) to an endpoint with the **ACCEPT** number of 963-8615, set the trunk number to 963-8615.

STRIP MSD

Write security: 3; Read security: 5
Strips a selected quantity (choose from **NONE**, **1**, **2**, and **3**) of the Most Significant Digits (MSD) of a dialed number prior to being forwarded out of the port.

Example:
A network port could be set to accept all calls beginning with 9 (9$) and **STRIP MSD** set to **1**. Then, all digits would be sent toward the network except the leading 9.

> **NOTE** **STRIP MSD** *does not affect* **CALL ACCEPT** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criterion.*

SOURCE ID

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

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

Example:
An application requires that all calls that originate from Port 1 of the ATLAS 550 in Slot 1 be switched to Port 2 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 2 to only accept calls from that unique Source ID (7).

DUAL T1/PRI MODULE: USER TERMINATION/PRI

When you are working in the user termination section of the **DIAL PLAN** menu, when **SLT** is defined as a **T1/PRI-2**, and when **SIG** is set to PRI, the following configuration options are available:

> **NOTE** *One HDLC resource is used by each PRI or each Packet Endpoint.*

SWITCH TYPE

Write security: 3; Read security: 5
Defines the type of PRI switch that the ATLAS 550 is going to emulate. If connected to another ATLAS 550, both need to be set to the same switch type.

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

FIRST DS0

Write security: 3; Read security: 5
Defines to the ATLAS 550 the first DS0 for this endpoint. The ATLAS 550 uses DS0s, starting with this selection, to send and receive calls to and from the network (PSTN). The outgoing calls which are allowed or restricted over these DS0s are set by the **OUTGOING CALL ACCEPT** and **REJECT NUMBERS** (discussed in the ATLAS 550 *User Manual*).

NUMBER OF DS0S

Write security: 3; Read security: 5
Specifies the number of DS0s ATLAS 550 uses for this endpoint.

STRIP MSD

Write security: 3; Read security: 5
Strips a selected quantity (choose from **NONE**, **1**, **2**, and **3**) of the Most Significant Digits (MSD) of a dialed number 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.

STRIP MSD *does not affect* **CALL ACCEPT** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criterion.*

NETWORK SPECIFIC FACILITY

Write: 3; Read: 5
Enables the sending of appropriate information to the PSTN. The default for this option is **NORMAL**, and in this case no Network Specific Facility information element is sent. Unless one of the services listed below is subscribed to, the selection should remain set to **NORMAL**.

The list below indicates services that may be subscribed to from the PSTN. These services require that specific information (such as a Network Specific Facility information element) be sent to the network during call setup.

- AT&T SDN
- AT&T Megacom 800
  - AT&T Megacom
  - AT&T Accunet
- AT&T Long Distance
- AT&T International-800
- AT&T Dial-It 900 / Multiquest
- National ISDN INWATS
- Nortel Private Network
- Nortel InWats
- Nortel OutWats
- Nortel Foreign Exchange
- Nortel Tie Trunk

CALLED DIGTS TRANSFERRED

Write security: 3; Read security: 5
Defines to ATLAS 550 the number of digits to forward from the called number. 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; however, this option would normally be set to **ALL**. Choose from **NONE**, **THREE**, **FOUR**, **SEVEN**, or **ALL**.

OUTGOING CALLER ID

Write security: 3; Read security: 5
Defines the number for ATLAS 550 to use to provide Caller ID to the Network for outgoing calls sent through this endpoint. Choose from **SEND AS PROVIDED**, **SUBSTITUTE IF NOT PRESENT**, and **SUBSTITUTE ALWAYS**.

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

SOURCE ID

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

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

Example:
An application requires that all calls that originate from Port 1 of the ATLAS 550 in Slot 1 be switched to Port 2 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 2 to only accept calls from that unique Source ID (7).

SWAP ANI/DNIS

Write security: 3; Read security: 5
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.

> **NOTE** *With this swap, the ATLAS 550 switchboard uses ANI to route the call. The accept number in the Dial Plan must use the ANI number, not the DNIS number.*

DUAL T1/PRI MODULE: USER TERMINATION/RBS

When you are working in the user termination section of the **DIAL PLAN** menu, when **SLT** is defined as **T1/PRI-2**, and when **SIG** is set to RBS, the following configuration options are available:

FIRST DS0

Write security: 3; Read security: 5
Defines to the ATLAS 550 the first DS0 for this endpoint. The ATLAS 550 uses DS0s, starting with this selection, to send and receive calls to and from the network (PSTN). The outgoing calls which are allowed or restricted over these DS0s are set by the **OUTGOING CALL ACCEPT** and **REJECT NUMBERS** (discussed in the ATLAS 550 *User Manual*).

NUMBER OF DS0S

Write security: 3; Read security: 5
Specifies the number of DS0s ATLAS 550 uses for this endpoint.

DS0S AVAILABLE

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

- **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 **DIAL PLAN**.
- **S** This DS0 is in the switched dial plan 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 the ATLAS 550 the type of signaling to be used across this trunk. The selected signaling must match that being used by the user equipment (PBX). The choices are as follow:

- E&M Immediate
- E&M Wink
- Loop Start
- Ground Start
- Feature Group D

The ATLAS 550 converts signaling types between network and user terminations.

FGD TX SEQUENCE

Write security: 3; Read security: 5
Defines to the ATLAS 550 the format in which to present the outgoing digits. Choices: **NORMAL** if no digits are to be sent; **ANI/DNIS** to send both ANI and DNIS; **DNIS** to send DNIS only; **ANI** to send ANI only.

FGD RX SEQUENCE

Write security: 3; Read security: 5
Defines to the ATLAS 550, the format in which to receive the incoming digits. Choices: **NORMAL** if no digits are to be received; **ANI/DNIS** to receive both ANI and DNIS; **DNIS** to receive DNIS only; **ANI** to receive ANI only.

WINK AFTER ANI/ DNIS

Write security: 3; Read security: 5
When enabled, the ATLAS 550 will transmit a wink after ANI/DNIS digits are transmitted.

DIRECT INWARD DIALING

Write security: 3; Read security: 5
Defines to the ATLAS 550 whether Direct Inward Dialing (DID) is used by the user equipment. If **DID** is **ENABLED**, then the following information must be defined:

DID DIGTS TRANSFERRED

Write security: 3; Read security: 5
Defines the number of digits the ATLAS 550 sends on to the user equipment. This field only displays if **DID** is set to **ENABLED**.

If Feature Group D is used, DID refers only to DNIS digits.

CALLER ID NUMBER

Defines the number the ATLAS 550 uses to provide caller ID to the network for outgoing calls sent through this endpoint. This option only displays if **DID** is set to **DISABLED**. This item is optional.

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

STRIP MSD

Write security: 3; Read security: 5
Strips a selected quantity (choose from **NONE**, **1**, **2**, and **3**) of the Most Significant Digits (MSD) of a dialed number 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** **STRIP MSD** *does not affect* **CALL ACCEPT** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criterion.*

SOURCE ID

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

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

Example:
An application requires that all calls that originate from Port 1 of the ATLAS 550 in Slot 1 be switched to Port 2 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 2 to only accept calls from that unique Source ID (7).

DIAL ON OFFHOOK

Write security: 3; Read security: 5
Defines a number that is automatically sent to the switchboard when a call on this endpoint goes off hook.

> **NOTE** *The Dial on Offhook number must be specific (i.e., no "wild cards").*

DUAL NX56/64 MODULE: USER TERMINATION

> **NOTE** *The Dual Nx56/64 can only serve as a* **USER TERMINATION** *endpoint.*

When you are working in the **USER TERM** section of the **DIAL PLAN** menu, and the **SLT** is defined as **V35NX-2**, the following Interface Configuration options are available:

PORTS AVAILABLE Indicates which of the two ports of the ATLAS 550 have already been defined either in another switched endpoint (indicated by **S**) or in a **DEDICATED MAP** (indicated by **N**). This field is read-only.

NUMBER OF PORTS Defines to the ATLAS 550 how many of the ports could be used to answer calls to the number(s) defined in the **INCOMING ACCEPT CALL LIST**. You can enter numbers 1 or 2. The ports are contiguous beginning with the port number selected and the number of ports.

Example:
If the port selected (as a part of the **SLOT/PORT** selection) is 2, and the number of ports selected here was 1, then only port 2 would be enabled to receive calls to the numbers listed under the **INCOMING CALL ACCEPT LIST**.

NUMBER TO DIAL Indicates the number to be dialed.

CALL TYPE Indicates whether the call will be **64K** or **56K** data rate: **56K** is intended for use in applications where interoperability with **SWITCHED 56** service is desired. **64K** is the default call type.

DIAL CALL AS Indicates how the call will be handled over the network: **DIGITAL**, **VOICE**, or **AUDIO**.

DIGITAL Requests a 56 kbps data circuit that is rate-adapted to 56 kbps or an unrestricted 64 kbps data circuit.

VOICE Requests a Mu-law / A-law speech circuit as the bearer capability for outgoing calls. Use **VOICE** with an ISDN line configured for voice service. In some areas, voice service costs less than data service. A **VOICE** call type does not guarantee an end-to-end digital connection with some local and long distance carriers.

AUDIO Requests a 3.1 kHz audio circuit as the bearer capability for outgoing calls. Use **AUDIO** with an ISDN line configured for voice service. In some areas audio service is less expensive than data service. An **AUDIO** call type guarantees a digital end-to-end ISDN connection.

SOURCE ID Simplifies the creation of a **DIAL PLAN** in applications where the criterion for switching calls to a certain endpoint is a function of which endpoint originated the call.

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

Example:
An application requires that all calls that originate from Port 1 of the ATLAS 550 in Slot 1 be switched to Port 2 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 2 to only accept calls from that unique Source ID (7).

QUAD BRI/U MODULE: NETWORK TERMINATION

The Quad BRI/U Module can interface directly with the network (PSTN). When you are working in the **NETWORK TERM** section of the **DIAL PLAN** menu, and **SLT** is defined as **U-BRI-4**, the following interface configuration options are available:

SWITCH TYPE

Write security: 3; Read security: 5
Defines the type of ISDN switch to which the port is connected. If connected to another ATLAS, both need to be set to the same switch type. Choices include **LUCENT 5E**, **NORTHERN DMS 100**, and **NATIONAL-ISDN**.

SPID LIST

Write security: 3; Read security: 5
To properly operate with a network (PSTN) ISDN switch, the BRI interface must have Service Profile Identifiers (SPIDs) and phone number(s) that match the SPID(s) and phone number(s) programmed into the ISDN switch for this line. Each BRI may have one or more phone numbers and SPIDs. The **SPID LIST** submenu defines these parameters to ATLAS.

PHONE NUMBER The phone number(s) assigned to this BRI phone line.

SPID NUMBER This entry must match the SPID number(s) which has 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 the network provisions for this SPID. If the BRI was purchased with different services provisioned for the SPIDs, then the call must match the services supported.

STRIP MSD

Write security: 3; Read security: 5
Strips a selected quantity (choose from **NONE**, **1**, **2**, and **3**) of the Most Significant Digits (MSD) of a dialed number 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.

STRIP MSD *does not affect* **CALL ACCEPT** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criterion.*

SOURCE ID

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

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

Example:
An application requires that all calls that originate from Port 1 of the ATLAS 550 in Slot 1 be switched to Port 2 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 2 to only accept calls from that unique Source ID (7).

QUAD BRI/U MODULE: USER TERMINATION

While interfacing to user equipment (terminal adapters), the ATLAS 550 acts like the network. When you are working in the **USER TERM** section of the **DIAL PLAN** menu and **SLT** is defined as **U-BRI-4**, the following interface configuration options are available:

SWITCH TYPE

Write security: 3; Read security: 5
Defines the type of ISDN switch that the port simulates. If connected to another ATLAS, both need to be set to the same type. Choices include **LUCENT 5E**, **NORTHERN DMS 100**, and **NATIONAL-ISDN**.

SPID LIST

Write security: 3; Read security: 5
The port, acting as the network, must use a SPID and a phone number in order to satisfy the ISDN connection protocol expected by the user's Terminal Adapter (TA).

PHONE NUMBER The phone number(s) assigned to this BRI phone line.

SPID NUMBER Defines the SPID number(s) 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.

The ATLAS 550 does not support autoSPID detection software which some terminal adapters offer.

CALLS For user terminations, the number of calls is fixed at **2**.

D64, D56, AUDIO, SPEECH These options reflect the network provisions for this SPID. If the BRI was purchased with different services provisioned for the SPIDs, then the call must match the services supported.

STRIP MSD Write security: 3; Read security: 5
Strips a selected quantity (choose from **NONE**, **1**, **2**, and **3**) of the Most Significant Digits (MSD) of a dialed number 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.

STRIP MSD *does not affect* **CALL ACCEPT** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criterion.*

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

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

EXAMPLE:
An application requires that all calls that originate from Port 1 of the ATLAS 550 in Slot 1 be switched to Port 2 of that same module. Assign a unique Source ID (e.g. 7) to Port 1 of the module, and then configure Port 2 to only accept calls from that unique Source ID (7).

CREATING DIAL PLANS—EXAMPLES

The ATLAS 550 **DIAL PLAN** acts as the numbering plan for switched connections. This menu defines to the ATLAS 550 the phone numbers and features associated with dual-tone-multifrequency (DTMF) dialing, Primary Rate ISDN (PRI), and Basic Rate ISDN (BRI). To operate as a switch, the ATLAS 550 must be able to terminate network connections (*Network terminations*) and emulate the network onto other termination equipment (*User terminations*).

Understanding Dial Plan Configurations

Understanding **DIAL PLAN** configurations results in the successful creation of a switched connection. This understanding includes determining which of the connections are acting as Network terminations and which are acting as User terminations. Use the following examples to help clarify the definitions for these two types of terminations.

Example 1 PSTN Connection Dial Plan Configuration

In this example, access to the PSTN is provided by a single PRI line. Therefore, this line is configured as a Network termination. The remaining circuits, which feed various types of switched equipment, are configured as User termination because ATLAS 550 is emulating the network on those connections (see Figure 11-3).

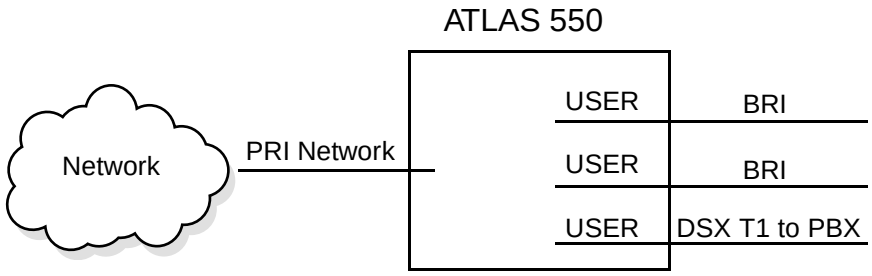


Figure 11-3. PSTN Connection

Example 2 Point-to-Point Connection Dial Plan Configuration

In this example, ATLAS 550 A operates as the network while ATLAS 550 B *terminates* the network. That is, ATLAS 550 A emulates the network and its PRI interface acts as the User termination. The PRI interface of ATLAS 550 B acts as the Network termination (see Figure 11-4).

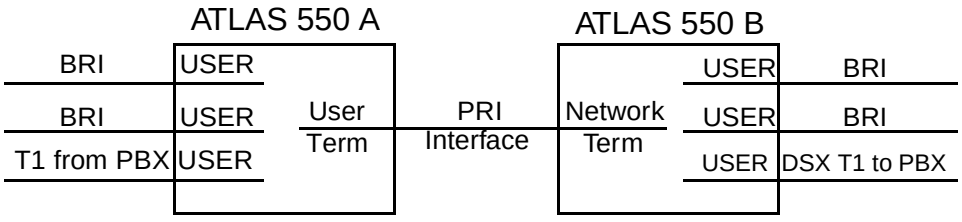


Figure 11-4. Point-to-Point Connection

CONNECTING PACKET ENDPOINTS IN FRAME RELAY

After packet endpoints are created, they must be connected to a physical port. You can connect the endpoints using either the **DEDICATED MAP** (see Chapter 10) or the **DIAL PLAN**. As described here, the **DIAL PLAN** associates a phone number with the endpoint.

You can enter two types of packet-switched endpoints into the **DIAL PLAN**: Packet Endpoints (**PKTENDPT**) and Packet Voice (**PKTVOICE**). See Figure 11-5. When using **PKTENDPT**, endpoints are entered via **USER TERM.** When using **PKTVOICE**, endpoints are entered via **NETWORK TERM** or **USER TERM**. (See also, *Menus for Network Termination* on page 11-33 and *Menus for User Termination* on page 11-34.)

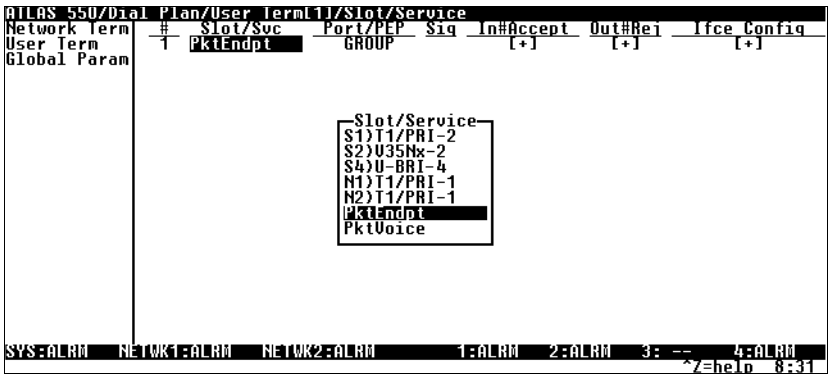


Figure 11-5. Dial Plan Menu for Endpoints

PKTENDPT

To facilitate dial-up packet services, the ATLAS 550 **DIAL PLAN** supports packet endpoints which must be entered in the **USER TERM** menu. The **USER TERM** menu includes **SLOT/SVC**, **PORT/PEP**, **SIG**, **IN#ACCEPT**, **OUT#REJ**, and **IFCE CONFIG.**

SLOT/SVC

Write security: 3; Read security: 5
Selects the service. Select **PKTENDPT**.

PORT/PEP

Write security: 3; Read security: 5
Accepts the packet endpoint you wish to configure. Select from a specific packet link that was configured with the **PACKET MANAGER** menus or select **GROUP** (see Figure 11-6). The **GROUP** option allows you to define a hunt group. The interface configuration (**IFCE CONFIG**) parameters vary, depending on whether a specific packet link (endpoint) or the **GROUP** option is selected.

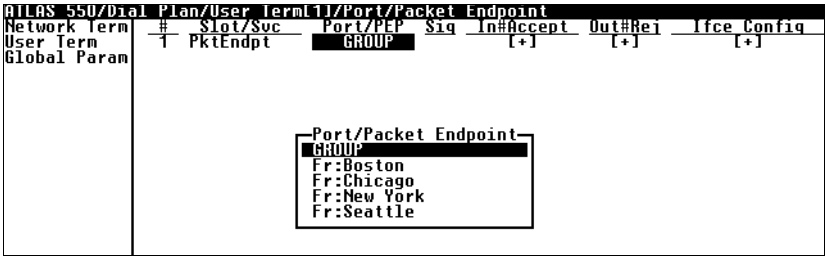


Figure 11-6. Port/PEP Menu

SIG Write security: 3; Read security: 5
Not used for specific packet links (endpoints).

IN#ACCEPT Write security: 3; Read security: 5
Configured as defined in *In#Accept* on page 11-6.

OUT#REJ Write security: 3; Read security: 5
Configured as defined in *Out#Rej* on page 11-8.

IFCE CONFIG Write security: 3; Read security: 5
Figure 11-7 shows an example of the interface configuration for a normal packet link. Figure 11-8 shows the interface configuration when the **GROUP** option is selected.

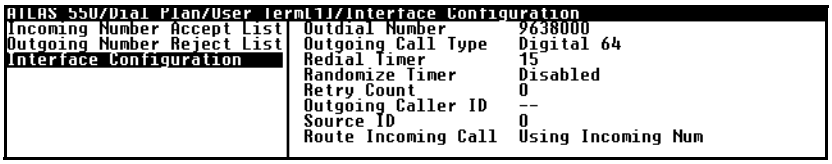


Figure 11-7. Packet Link Interface Configuration

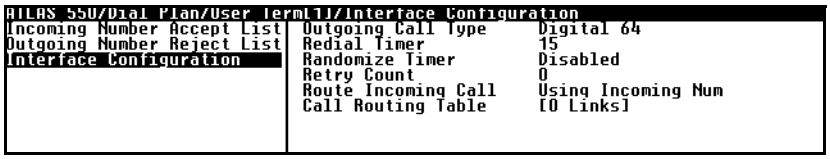


Figure 11-8. Packet Link GROUP Interface Configuration

OUTDIAL NUMBER
Write security: 3; Read security: 5
Defines the number dialed to originate a call.

OUTGOING CALL TYPE
Write security: 3; Read security: 5
Selects the terminating resource type, either **DIGITAL 64K** or **DIGITAL 56K**.

REDIAL TIMER
Write security: 3; Read security: 5
Selects the time delay in seconds between redial attempts.

RANDOMIZE TIMER
Write security: 3; Read security: 5
Enables / disables random delay added to the redial timer to avoid glare.

RETRY COUNT
Write security: 3; Read security: 5
Defines the number of redials to attempt.

OUTGOING CALLER ID
Write security: 3; Read security: 5
Defines the presentation of the calling party number for this endpoint.

SOURCE ID
Write security: 3; Read security: 5
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. For further details, see *Source ID* on page 11-14.

ROUTE INCOMING CALL
Write security: 3; Read security: 5
Used to define the method which incoming calls are associated to the packet endpoints. This item can have three options:

USING INCOMING NUM
Endpoint selection based on the incoming number.

USING CALLING PARTY NUM
Selection based on the Call ID as presented by the calling party. If this option is selected, the **CALL PARTY NUMBER** field is made available to the interface configuration. This number allows you to configure the calling part number used to select this packet endpoint.

CALL ROUTING TABLE
Read security: 5
This table is only visible if **GROUP** is selected in the **PRT/PEP** field. The table format changes, based on the selected routing option. See Figure 11-9, below and Figure 11-10 on page 31. For each case, **CALL PARAMS** contain **OUTDIAL#**, **CALLER ID,** and **SOURCE ID**.

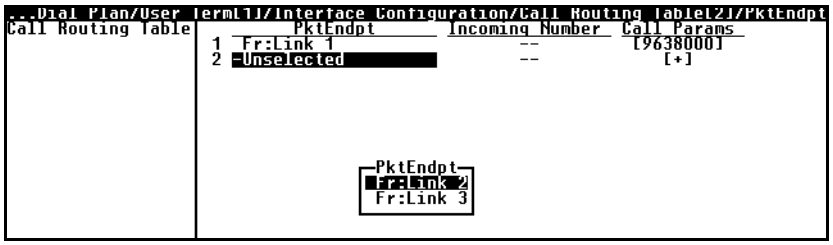


Figure 11-9. Call Routing Table for Routing Using Incoming Number

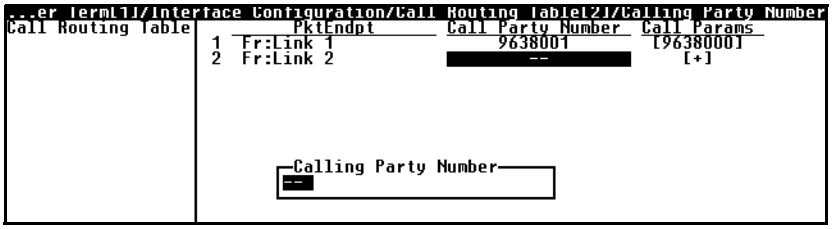


Figure 11-10. Call Routing Table for Routing Using Call Party Number

PKTVOICE

The ATLAS 550 provides the same level of capability for packet-switched voice as originally provided for circuit-switched voice.

IFCE CONFIGURATION (under **DIAL PLAN > USER TERM** or **NETWORK TERM**) sets configuration parameters for the endpoint. These parameters vary by the type of port selected. The following section describes the configuration options available for packet-switched voice (see Figure 11-11).

The first step in configuring the **DIAL PLAN** for packet voice is to select **NETWORK TERM** or **USER TERM**. Refer to *Connecting Packet Endpoints in Frame Relay* on page 11-28 for determining whether to use **NETWORK TERM** or **USER TERM**. (See also *Menus for Network Termination* on page 11-33 and *Menus for User Termination* on page 11-34.) Once this selection is made, a number of fields become available. These fields are discussed in the following sections.

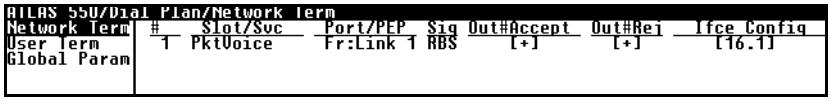


Figure 11-11. Packet Switched Voice Options

SLOT/SVC
Write Security: 3; Read Security: 5
Select **PKTVOICE** as the service.

PORT/PEP
Write Security: 3; Read Security: 5
Select the port / packet endpoint that you want to configure.

SIG
Not used for packet voice.

IN#ACCEPT
Write Security: 3; Read Security: 5
Configured as defined in *In#Accept* on page 11-6.

OUT#REJ
Write Security: 3; Read Security: 5
Configured as defined in *Out#Rej* on page 11-8.

IFCE CONFIG
Write Security: 3; Read Security: 5
Provides interface configuration parameters (see Figure 11-12).

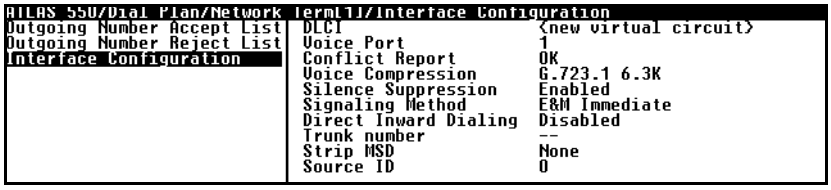


Figure 11-12. Interface Configuration (Network Termination)

DLCI

Write Security: 3; Read Security: 5
Selects the appropriate DLCI for this dial plan entry.

VOICE PORT

Write Security: 3; Read Security: 5
Identifies the voice port address of the remote unit. FSU 5622s support ports 1 and 2. A remote ATLAS supports ports 1 through 255.

CONFLICT REPORT

Read Security: 5
Provides a description of a conflict if it exists. Potential problems include DLCI unavailable or Voice port already in use.

VOICE COMPRESSION

Write Security: 3; Read Security: 5
Selects the voice compression algorithm used by this endpoint. Older ADTRAN 5622 FRADs use CCITT G.723.1 compression at 6.3 kbps. Newer FRADs also support the proprietary NETCODER algorithm at 6.4 kbps. Both endpoints must agree about the compression algorithm choice.

SILENCE SUPPRESSION

Write Security: 3; Read Security: 5
Reduces the total system bandwidth load by preventing ATLAS from sending frames containing a special silence code during periods of silence. Both endpoints must agree to use silence suppression. By default, silence suppression is **DISABLED**. To prohibit silence frames from transmitting and to decrease the total system bandwidth, **ENABLE** this feature.

SIGNALING METHOD

Write Security: 3; Read Security: 5
Selects the type of signaling that the remote port is configured to expect. Available options include the following: **E&M IMMEDIATE**, **E&M WINK**, **LOOP START**, and **FEATURE GROUP D**.

DIRECT INWARD DIALING

Write Security: 3; Read Security: 5
Defines whether or not Direct Inward Dialing (DID) is used by the remote equipment. If DID is enabled, then the following options must be configured for **NETWORK** and **USER TERM** configurations.

Menus for Network Termination

DID DIGITS TRANSFERRED Write Security: 3; Read Security: 5
Defines the number of digits sent to the ATLAS 550 from the Network if **DIRECT INWARD DIALING** (see page 11-32) is enabled.

DID PREFIX Write Security: 3; Read Security: 5
Defines to the ATLAS 550 the prefix digits which are not received as a part of the DID number. The ATLAS 550 uses the combination of prefix and DID number to determine the user endpoint that should receive the incoming call. This field only displays if **DIRECT INWARD DIALING** is enabled.

TRUNK NUMBER Write Security: 3; Read Security: 5
Determines which user endpoint should receive the incoming call when the network connection does not provide DID digits. This field only displays if **DIRECT INWARD DIALING** (see page 11-32) is set to Disabled, and **NETWORK TERM** (see page 11-33) is selected.

STRIP MSD Write Security: 3; Read Security: 5
Strips a selected quantity (choose from **NONE**, **1**, **2**, and **3**) of the Most Significant Digits (MSD) of a dialed number prior to being forwarded out of the port.

Example:
A network port could be set to accept all calls beginning with 9 (9$) and **STRIP MSD** set to **1**. Then, all digits would be sent toward the network except the leading 9.

STRIP MSD *does not affect* **CALL ACCEPT** *criteria. All of the digits (including the MSDs that are subsequently stripped) are used as accept criterion.*

SOURCE ID Write Security: 3; Read Security: 5
Defines the source ID. Setting this menu item is optional.

Menus for User Termination

DID DIGITS TRANSFERRED
Write Security: 3; Read Security: 5
Defines the number of digits the ATLAS 550 is to send to the user equipment. This field only displays if **DIRECT INWARD DIALING** (see page 11-32) is enabled.

CALLER ID NUMBER
Write Security: 3; Read Security: 5
Defines the number ATLAS uses to provide caller ID to the network for outgoing calls sent through this endpoint. This field only displays if **DIRECT INWARD DIALING** (see page 11-32) is set to **DISABLED**, and **USER TERM** is selected. Setting this menu item is optional.

SOURCE ID
Write Security: 3; Read Security: 5
Defines the source ID. Setting this menu item is optional.

Chapter 12 Updating Firmware

OVERVIEW

To provide feature enhancements in the future, ATLAS 550 supports firmware updating by field personnel. Two transfer methods are available for use in updating any modules that contain Flash memory, including the ATLAS 550 system controller. The first transfer method is via the ATLAS 550 Control / Chain In port using XMODEM protocol. The second transfer method is via the ATLAS 550 built-in Ethernet port using TFTP (Trivial File Transfer Protocol). To simplify the update procedure, a common menu interface is available for updating any upgradable module within the ATLAS 550 (see also *Update Firmware* on page 6-17). The following sections describe the procedure for updating using either transfer method.

Please consult the appropriate ATLAS 550 module manual to determine if the module supports Flash upgrading.

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

XMODEM FIRMWARE UPDATES

The ATLAS 550 supports firmware updating to any upgradable module using XMODEM transfer protocol via the base unit's Control / Chain In port. XMODEM is found in most PC communications software packages. To configure the Chain In port's data rate and other communication parameters, consult *Control/Chain In Port* on page 2-4 and *Control/Chain Out Port* on page 2-5.

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

Updating Firmware using XMODEM

Before beginning this procedure,

- you must have a level 1 password for updating any module within ATLAS 550. Please consult the ATLAS 550 administrator if you do not know the password.
- you must obtain the appropriate update file for the particular module from the ADTRAN web page, www.adtran.com, in the Support section.
- you may want to review *Update Firmware* on page 6-17.

Instructions for Updating Firmware Using XMODEM

Step	Action
1	Using a VT-100 terminal emulation communication software package which contains XMODEM protocol support, **log in** to ATLAS 550.
2	Select **SYSTEM UTILITY / UPDATE FIRMWARE** (see Figure 12-1). ATLAS 550/System Utility/Update Firmware/Module Slot Update Firmware — Module Slot — Slot 0 Update Status — Module Type — Sys Ctrl Config Transfer — Transfer Method — XMODEM System Utilization — Restart Schedule — Restart Immediately after Update System Selftest — Current Update Status — Idle Ping — Previous Update Status — Has not been attempted Begin Firmware Update — <+> **Figure 12-1. Update Firmware Menu Interface**
3	Move the cursor to **MODULE SLOT**, and press **Enter**. Select the appropriate module slot to update. To update multiple modules of the same type, select **ALL MODULES OF A TYPE** from **MODULE SLOT**. (Only upgradable modules are displayed as choices for **MODULE TYPE** when updating **ALL MODULES OF A TYPE** in the ATLAS 550.)
4	Select **XMODEM** for **TRANSFER METHOD**.
5	From **RESTART SCHEDULE**, select the time for the module to perform a restart after completing the update process (see *Restart Schedule* on page 6-18).
6	View **CURRENT UPDATE STATUS** to verify the progress of the current firmware update or any errors encountered during the download process (see *Current Update Status* on page 6-19).
7	Select **BEGIN FIRMWARE UPDATE** to start the update process. Enter **Y** to confirm the transfer and to set up the module to receive the XMODEM upload. *When* ATLAS 550 *is ready to receive the XMODEM upload, the menu screen will clear and display* **Awaiting XMODEM Upload…… <CTRL-X> to Cancel**. *If this does not appear, please review the steps above for possible configuration errors.*

Instructions for Updating Firmware Using XMODEM (Continued)	
Step	**Action**
8	From the terminal emulation software, begin the XMODEM upload by using the appropriate command sequence. (If necessary, refer to your terminal emulation software documentation for help. Also, when specifying the filename, ensure that the file transferred is the one provided by ADTRAN; otherwise, the update will not complete successfully.) Because XMODEM data is being transferred in-band through the menu interface, the VT-100 menus of ATLAS 550 will be inoperable from the Control/Chain In port. You can cancel the update at any time within the terminal emulation software. (Please consult the documentation provided by the terminal emulation software to determine how to do this.)
9	To update additional modules, begin at step 3 and repeat this process.

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

If an error occurred during the update process, **PREVIOUS UPDATE STATUS** displays an appropriate error message.

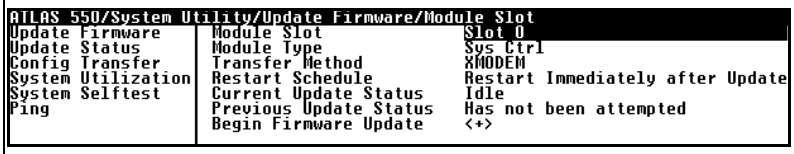
TFTP FIRMWARE UPDATES

ATLAS 550 supports firmware updates to any module via the Ethernet port using TFTP from a network server. The network server must be capable of supporting TFTP Server requests from the TFTP client within ATLAS 550.

Updating Firmware using TFTP

Before beginning this procedure,

- you must have a level 1 password to perform updates of any modules within ATLAS 550. Please consult the ATLAS 550 administrator if this password is not known.
- you must obtain the appropriate update file for the particular module from the ADTRAN web page, www.adtran.com, in the support section.
- you must copy the update file provided by ADTRAN to a network server that supports TFTP Server requests. Record both the IP address of the server and the full path location of the update file to be downloaded.

Instructions for Updating Firmware Usin g TFTP	
Step	**Action**
1	Using a Telnet program, **log in** to ATLAS 550.
2	Select **SYSTEM UTILITY / UPDATE FIRMWARE** (see Figure 12-2).  **Figure 12-2. Update Firmware Menu Interface**
3	Move the cursor to **MODULE SLOT**, and press **Enter**. Select the appropriate module slot to update. To update multiple modules of the same type, select **ALL MODULES OF A TYPE** from **MODULE SLOT**. (Only upgradable modules are displayed as choices for **MODULE TYPE** when updating **ALL MODULES OF A TYPE** in the ATLAS 550.)
4	Select **TFTP** for the **TRANSFER METHOD**.
5	Enter into **TFTP SERVER IP ADDRESS**, the IP address of the network server that was recorded earlier.
6	Enter into **TFTP SERVER FILENAME**, the full path name and filename of the update file that was recorded earlier.
7	From **RESTART SCHEDULE**, select the time for the module to perform a restart after completing the update process (see *Restart Schedule* on page 6-18).
8	View **CURRENT UPDATE STATUS** to verify the progress of the current firmware update or any errors encountered during the download process (see *Current Update Status* on page 6-19).
9	Select **BEGIN FIRMWARE UPDATE** to start the update process. Enter **Y** to confirm the transfer and to set up the module to receive the TFTP upload.
10	To update additional modules, begin at step 3 and repeat this process.

Status Messages During Upload

During the TFTP upload process, various status messages display in Current Update Status to indicate progress. Table 12-1 describes these messages.

Table 12-1. TFTP Upload Messages

Message	Meaning
Contacting Server	Indicates communication with the TFTP Network Server is trying to be established with the specified server address in the TFTP Server IP Address field.
Beginning TFTP Transfer	Indicates communication with the TFTP Network Server has been established and the update file is being transferred between ATLAS 550 and the TFTP Network Server.
Completed	Indicates the ATLAS 550 product successfully received the update file.
Error: File Not Found	Indicates the TFTP Network Server was unable to locate the specified file name or path in the TFTP Server Filename field.
Error: Access Violation	Indicates the TFTP Network Server denied ATLAS 550 access to the given update file name and path. Please verify appropriate user rights are selected for the specified path.
Error: Illegal Operation	An unknown operation was detected by ATLAS 550 when transferring the update file from the TFTP Network Server.
Error: User Aborted	Indicates the user selected Cancel Update to abort reception of the update file from the TFTP Network Server.

Complete Upload

When the update process has successfully completed, **IDLE** displays in **CURRENT UPDATE STATUS**, and **MODULE UPDATE COMPLETE** displays in **PREVIOUS UPDATE STATUS**. Either the module restarts immediately and resumes operation, or it restarts at the specified time and day of the week—depending on your selection.

Incomplete Upload

If an error occurred during the update process, **PREVIOUS UPDATE STATUS** displays the appropriate error message (see Tabl e12-1). In this case, return to step 3 and attempt the update process again. If the same error occurs, contact ADTRAN Technical Support.

Chapter 13 SNMP Management

SNMP OVERVIEW

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

SNMP BASIC COMPONENTS

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

Network Manager

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

Agent

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

MIB

The MIB is an index to the organized data stored within a network device. The MIB defines the operating parameters that can be controlled or monitored. When the MIB requests the network manager to retrieve or modify a particular piece of information about a network device, the network manager transmits that request to the network device. The **agent** in that device in-

terprets the incoming request, performs the requested task, and sends its response to the network manager. The network manager collects all of the data from the various network devices and presents it in a consistent form.

SNMP TRAPS

An SNMP trap is a message sent by a network device, such as the ATLAS 550, to report an operational anomaly or an alarm condition.

Trap Destination List

A trap destination list contains information about sites designated to receive SNMP traps. You can configure this list via a Telnet session or the VT-100 terminal menu. The ATLAS 550 supports up to four trap destination lists. By default, the destination list is empty.

Configuring a Trap Destination List via the Terminal Menu

To configure the trap destination list from the terminal menu, select **SYSTEM CONFIG/SNMP/TRAPS DESTINATION**. Enter the information similarly to that shown in Figure 13-1. See also *Traps Destination* on page 6-11.

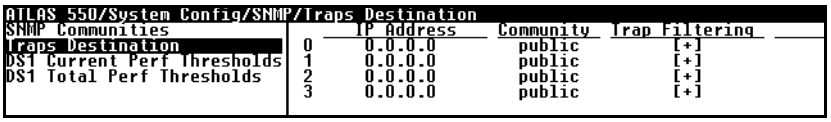


Figure 13-1. Traps Destination List

- *IP Address* is the address of the network management station to which the ATLAS 550 sends the trap.
- *Community* is the trap community name used for the selected network device.
- *Trap Filtering* is a record allowing you to assign thresholds to each category of the ATLAS 550 events.

Disabling Trap Generating Events

You can disable trap generating events in three ways:

1. Disable **TRAP TRANSMISSION.** From the terminal menu, select **SNMP** and set **TRAP TRANSMISSION** to **DISABLED.**

OR

2. Define trap thresholds to disable specific trap events. Refer to the ATLAS 550 MIB in *System Event Logging* on page A-1 for a description of each trap event supported by the ATLAS 550.

   For example, consider the *coldStart* trap which is a system controller event. If you defined for destination 0, a trap filtering threshold of **WARNING** for the system controller, then the *coldStart* trap would not generate to that destination because the *coldStart* trap severity level is defined as **NORMAL**.

   (Recall that each trap event has a severity level: **DISABLED, INFORMATIONAL, NORMAL, WARNING, MINOR, MAJOR,** and **CRITICAL**.)

OR

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

Standard Traps

RFC1213, or MIB II, defines the object type *snmpEnabledAuthenTraps.* If you set this value to *2*, the generation of the *authenticationFailure* trap is disabled. This trap is enabled by setting *snmpEnableAuthenTraps* to *1*. One possible reason for an authentication failure would be an invalid community name in the received protocol message. Table 13-1 describes the standard traps supported by ATLAS 550.

Table 13-1. Standard SNMP Traps

Index	Trap Name	Severity	Description
0	coldStart	Normal	ATLAS 550 is such that its configuration may be altered; this trap is generated on power up.
1	warmStart	Normal	ATLAS 550 is reinitializing without altering its configuration.
2	linkDown	Warning	One of the ATLAS 550 communication links has failed.
3	linkUp	Normal	One of the ATLAS 550 communication links has come up.
4	authenticationFailure	Informational	ATLAS 550 has received a protocol message that has failed authentication.

DS1 Traps

The ATLAS 550 supports RFC1406, the DS1 standard MIB, as well as the ADTRAN DS1 MIB, an extension to RFC1406. The ADTRAN DS1 group allows you to send traps for DS1 alarm failures (DS1 alarm traps) and performance threshold crossing alerts (DS1 alert traps).

DS1 Alarm Traps

The ADTRAN DS1 extension MIB contains a DS1 Alarm Table which holds entries that enable status bits to send an alarm trap. Each Alarm Table row entry corresponds to a DS1 interface managed by the device. DS1 line status is reported in the bit-encoded *dsx1LineStatus* object variable. Each trap represents a bit value equal to 1 change in the *dsx1LineStatus*. Table 13-2 describes the DS1 alarm traps supported by the ATLAS 550.

When enabled, the ATLAS 550 sends alarm traps to the each member of the trap destination list upon detecting status bit changes in *dsx1LineStatus*. Each status change sets an event bit = 1 in the *adDS1LineEvent* variable in the DS1 alarm table. If you have previously set the corresponding enable bit in the *adDS1LineArm* variable equal to one and if *adDS1AlarmEnable = On*, then the ATLAS 550 sends an alarm trap message. A single alarm trap message may report multiple event changes.

Clearing DS1 Alarm Traps

The ATLAS 550 clears the event bits after sending the trap message or sending the response to a *Get* request for the *adDS1LineEvent* variable.

Table 13-2. DS1 SNMP Alarm Traps

Alarm	Severity	Description
adATLAS550NoAlarm	Warning	No alarms are present.
adATLAS550RxYellow	Minor	The Far End is experiencing Red Alarm (a.k.a. Yellow Alarm).
adATLAS550TxYellow	Warning	The Near End is sending Loss Frame Indication (a.k.a. Yellow Alarm).
adATLAS550RxAIS	Minor	The Far End is sending Alarm Indication Signal (a.k.a. Blue Alarm).
adATLAS550TxAIS	Warning	The Near End is sending Alarm Indication Signal (a.k.a. Blue Alarm).
adATLAS550RedAlarm	Major	The Near End is experiencing Loss of Frame (a.k.a. Red Alarm).
adATLAS550LOS	Major	The Near End is experiencing Loss of Signal.

DS1 Alert Traps

The ADTRAN DS1 extension MIB contains the DS1 Alert Table which holds entries that enable event bits to send an alert trap. Each Alert Table row entry corresponds to a DS1 interface managed by the device. A single alert trap may report multiple event changes.

RFC1406 also defines a series of *Current* and *Total Alert* threshold values. You can enable the ATLAS 550 to send an Alert Trap to each member of the trap destination list when accumulated error statistics exceed these

threshold values. Table 13-3 describes the Alert Traps supported by the ATLAS 550 for events that have occurred in the last 15-minute interval, and Table 13-4 on page 13-6 describes the events occurring in the last 24-hour interval.

Current Alert SNMP Traps

When one of the current alert thresholds is exceeded, the corresponding event bit is set to 1 in the DS1 alert table variable, *adDS1CurrentAlert*. When enabled, the ATLAS 550 sends alert traps to each member of the trap destination list upon detecting the status bit changes in *adDS1CurrentAlert*.

If you have previously set the corresponding event bit in the variable, *adDS1CurrentArm*, equal to one and *adDS1AlertEnable* = *On*, then the ATLAS 550 sends an alert trap message.

Table 13-3. DS1 SNMP Current Alert Traps

Current Alert	Severity	Description
adATLAS550CurrentES	Warning	The current interval errored second threshold has been exceeded.
adATLAS550CurrentSES	Warning	The current interval severely errored second threshold has been exceeded.
adATLAS550CurrentSEFS	Warning	The current interval severely errored framing second threshold has been exceeded.
adATLAS550CurrentUAS	Major	The current interval is unavailable.
adATLAS550CurrentCSS	Warning	The current interval path code violations have been exceeded.
adATLAS550CurrentLES	Warning	The current interval line errored second threshold has been exceeded.
adATLAS550CurrentCV	Warning	The current interval line code violation threshold has been exceeded.

Total Alert SNMP Traps

When one of the total alert thresholds is exceeded, the DS1 alert table's corresponding event bit is set to 1 in the *adDS1TotalAlert* variable. If enabled, the ATLAS 550 then sends alert traps to each member of the trap destination list upon detecting status bit changes in *adDS1TotalAlert*.

If you have previously set the corresponding enable bi tequal to one in the *adDS1TotalArm* variable and *adDS1AlertEnable* = *On*, then the ATLAS 550 sends an alarm trap message.

Table 13-4. Total Alert Traps

Total Alert	Severity	Description
adATLAS550TotalES	Warning	The total interval errored second threshold has been exceeded.
adATLAS550TotalSES	Warning	The total interval severely errored second threshold has been exceeded.
adATLAS550TotalSEFS	Warning	The total interval severely errored framing second threshold has been exceeded.
adATLAS550TotalUAS	Major	The total interval unavailable second threshold has been exceeded.
adATLAS550TotalCSS	Warning	The total interval controlled slip second threshold has been exceeded.
adATLAS550TotalPCV	Warning	The total interval path code violations have been exceeded.
adATLAS550TotalLES	Warning	The total interval line errored second threshold has been exceeded.
adATLAS550TotalLCV	Warning	The total interval line code violation threshold has been exceeded.

Clearing DS1 Alert Traps

The ATLAS 550 clears the event bits after sending the alert trap or a response to a *Get* request for the *adDS1CurrentAlert* variable. The ATLAS 550 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.

Far End Alert Traps

Current alert and total alert traps are *near end* events; however, the ATLAS 550 also supports current alert and total alert traps for the *far end*. Far end alert traps are generated upon event bit changes in *adDS1FarCurrentAlert* (for current alerts) and in *adDS1FarTotalAlert* (for total alerts).

Clearing Far End Alert Traps

Current and total far end alert traps can be disabled by setting the corresponding enable bit equal to zero in the *adDS1FarCurrentArm* and the *adDS1FarTotalArm* variables, respectively.

Far end alert traps can also be disabled by setting *adDS1AlertEnable* = *Off*.

Chapter 14 ADTRAN Utilities

OVERVIEW

ADTRAN delivers several PC software utilities along with the ATLA S550. These utilities are located on the three diskettes that came with your shipment. They also include MIB files (located in the MIB directory).

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

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

SYSLOG HOST DAEMON

The SysLog Host Daemon allows remote monitoring, collecting, and logging of ATLAS 550 events in realtime. This information can be useful during installation setups and / or troubleshooting.

To use this utility, you must configure the remote ATLAS 550 (using a Telnet or VT-100 connection) with destination IP address of the PC to which you want to transmit SysLog messages; i.e., the IP address of the PC running the SysLog host utility.

SysLog GUI

Figure 14-1 shows the SysLog Host GUI. The conventional Menu Bar is described beginning on page 14-3 (see also Figure 14-2 on page 14-3). Other features are described here.

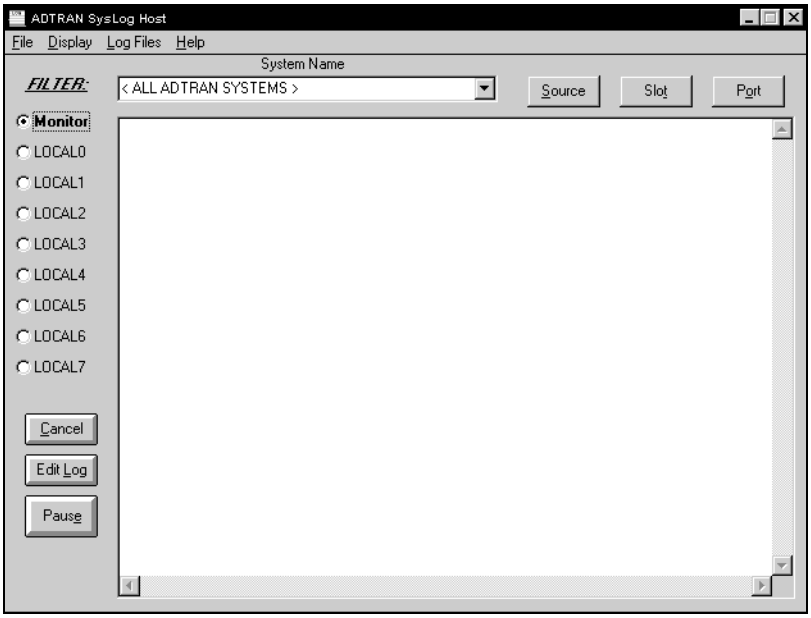


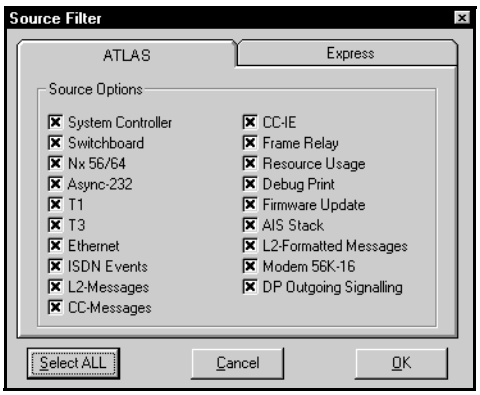
Figure 14-1. ATLAS 550 SysLog Host GUI

Monitor

The **MONITOR** feature allows all SysLog messages to be pre-filtered by **SYSTEM NAME, SOURCE, SLOT** and **PORT** before displaying these messages to the user and logging the message to the pre-designated monitor log file.

System Name — Select from pull-down menu.

Source — Provides various filter options for the ATLAS 550.



Slot — Select applicable slots (0—4).

Port — Select applicable port range.

Menu Bar

The SysLog Menu Bar provides common functions. The menu tree shown in Figure 14-2 shows the structure.

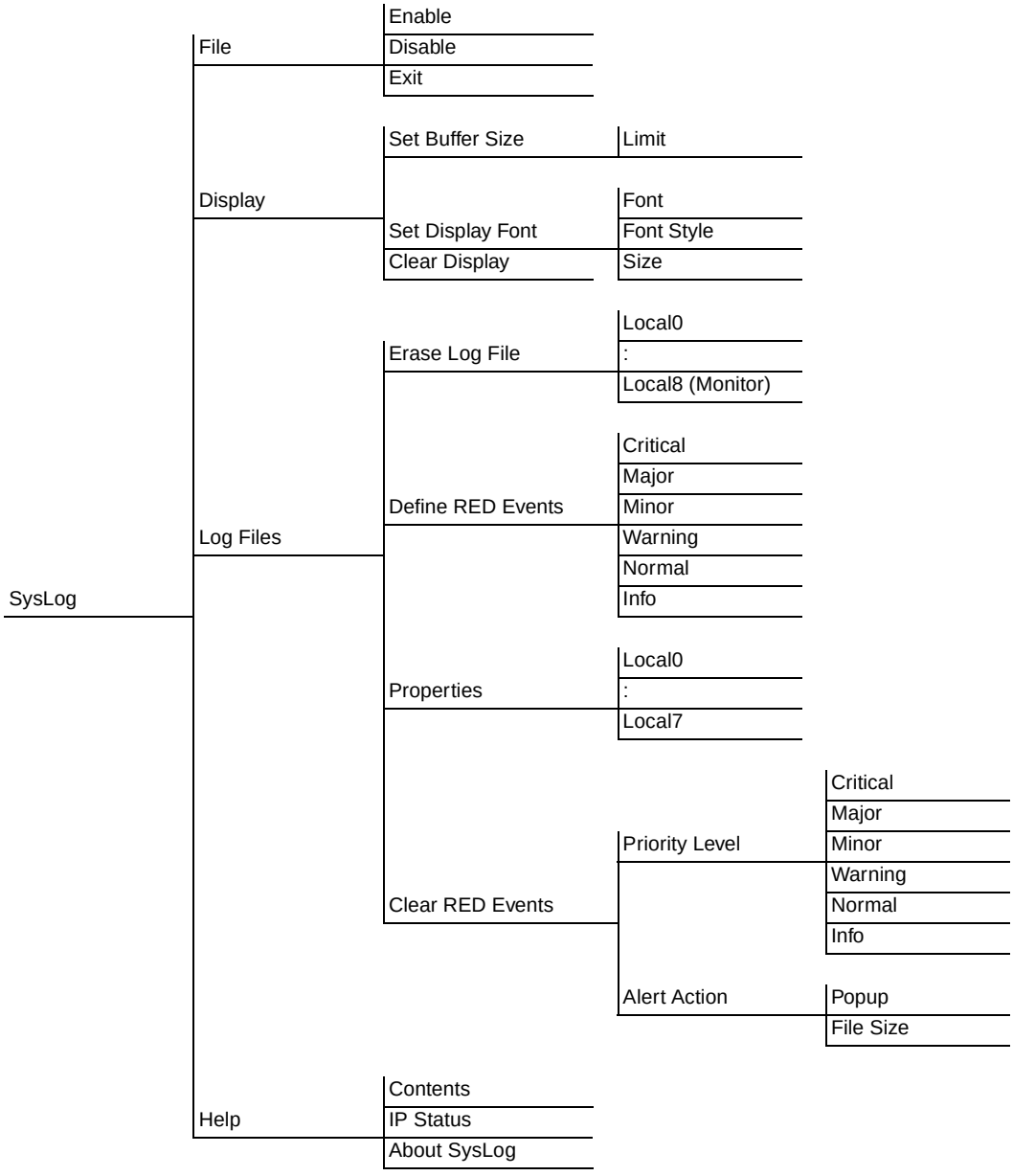


Figure 14-2. SysLog Menu Tree for the Menu Bar

FILE

Enables, disables, and exits the SysLog Host program.

DISPLAY

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

LOG FILES

Erases log files, defines Red events, sets priorities and action to be taken when an event occurs, and clears Red events. (See *Define RED Events* in the following paragraphs.)

ERASE LOG FILES

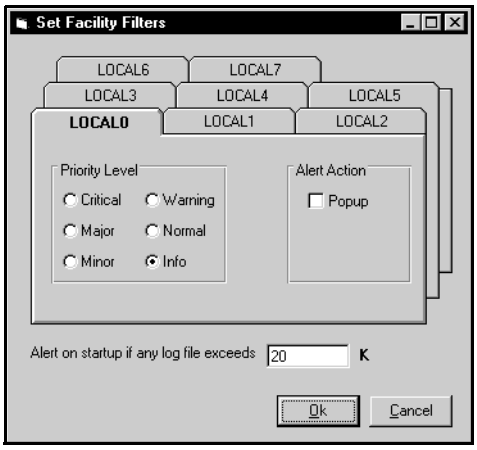
The SysLog utility, by default, stores all messages of a certain priority in a specified local log file or facility. These files are named LOCAL0.txt, LOCAL1.txt, LOCAL2.TXT, and so on. To erase the file, click on this menu.

DEFINE RED EVENTS

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

PROPERTIES

When you click on **PROPERTIES**, the **SET FACILITY FILTERS** dialog box opens, allowing you to specify what types of messages will be logged to an ASCII text file. In the example shown here, all SysLog event messages of **NORMAL** and above (i.e., **CRITICAL, MAJOR, MINOR** and **WARNING**) will be logged. **INFO** (debug) messages will be blocked. In this example, if the log file exceeds 20K, SysLog alerts the user on startup to this fact. Also, from this box, you can set the alert action.



CLEAR RED EVENTS

Click this item to clear all predefined RED events.

HELP

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

TELNET UTILITY

The Telnet utility delivered with the ATLAS 550 provides enhancements to standard Telnet programs that make it easier to work with ATLAS 550 options.

Access the Telnet program remotely through the Ethernet port. For a detailed description of how to work with the Telnet program, refer to *Navigating the Terminal Menus* on page 5-1. For a detailed description of the Telnet interface, see Figure 5-1 on page 5-1. If you need help setting up the ATLAS 550 for a Telnet session, refer to *Using The Terminal Menus* on page 3-1.

The Telnet menus include **SESSION**, **EDIT**, **OPTIONS**, **CAPTURE**, and **HELP** (see the menu tree in Figure 14-3).

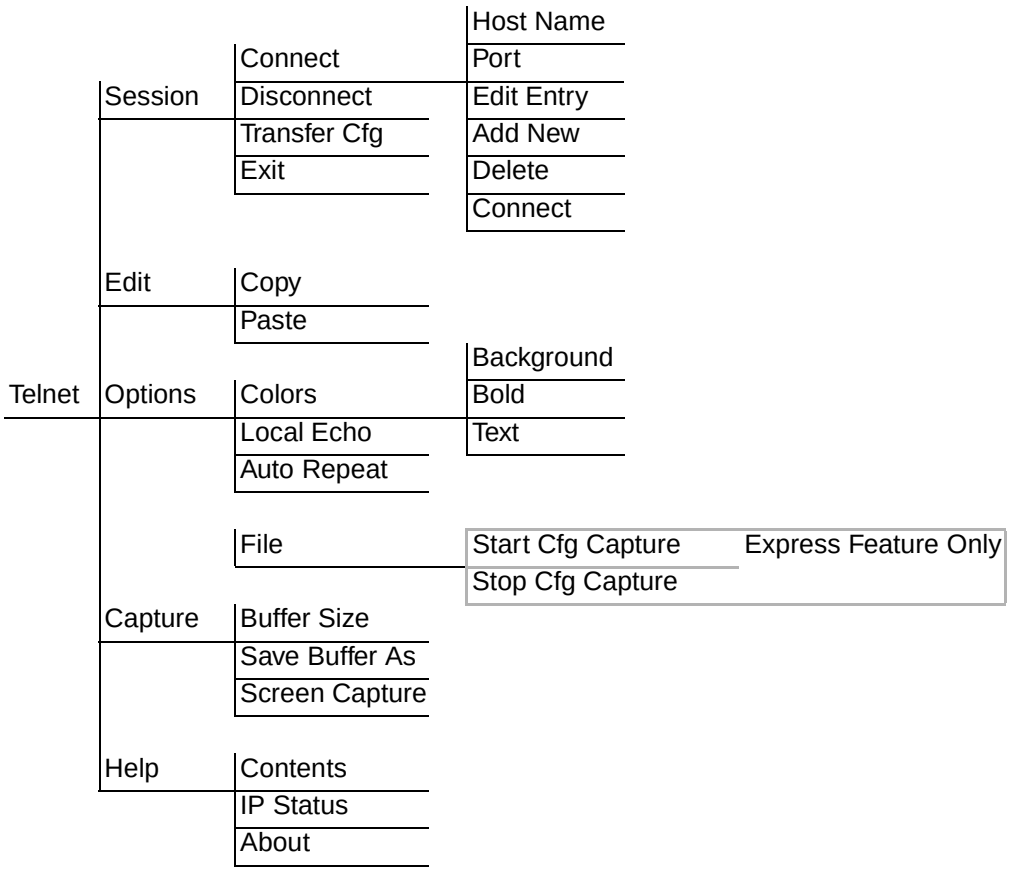
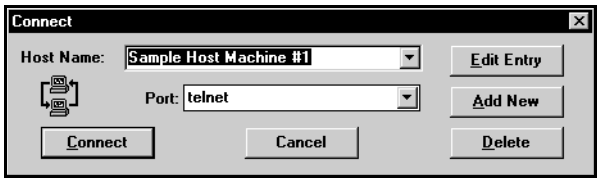


Figure 14-3. Telnet Menu Tree

SESSION

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

CONNECT



Opens dialog box for setting **HOST NAME** and **PORT** parameters for a Telnet session. Also lets you **EDIT ENTRY**, **ADD NEW** entry, and **DELETE** stored entries. When the parameters are set, click **CONNECT** to make the connection. Click **CANCEL** to end the session.

HOST NAME

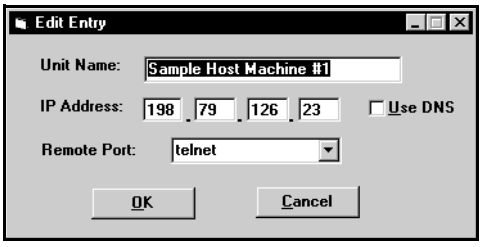
Accepts and stores host names. You may either enter a name, an IP address, or a domain name directly from this field. Click on the drop-down arrow to display a complete list of previously stored host names.

PORT

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

TELNET	Establishes a Telnet session
ECHO	Provides a loopback for troubleshooting
DISCARD	Bit bucket; discards data
DAYTIME	Returns the time
CHARGEN	Displays as a unique character stream; used for self-tests

EDIT ENTRY



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

ADD NEW

Prompts you for the same information as the **EDIT ENTRY** dialog box for new host. When enabled, the **USE DNS** (Domain Name Server) feature allows users to request **DOMAIN LOOK UP** via a DNS server on the network, rather than specifying an IP address. The name then appears in the **HOST NAME** field.

DELETE

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

CONNECT

Establishes the Telnet session.

DISCONNECT Terminates the Telnet session. To re-establish the session, select **CONNECT** from **SESSION MENU** or press **Enter** three times. This action restores the previous connection.

TRANSFER CFG This feature is used with Express products primarily for sending configuration files to the unit.

EXIT Ends the Telnet session and closes the Telnet screen.

EDIT

Provides **COPY** and **PASTE** commands.

OPTIONS

Provides viewing alternatives for the terminal screen.

COLORS Three options change the color of the background window (**BACKGROUND**), bold highlights (**BOLD**), and text (**TEXT**).

LOCAL ECHO Echoes each character that you enter.

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

CAPTURE

Provides options for capturing screen images.

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

- **START CFG CAPTURE** Used with the Express product line to start sending the scrolling screen capture to a file storage location.
- **STOP CFG CAPTURE** Used with the Express product line to stop sending the scrolling screen capture to a file storage location.

BUFFER SIZE Disables terminal window scroll bars when set to zero. (This is the normal setting for ATLAS 550.) This number represents the number of lines to capture in the memory buffer.

SAVE BUFFER AS Save screen capture to a file.

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

HELP Provides on-line help for using the ADTRAN Utilities.

CONTENTS Opens the on-line help.

IP STATUS Displays the local port address and the status of the connection.

ABOUT Displays version and owner information.

VT-100 UTILITY

Use the VT-100 to configure an ATLAS 550 which is directly connected to a PC. The VT-100 display is almost identical to the Telnet display. If you need help setting up the ATLAS 550 for a VT-100 session, refer to *Using VT-100 Terminal Emulation* on page 3-1. VT-100 menus include **SESSION**, **EDIT**, **PORT**, **OPTIONS**, **CAPTURE**, and **HELP** (see the menu tree in Figure 14-4).

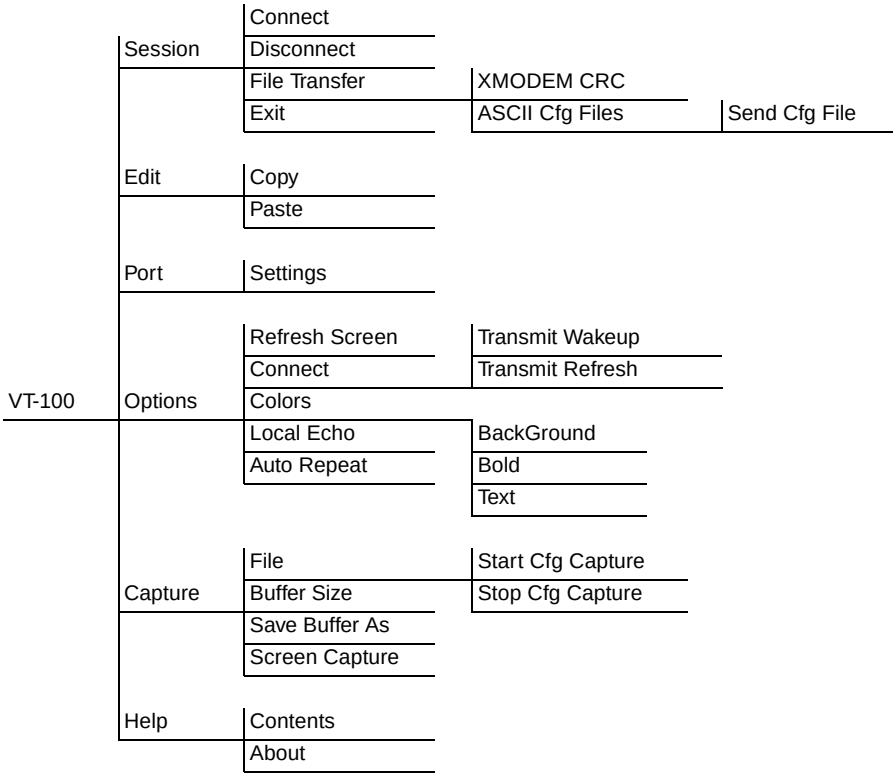


Figure 14-4. VT-100 Menu Tree

SESSION Opens VT-100 terminal emulation session.

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

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

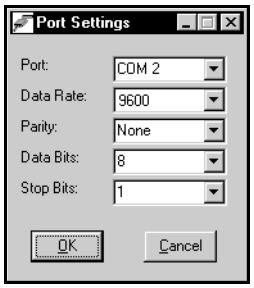
FILE TRANSFER Uploads and downloads files to and from an ATLA S550.

XMODEM CRC Selects the XMODEM file transfer protocol.

ASCII CFG FILES Selects ASCII transfer mode. Primarily used for configuration transfers for the Express products.

EDIT Identical to the Telnet **EDIT** menu (see *Edit* on page 14-7).

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



OPTIONS Provides terminal screen commands.

REFRESH SCREEN Redraws the screen.

CONNECT Provides the options **TRANSMIT WAKEUP** and **TRANSMIT REFRESH**.

TRANSMIT WAKEUP Provides a control sequence that puts the ATLAS 550 Control Port online in terminal mode.

TRANSMIT REFRESH Provides a control sequence to automatically refresh the screen when connecting. (This is the default setting for the ATLAS 550.)

COLORS Identical to the Telnet **COLORS** menu (see *Colors* on page 14-7).

LOCAL ECHO Echoes each character that you enter.

AUTOREPEAT Repeats characters you select from the keyboard if you hold down the key.

CAPTURE Identical to the Telnet **CAPTURE** menu (see *Capture* on page 14-7).

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

CONTENTS Opens on-line help.

ABOUT Displays version and owner information.

TFTP SERVER UTILITY

The TFTP Server utility transfers ATLAS 550 configuration files to and from a TFTP Server (see Figure 14-5 on page 14-11). You can install this program on a PC running any version of Microsoft Windows. The configuration of an ATLAS 550 can be saved offline as a backup file. The saved file may also be used to send the same configuration to multiple ATLAS 550 units. Transfer configuration files using the TFTP protocol (a TCP/IP user protocol) via the Ethernet port. The ATLAS 550 must have a valid IP address, subnet mask, and default gateway (if required), and be connected to an Ethernet network before proceeding. Figure 14-6 on page 14-11 shows the TFTP Server interface.

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

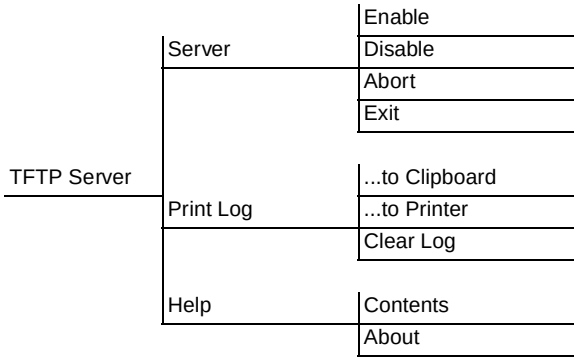


Figure 14-5. TFTP Server Interface Menu Tree

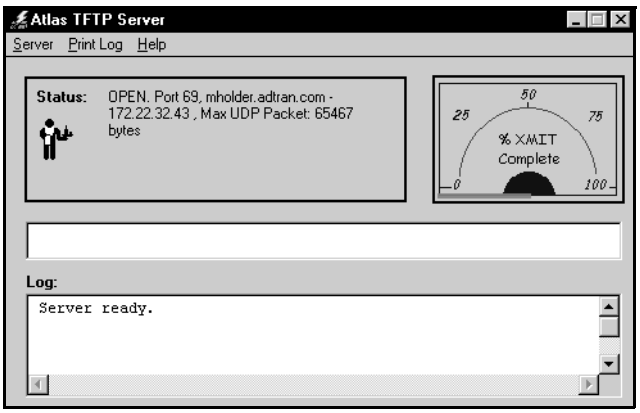


Figure 14-6. TFTP Server Interface

Only one configuration transfer session (upload or download) may be active at a time. The TCP / IP parameters are not saved or overwritten as part of an ATLAS 550 unit's transferred configuration to allow sending identical configurations to multiple units. When you start this program, a port is automatically opened.

SERVER

Provides **ENABLE**, **DISABLE**, **ABORT**, and **EXIT** options.

ENABLE

Enables the TFTP Server. The IP address displays in the **STATUS** field and "Server Ready" displays in the Log field.

DISABLE

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

ABORT

Terminates a transfer that is in progress.

EXIT Terminates active transfers and closes the TFTP window.

PRINT LOG Provides print options.

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

...TO PRINTER Sends the information in the Log field to the default printer.

CLEAR LOG Deletes the information stored in the Log field.

HELP Provides on-line help and version information.

CONTENTS Opens on-line help.

ABOUT Displays version and owner information.

STATUS FIELD

This field displays general information about port and transfer status. This field is read-only. The unlabeled field in the center of the screen displays prompts about the status of active transfers, such as bytes transferred and received.

METER FIELD

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

LOG FIELD

This field displays a record of all of the events that occur during the time the TFTP Server is enabled. Use the scroll bar to move up and down the list. To clear the information in this field, from the **PRINT LOG** menu, select **CLEAR LOG**. Save this information to a file before deleting it with the **...TO CLIPBOARD** command.

Saving the Current Configuration to a TFTP Server

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

- A level 3 or better password is required for a configuration download—the same level required to modify most configuration parameters. Please consult the ATLAS 550 administrator if level 3 access is not available.
- Some TFTP Servers constrain filename formats. For example, a TFTP Server running on a PC under any platform may only permit 8.3 format filenames (8 characters, period, and three extension characters).

To save the current configuration, follow these steps:

Instructions for Saving the Current Configuration

Step	Action
1	Use Telnet and **log in** to the ATLAS 550 for which you want to save the configuration file.
2	Select the **SYSTEM UTILITY** menu, then the **CONFIG TRANSFER** menu.
3	Set the TFTP Server IP Address to the IP address of the machine running the TFTP Server program. (If you are using the ADTRAN TFTP Server, the IP address displays in the Status field.)
4	Change the TFTP Server filename to a unique filename for saving the configuration file to the remote server. (Enter the complete directory path to the file.)
5	Move to the **SAVE CONFIG REMOTELY** button and press **Enter**. Press **Y** to confirm the transfer request.

Successful Transfer

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

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

Unsuccessful Transfer

There are various reasons why a configuration download may fail. For example, the server may not allow the specific filename to be created or overwritten, the specified directory path may not be valid, or there may not be

sufficient disk space on the remote server for the new file (although configuration files are not normally large). A specific error message displays when the transfer is unsuccessful.

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

Retrieving the Configuration from a TFTP Server

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

Also, a level 3 or better password is required for performing a configuration upload. Please consult the ATLA S550 administrator if level 3 access is not available.

Instructions for Retrieving a Configuration from TFTP Server	
Step	**Action**
1	Use Telnet to **log in** to the ATLAS 550 to which you want to upload a configuration file.
2	Select the **SYSTEM UTILITY** menu, then the **CONFIG TRANSFER** menu.
3	Set the TFTP Server IP Address to the IP address of the machine running the TFTP Server program. (If you are using the ADTRAN TFTP Server, the IP address displays in the Status field.)
4	Change the TFTP Server filename to the filename of a previously saved configuration you wish to load. (Enter the complete directory path to the file.)
5	Move to the **LOAD AND USE CONFIG** button and press **Enter** to proceed with the transfer. Respond with **Y** to confirm the transfer request.

The ATLAS 550 reboots immediately after a configuration successfully loads. No additional confirmation is requested, and any online sessions are terminated.

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

Appendix A System Event Logging

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

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

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

Table A-1. System Event

Event	Category	Console Log String
-24 V power supply is functioning normally again	Critical	"-24 V Power Failure Cleared"
-24 V power supply is not operating properly	Critical	"-24 V Power Failure"
-58 V power supply is functioning normally again	Critical	"-58 V Power Failure Cleared"
-58 V power supply is not operating properly	Critical	"-58 V Power Failure"
ACO switch pressed	Minor	ACO Switch pressed
Alarm detected on External Alarm Monitor	Minor	External Alarm Detected
ATLAS configuration file loaded into the system and activated	Critical	System Configuration Uploaded
Console login failure[a]	Minor	Login Failure
Corrupted firmware	Critical	Firmware invalid
External alarm cleared	Minor	External Alarm Cleared
Flash download failed	Critical	Firmware update failed
Flash download successful	Info	Firmware update completed
Internal system temperature has cooled below 70^{o} C	Critical	>70 Internal Temperature Warning Cleared
Internal system temperature has cooled below 85^{o} C	Critical	>85 Internal Temperature Warning Cleared
Internal system temperature is greater than 70^{o} C	Critical	>70C Internal Temperature Warning
Internal system temperature is greater than 85^{o} C	Critical	>85C Internal Temperature Warning
Module found	Info	Module Found
Module removed or not responding	Warning	Module Not Responding
Neither the primary nor the backup are valid	Minor	Timing source changed to Internal
SNMP authentication failure[b]	Info	SNMP Authentication Failure
System cold start[c]	Normal	Cold
The primary source is not Backup valid	Minor	Timing source changed to Backup
The timing source changed to primary	Minor	Timing source changed to Primary
Unable to program module	Minor	Not responding to programming

a. Three consecutive login attempts were attempted and failed.

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

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

Table A-2. Switchboard Events

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

a. No such number in dial plan.

b. Number is on outgoing reject list.

c. All endpoints busy.

Table A-3. Nx 56/64 Events

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

Table A-4. T1 Events

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

Table A-4. T1 Events (Continued)

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

Table A-5. Ethernet Events

Event	Category	Console Log String
Not enough memory for Ethernet driver	Critical	Out of memory

Table A-6. ISDN Events

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

Table A-6. ISDN Events (Continued)

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

ISDN CAUSE CODES

In addition to the above events, certain recognized ISDN cause codes are sent to the event log from the ISDN message facility. Table A-7 lists the codes applicable to the ATLAS 550 and the minimum category required for logging the cause code event.

Table A-7. ISDN Cause Code Events

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

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

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

CAUSE CODE LOG ENTRIES

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

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

The coding standard field is one of the following: Reserved, National, or Local. Each Cause Code IE log entry ends with a location designation. Table A-8 on page A-9 shows these designations.

Table A-8. Cause Code Log Entry Location Designations

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

Table A-9. ISDN L2 Messages

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

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

Table A-10. ISDN Call Control Messages

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

Table A-11. Source: ISDN Information Elements

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

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

Appendix B OSI Model and Frame Relay Technology Overview

This chapter discusses the OSI Model, Frame Relay Protocol, and Transparent Bit Oriented Protocol (TBOP).

OSI MODEL

The Open Systems Interconnection (OSI) model is an internationally accepted standard for communication between multiple vendors' communication equipment. It relies on a seven-layer model to allow communication between communication equipment. Table B-1 describes these layers.

Table B-1. Seven-Layer OSI Model

Layer	Title	Description
Layer 7	Application	Contains functions for end-user services. These include FTP, remote file access, and network management. This is not the application, but the interface.
Layer 6	Presentation	Provides transparent communication by creating code and syntax compatibility between systems.
Layer 5	Session	Takes care of the communication facility provided by the transport layer (layer 4). Allows sessions to be established, recovered, and terminated.
Layer 4	Transport	Provides some error correction and end-to-end flow control. Also decides best route for the information being transmitted.
Layer 3	Network	Determines the method for transmitting data and also deals with routing the data between networks. Moves data based on addressing.
Layer 2	Data Link	Deals with procedures and protocols for controlling the transmission line. Provides some error detection and correction.
Layer 1	Physical	Deals with the electrical, mechanical, and functional control of sending data over the transmission lines.

By defining standard interfaces between each of the seven layers, an individual layer only has to know about the interface to the layer above, to the layer below, and to the same layer on the other end of the network. This interface definition simplifies the process of networking.

The Router and Frame Relay software in ATLAS involves layer 3 and layer 2 data processing. The OSI model is not limited to digital data networks, but can be extended to such networks as the U.S. Postal Service. The examples below should clarify the roles of the first three layers and how they interface with each other. Example 1 relates the OSI model to the process of mailing a letter.

Example 1: OSI Model Related to Process of Mailing a Letter

Upper Layers		Letters and Advertisements
Layer 3	Network	Envelopes and Boxes
Layer 2	Data Link	Mailbags
Layer 1	Physical	Planes and Trucks

Send Process		**Receive Process**
Person A writes a letter.	Upper Layers	Person B reads the letter.
Person A places the letter in an envelope, addresses it to person B, and puts envelope in mailbox.	Layer 3	Person B opens envelope and removes the letter.
The envelope is collected from mailbox and placed into a mailbag destined for post office B.	Layer 2	The mailbag is opened and the envelope is placed in person B's post office box.
A truck takes the mailbag and drives to post office B.	Layer 1 Roads and Interstates	The truck delivers the mailbag to post office B.

Since the postal service specifies how mail is transferred between layers, the person addressing the letter only needs to know the address of the person receiving the letter to pass the letter down to the next layer. The letter writer has no knowledge of the details of mailbags and moving letters between post offices, but knows to place the letter in the mailbox so that the post office delivers the letter to the reader. The lower layers have no knowledge of the letter, but take responsibility for getting it to the appropriate location.

Example 2: OSI Model Related to Process of Moving Data Packet

A more typical example of the OSI model involves moving a data packet across an IP network.

Upper Layers	E-mail message
Layer 3	Network - IP/IPX
Layer 2	Data Link - Frame Relay/PPP
Layer 1	Physical - T1/DDS

Send Process		Receive Process
Creates a data packet.	Upper Layers	Data packet is processed.
Wraps the data in an IP packet, specifies the IP address of the far end computer, and determines the appropriate route.	Layer 3	The IP wrapper is removed and the data is then passed to the upper layers.
The IP packet is placed inside a frame relay packet with the appropriate DLCI and placed on the correct DS-1.	Layer 2	The frame packet is unwrapped and the IP packet is sent to layer 3.
The frame relay packet is placed in the appropriate DS0s.	Layer 1 LEC and IXC	The frame relay packet is removed and passed to layer 2.

FRAME RELAY

Frame relay is one of several layer 2 (data link) protocols that transport data across a serial data network. These protocols also include Point-to-Point Protocol (PPP) and High-level Data Link Connection Protocol (HDLC). Frame relay networks are composed of virtual circuits that connect customer locations. To reduce a customer's overall monthly connection, multiple virtual circuits could be delivered to the customer's location over a single physical connection.

Virtual Circuits

Virtual circuits can be either permanent (PVC) or switched (SVC). PVC bandwidths are determined when the circuit is ordered from the frame relay provider. PVCs are always active, even when no data is being transmitted. SVC bandwidths are created and used only when needed and allow for ne-

gotiation of the bandwidth parameters during the circuit setup. SVCs are currently unavailable from most frame relay providers, and ATLAS only supports PVCs.

PVC Physical Connections

Figure B-1 illustrates three PVCs being delivered over one physical circuit. The frame relay switch within the frame relay provider's circuit makes a physical connection for each PVC. Each of the PVCs could connect to a different physical location at the other end of the circuit. Figure B-2 illustrates a frame relay network topology.

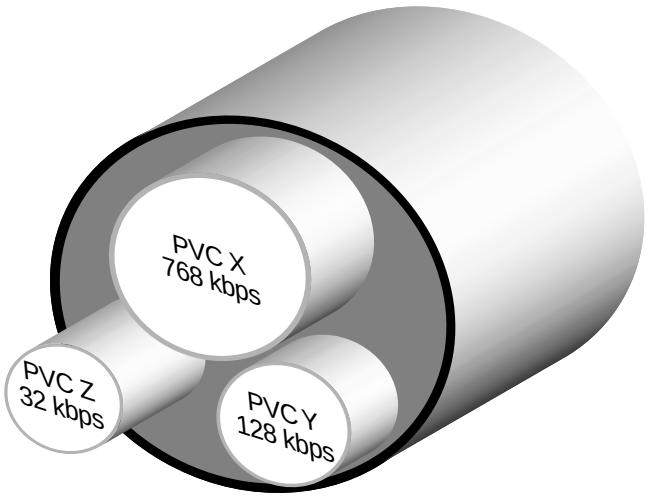


Figure B-1. Three Virtual Circuits in One Physical Circuit

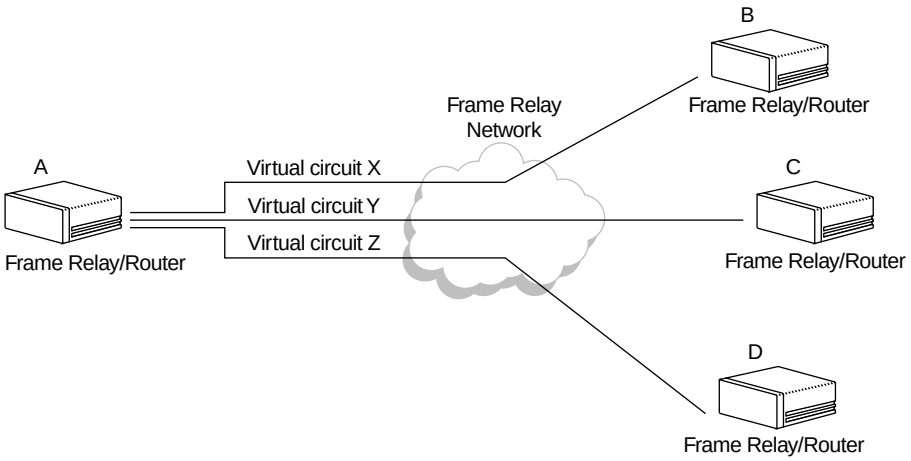


Figure B-2. Frame Relay Network using Virtual Circuits

Data Link Connection Identifier (DLCI)

An address called a Data Link Connection Identifier (DLCI) uniquely identifies each of the virtual circuits in the frame relay network. A DLCI does not address the equipment at the far end of the virtual circuit, but addresses the next piece of frame relay equipment within the network. The next piece of frame relay equipment now becomes responsible for transporting all frames from the incoming port to the appropriate outgoing port.

Figure B-3 illustrates a network using DLCI assignments. In this example, the router at site A sends a frame packet to site B, by placing the data on DLCI 100. Knowing that all packets coming in DLCI 100 must go out DLCI 225, Frame Relay Switch A places the packets on DLCI 225 and sends them out to Frame Relay Switch B. Frame Relay Switch B then takes the frame packets from DLCI 225 and places them on DLCI 35 for delivery to the site B router. From this example, you can see that each piece of frame relay equipment only knows about the DLCIs local to it. Hence, you will hear "DLCIs only have local significance."

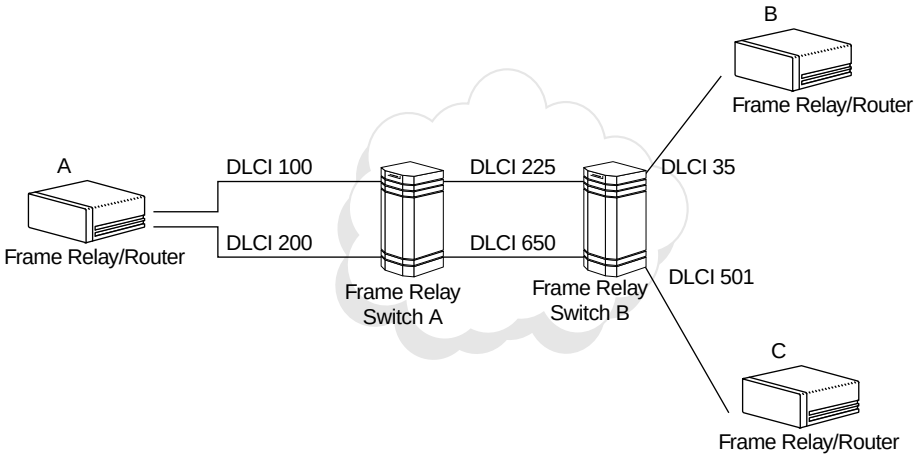


Figure B-3. Network Using DLCI Assignments

User-to-Network Interface

The interface between the customer and the frame relay switch is called the User-to-Network Interface (UNI). Three different types of signaling can transmit across this interface: LMI (Group of Four), Annex A (ITU-T Q.933-A), and Annex D (ANSI T1.617-D). Unfortunately, due to signaling differences among the three types, they are incompatible with one another, and DLCI assignments vary among the three types. Table B-2 on page B-6 and Table B-3 on page B-6 give the assignments for the three types.

Local Management Interface (LMI)

LMI is the standard published by the Frame Relay Consortium in 1990 to create a defined interface on the UNI. The Consortium, composed of Cisco

Systems, DEC, Nortel, and StrataCom, is commonly referred to as the Group of Four.

Table B-2. LMI (Group of Four) DLCI Assignments

DLCI	Use
0	Call control signaling channel.
1-15	Reserved for future use.
16-1007	Available for customer data.
1008-1022	Reserved for future use.
1023	LMI channel.

Annex A and Annex D

The International Telecommunications Union Telecommunication Standardization Sector (ITU-T) adopted Annex A as the interface standard for international frame relay applications. The American National Standards Institute (ANSI) modified the Frame Relay Consortium's interface specification and ratified it as Annex D—an interface standard for the United States.

Table B-3. Annex A and Annex D DLCI Assignments

DLCI	Use
0	Carries frame relay signaling (LMI channel).
1-15	Reserved for future use.
16-991	Available for customer data.
992-1007	Management DLCIs for layer 2.
1008-1022	Reserved for future use.
1023	Higher layer protocol communication channel.

Committed Information Rate (CIR)

Customers can order a circuit with a guaranteed amount of bandwidth for their virtual connections. This amount is called the Committed Information Rate (CIR), and it defines how much bandwidth the customer is guaranteed during normal network operation. Any data transmitted above this purchased rate is discard eligible (DE) by the network. That is, this data can be discarded in the event of network congestion.

The CIR can be thought of as the size of the virtual connection from end to end. The CIR can be purchased in different increments up to the wire speed of the slowest link. For example, if the circuit in Figure B-3 had T1 access from site A to the frame relay network and a 56-kbps DDS line from site B to

the frame relay network, the largest CIR available for purchase would be 56k. Although data could burst from site A to the frame relay network at the full T1 speed of 1.536 Mbps, it would queue up in the frame relay network until it could be sent across the 56-kbps DDS circuit. This queue could cause network congestion.

Managing Network Congestion

If congestion becomes a problem within the network due to excessive data being delivered from one of the sites, the frame relay switch attempts to flow control the data by sending bits that notify network devices that transmissions in the opposite direction are congested. These bits are called Backward Explicit Congestion Notification (BECN) and Forward Explicit Congestion Notification (FECN).

For example, if a frame relay switch begins to experience congestion, it sends the upstream site a FECN and the downstream site a BECN. This notification indicates to the frame relay equipment that the frame relay switch is experiencing difficulty and that the frame relay device should begin to flow control its traffic.

Figure B-4 shows an example of FECN and BECN messages being transmitted to the frame relay equipment when congestion occurs. Both ends are notified that congestion is occurring within the switch. You might wonder why the receiving end should receive notification of congestion and then flow control its data when the other end is causing the problem by sending large amounts of data. Flow control is used by the receiving end so that upper layer acknowledgments from the destination slow down, thereby reducing the amount of data being transmitted from the source.

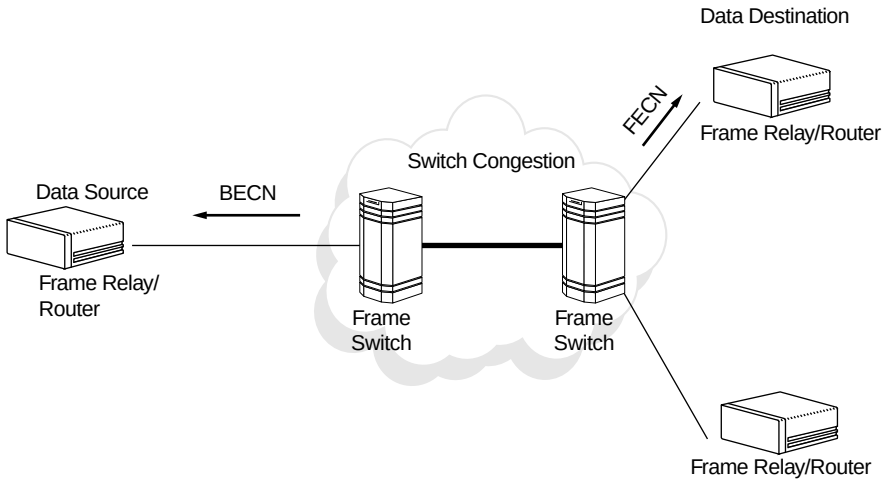


Figure B-4. Network Congestion and Flow Control

This overview is not intended to be all inclusive of the operation of a frame relay network. It is intended to help simplify the frame relay configuration within the ATLAS 550.

TBOP

Transparent Bit Oriented Protocol (TBOP) is an ADTRAN-proprietary protocol that is used to transmit HDLC-formatted traffic across the frame relay network. TBOP allows the transportation of protocols "unknown" to the ATLAS 550 to be encapsulated in frame relay and sent to a remote location via frame relay. This protocol can be useful in transporting other vendors' proprietary protocols across the WAN.

The ATLAS 550 accepts HDLC-formatted data on one of the V.35 or T1 ports and forwards that data across a frame relay network to another ATLAS or an ADTRAN frame relay device (for instance, if the ATLAS 550 is communicating with an IQ product).

Appendix C Frame Relay Examples

This chapter provides step-by-step examples to help you configure your ATLAS 550 for frame relay. Figure C-1 illustrates an ATLAS 550 configured to support packet data.

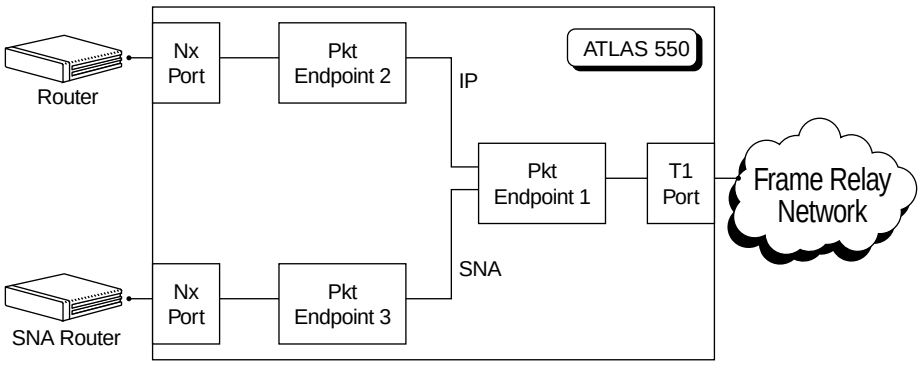


Figure C-1. ATLAS to Support Packet Data Configuration

The general procedure for configuring the ATLAS 550 depicted in Figure C-1 is as follows:

1. From **PACKET MANAGER** / **PACKET ENDPNTS** / **CONFIG**, create three packet endpoints.
2. From **PACKET MANAGER** / **PACKET CNCTS**, make the IP and SNA protocol connections.

From **DEDICATED MAP**, connect the packet endpoints to the physical ports.

EXAMPLE 1: IP ROUTING NETWORK—ATLAS 550 AS THE CENTRAL-SITE ROUTER

Example 1 (see Figure C-2 on page C-2) depicts a typical IP routing network using an ATLAS 550 as the central-site router. A TSU 100e with a router module is located at each of the two remote sites, and an FSU with an external router is located at a third site. The central-site ATLAS 550 terminates a full T1 frame relay connection from the XYZ service provider, and the internal router terminates the IP traffic. To re-create this example, follow the process that follows.

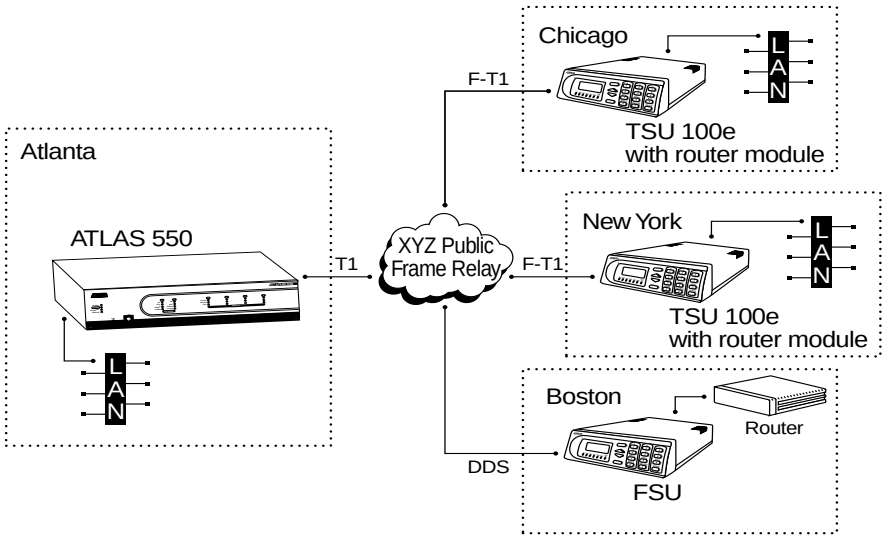


Figure C-2. IP Routing Network with ATLAS 550 as the Central-Site Router

Step 1 From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG**, create the packet endpoint (see Figure C-3).

```
ATLAS 550/Packet Manager/Packet Endpnts/Config
Status          Endpnt Name      Protocol    Config Sublinks  Usage
Performance   1 Example 1        Frame Relay [+]    [+]       -------
Config
Test
```

Figure C-3. Menu for Creating Packet Endpoints

Step 2 From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG/SUBLINKS**, create three sublinks or DLCIs for frame relay (see Figure C-4).

```
ATLAS 550/Packet Manager/Packet Endpnts/Config[1]/Sublinks
Config          Name          DLCI    QOS    Burst   Config
Sublinks      1 Boston        101     64     0       [+]
              2 Chicago       102     384    0       [+]
              3 New York      103     384    0       [+]
```

Figure C-4. Menu for Creating Sublinks or DLCIs

Step 3 From **PACKET MANAGER/PACKET CNCTS**, connect the IP traffic to the internal router (see Figure C-5).

```
ATLAS 550/Packet Manager/Packet Cncts
Packet Endpnts    FROM: PEP   Sublink    TO: PEP    Sublink    Protocol  Config
Packet Cncts    1 Fr:Exampl   Boston     Router     Not used   IP        N/A
Frame Relay IQ  2 Fr:Exampl   Chicago    Router     Not used   IP        N/A
                3 Fr:Exampl   New York   Router     Not used   IP        N/A
```

Figure C-5. Menu for Connecting IP Traffic to Internal Router

Step 4 From **DEDICATED MAPS/CREATE/EDIT MAPS/CONNECTS**, attach the packet endpoint to the appropriate physical interface (see Figure C-6).

Figure C-6. Menu for Attaching Packet Endpoint to Physical Interface

Example 2: IP Routing Network—External Routers

Example 2 (see Figure C-7) depicts an IP network with external routers. An ATLAS 550 is located at the central site. A TSU 100e with an external router connected to an Nx56/64 module is located at each of two remote sites, and an FSU with an external router is located at the third remote site. At the central site, ATLAS 550 terminates a full T1 frame relay connection from the XYZ service provider and switches the PVCs to the external router. To re-create this example, follow the process discussed below.

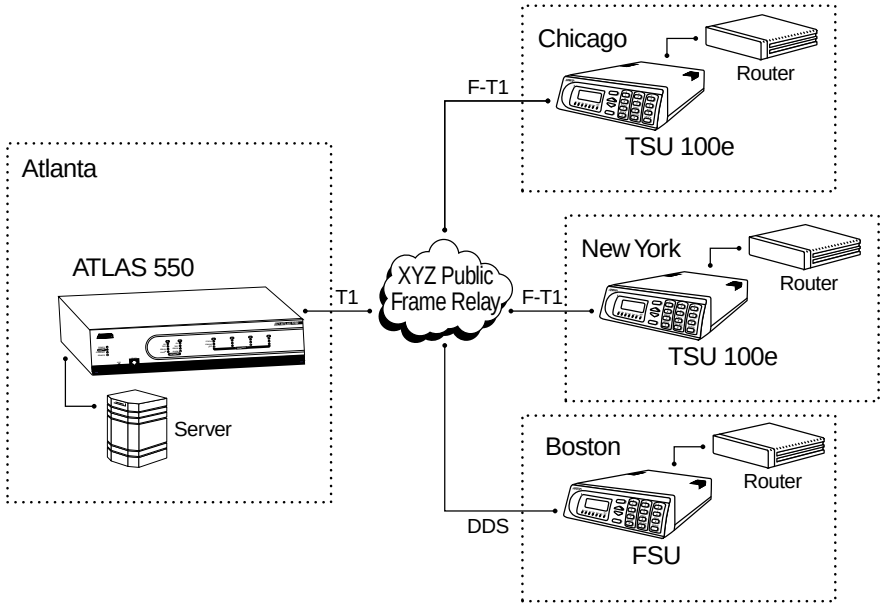


Figure C-7. IP Network With External Routers

Step 1 From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG**, create the packet endpoints (see Figure C-8).

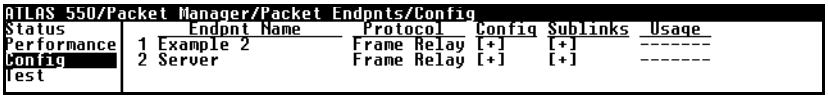


Figure C-8. Menu for Creating the Packet Endpoints

Step 2 From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG/SUBLINKS**, configure the sublinks for both packet endpoints. For simplicity, use the same DLCI number going to the server as going to the frame relay network (see Figure C-9 and Figure C-10).

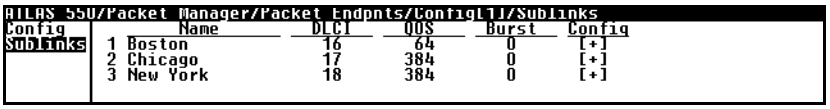


Figure C-9. Menu for Configuring Packet Endpoints (1) Sublinks

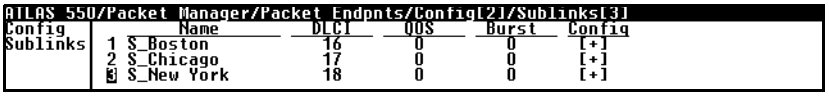


Figure C-10. Menu for Configuring Packet Endpoints (2) Sublinks

Step 3 Make the packet connections (see Figure C-11).

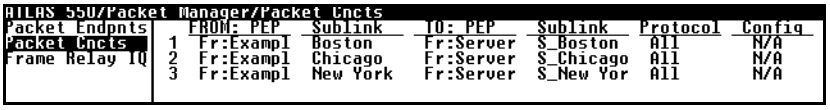


Figure C-11. Menu for Making the Packet Connections

Step 4 Connect the packet endpoints to the physical port. The server connects to an Nx56/64 module, and the frame relay network connects to a T1 port on the controller (see Figure C-12).

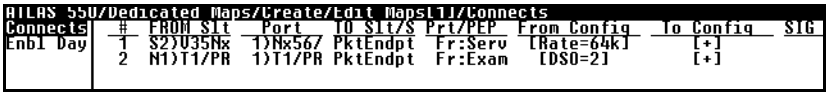


Figure C-12. Menu for Connecting Packet Endpoints to Physical Port

Example 3: Private Frame Relay Network—ATLAS 550 Central-Site Router

Example 3 (see Figure C-13 on page C-5) depicts a private frame relay network using ATLAS 550 as the central-site router and a frame relay switch. A TSU 100e with a router module is located at each of three remote sites. At the central site, ATLAS 550 terminates a full T1 with eight DS0s from each of the remote sites DACSed onto the single T1. (See, also, the discussion of DACSing in the ATLAS 550 *User Manual*.) To re-create this example, follow the process discussed below.

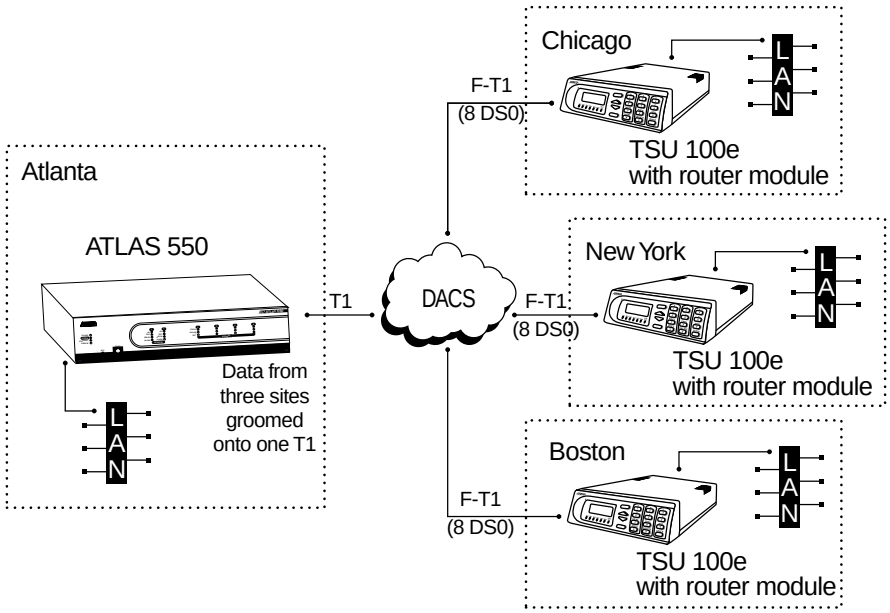


Figure C-13. Private Frame Relay Network—ATLAS 550 Central-Site Router

Step 1 From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG**, create the packet endpoints (see Figure C-14).

```
ATLAS 550/Packet Manager/Packet Endpnts/Config
Status          Endpnt Name      Protocol    Config Sublinks  Usage
Performance   1 Boston           Frame Relay [+]    [+]       -------
Config        2 Chicago          Frame Relay [+]    [+]       -------
Test          3 New York         Frame Relay [+]    [+]       -------
```

Figure C-14. Menu for Creating Packet Endpoints

Step 2 From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG/SUBLINKS**, create three identical sublinks. (Only one sublink is shown in Figure C-15).

```
ATLAS 550/Packet Manager/Packet Endpnts/Config[1]/Sublinks
Config          Name          DLCI    QOS     Burst   Config
Sublinks      1 DLCI 100      100     512     0       [+]
```

Figure C-15. Menu for Creating Sublinks

Step 3 From **PACKET MANAGER/PACKET CNCTS**, connect the packet endpoints (see Figure C-16).

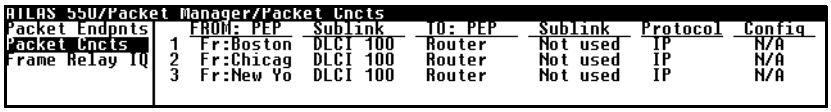


Figure C-16. Menu for Connecting Packet Endpoints

Step 4 Connect the packet endpoint to the physical interface (see Figure C-17).

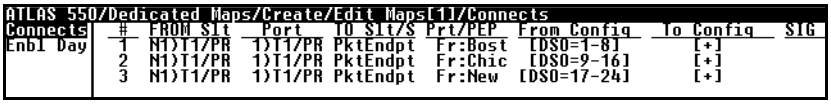


Figure C-17. Menu for Connecting Packet Endpoint to Physical Interface

Example 4: Public Frame Relay Network—IP Data and Packet Voice

Example 4 (see Figure C-18 on page C-7) depicts a public frame relay network with IP data and packet voice. An ATLAS 550 is located at the central site, and an Express 5210 is located at each remote site. ATLAS 550 acts as the central-site router and performs voice switching. To re-create this example, follow the process discussed below.

Packet voice termination requires the **VOICE COMPRESSION MODULE**.

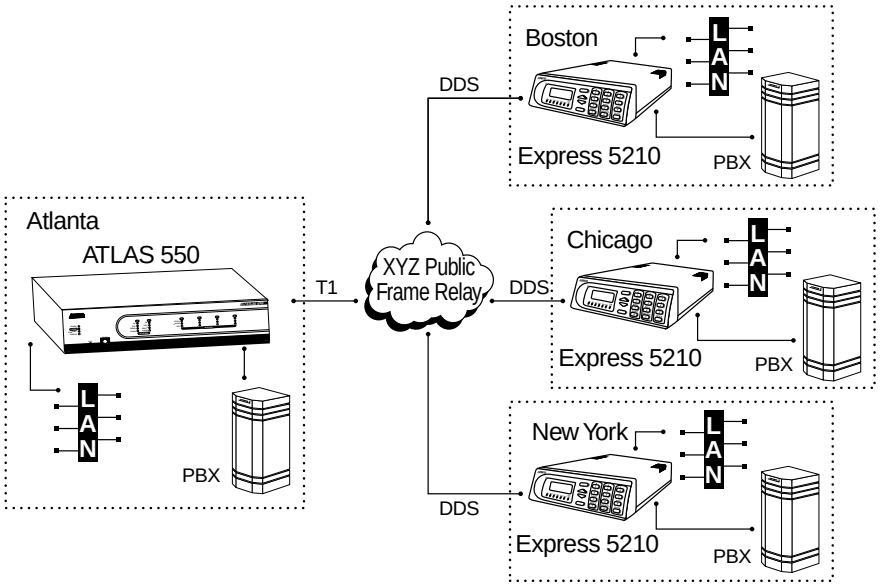


Figure C-18. Public Frame Relay Network

Step 1 From **PACKET MANAGER/PACKET ENDPNTS/CONFIG**, create the packet endpoint (see Figure C-19).

```
ATLAS 550/Packet Manager/Packet Endpnts/Config
Status          Endpnt Name      Protocol     Config Sublinks  Usage
Performance   1 Public           Frame Relay  [+]    [+]       -------
Config
Test
```

Figure C-19. Menu for Creating Packet Endpoint

Step 2 From **PACKET MANAGER/PACKET ENDPNTS/CONFIG**, configure the sublinks (see Figure C-20).

```
ATLAS 550/Packet Manager/Packet Endpnts/Config[1]/Sublinks
Config          Name          DLCI    QOS    Burst   Config
Sublinks      1 Boston        100     56     0       [+]
              2 Chicago       101     56     0       [+]
              3 New York      102     56     0       [+]
```

Figure C-20. Menu for Configuring Sublinks

Step 3 From **PACKET MANAGER/PACKET CNCTS**, connect the packet data to the internal router (see Figure C-21).

```
ATLAS 550/Packet Manager/Packet Cncts
Packet Endpnts    FROM: PEP   Sublink   TO: PEP   Sublink    Protocol  Config
Packet Cncts    1 Fr:Public   Boston    Router    Not used   IP        N/A
Frame Relay IQ  2 Fr:Public   Chicago   Router    Not used   IP        N/A
                3 Fr:Public   New York  Router    Not used   IP        N/A
```

Figure C-21. Menu for Connecting Packet Data

Step 4 Configure the dial plan for packet voice. Refer to Chapter 11, *Dial Plan* for details on configuration (see Figure C-22).

```
ATLAS 550/Dial Plan/User Term
Network Term  #  Slot/Svc     Port/PEP   Sig  In#Accept      Out#Rej   Ifce Config
User Term     1  PktVoice     Fr:Public  RBS  [555-1000]     [+]       [100.1]
Global Param  2  PktVoice     Fr:Public  RBS  [555-2000]     [+]       [101.1]
              3  PktVoice     Fr:Public  RBS  [555-3000]     [+]       [102.1]
```

Figure C-22. Menu for Configuring Dial Plan

Step 5 Connect the packet endpoint to the physical interface (see Figure C-23).

```
ATLAS 550/Dedicated Maps/Create/Edit Maps[11]/Connects
Connects  #  FROM Slt   Port    TO Slt/S Prt/PEP  From Config   To Config   SIG
Enbl Day  1  N1)T1/PR  1)T1/PR PktEndpt  Fr:Publ  [DS0=1-24]     [+]
```

Figure C-23. Menu for Connecting Packet Endpoints

Example 5: Private Frame Relay Network—Packet Voice

Example 5 (see Figure C-24) shows a private frame relay network using compressed voice. An ATLAS 550 is located at two sites (Atlanta and Boston) and a PBX is connected to each ATLAS 550 using a clear-channel T1 connection. Each PBX uses DS0s 1—23 for voice and DS0 24 for signaling; all calls are to be completely managed by the PBXs. In this network, the ATLAS 550 does not terminate the signaling information, but forwards the signaling between endpoints using a transparent bit oriented protocol (TBOP) frame relay connection (requires the Voice Compression Module). To re-create this example, follow the process discussed below.

> **NOTE** *Packet voice transmission requires the* **VOICE COMPRESSION MODULE**.

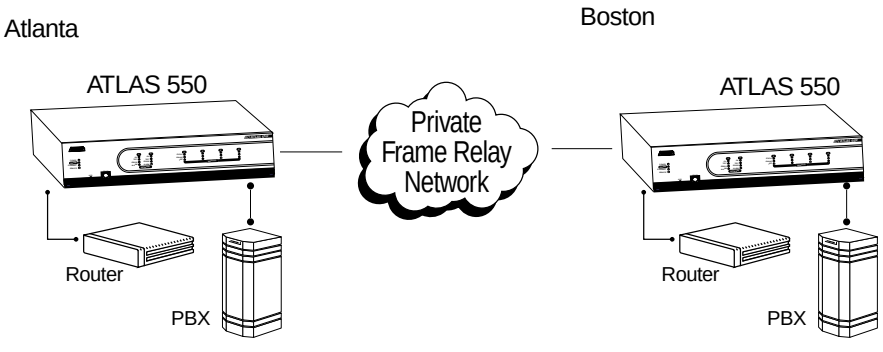


Figure C-24. Private Frame Relay Network Using Compressed Voice

Step 1

From **PACKET MANAGER/PACKET ENDPNTS/CONFIG**, create the packet endpoints: create a frame relay endpoint for the private frame relay link, and create a TBOP link to carry the signaling between the PBXs (see Figure C-25).

Figure C-25. Menu for Creating Packet Endpoints

Step 2

From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG/SUBLINKS**, configure the sublinks.

All 23 voice channels can be carried by one DLCI transported on five DS0 channels. One DS0 and one DLCI are required for the TBOP channel carrying the signaling between the PBXs. To ensure that both the voice and the TBOP DLCIs are allocated their necessary frame relay bandwidth, set the Quality-Of-Service (**QOS**) parameter with 64K allocated to the TBOP channel and 320K (5*64) allocated to the voice channels (see Figure C-26).

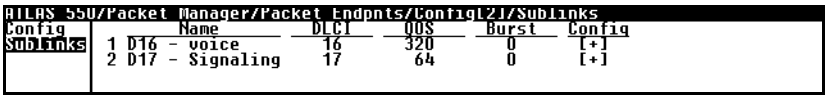


Figure C-26. Menu for Configuring Sublinks

Step 3

Connect the TBOP packet endpoints. Connect the TBOP data path between the DS0 containing the signaling information and the private frame relay resource (see Figure C-27).

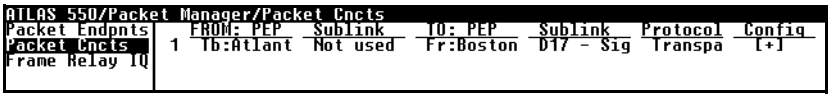


Figure C-27. Menu for Connecting the TBOP Endpoints

Step 4

Connect packet endpoints to the physical links. Each DS0 carrying voice from the PBX must be connected to the frame relay endpoint (see Figure C-28).

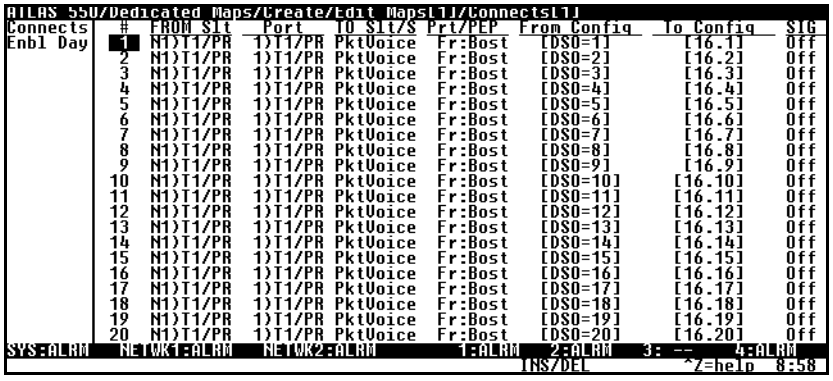


Figure C-28. Menu for Connecting Packet Endpoints to Physical Links

Step 4-a

TBOP Connection Details. The PBX DS0 carrying the signaling information must be connected to the frame relay endpoint (see Figure C-29).

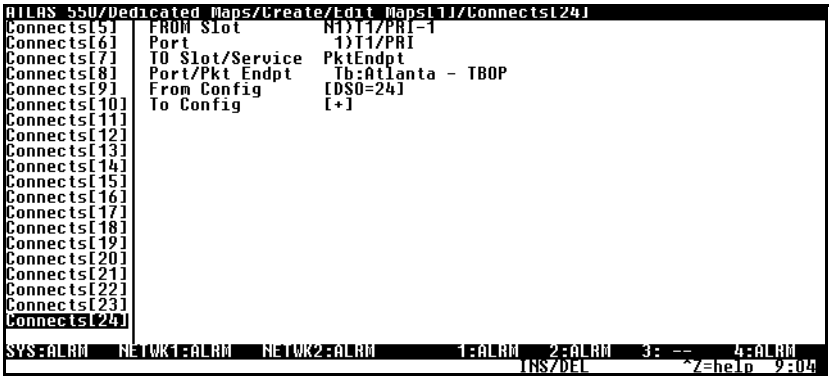


Figure C-29. Connecting PBX DS0 to Frame Relay Endpoint

Step 4-b

Frame Relay Connection Details. Connecting the frame relay endpoint to the private frame relay network requires six DS0s, one for the TBOP connection and five for the compressed voice connections (see Figure C-30). Hint: Use **N2)T1/PRI** as the **FROM SLOT**.

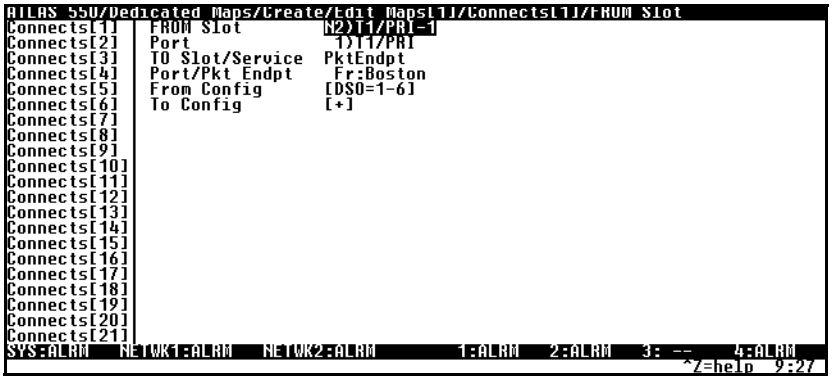


Figure C-30. Connecting FR Endpoint to FR Private Network

Appendix D Router Examples

This appendix provides step-by-step instructions for configuring your ATLAS 550 internal router. Figure D-1 illustrates an ATLAS 550 using the internal router.

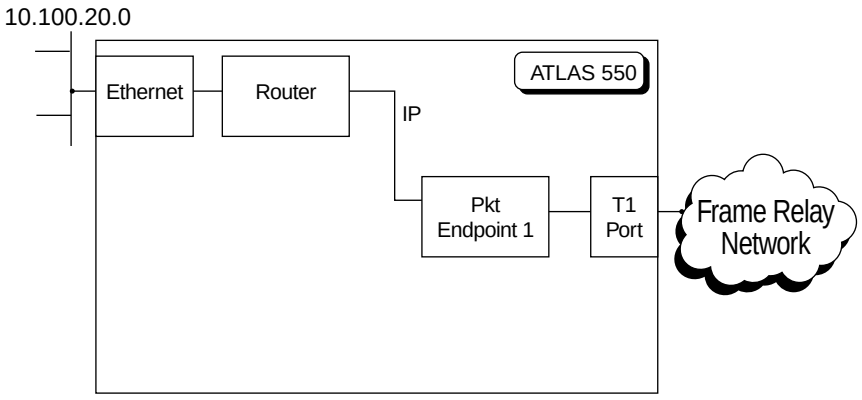


Figure D-1. ATLAS 550 Configured for the Router Option

The general procedure for configuring the ATLAS 550 depicted in Figure D-1 is as follows:

1. From **PACKET MANAGER/PACKET ENDPNTS/CONFIG**, create the frame relay packet endpoint. Refer to the *Frame Relay User Manual* for more information.
2. From **PACKET MANAGER/PACKET ENDPNTS/CONFIG/SUBLINKS**, create the necessary PVCs.
3. From **PACKET MANAGER/PACKET CNCTS**, connect the frame relay endpoint to the Router.
4. From **DEDICATED MAP**, connect the frame relay packet endpoint to the appropriate physical interface.
5. From **ROUTER/IP/INTERFACES**, enable routing on the interface.
6. (Optional) Configure any static routes that might be required.

EXAMPLE 1: IP ROUTING NETWORK—ATLAS AS THE CENTRAL-SITE ROUTER

Example 1 (see Figure D-2) depicts a typical IP routing network using an ATLAS as the central-site router. (This ATLAS unit is the ATLAS 800^{PLUS} with a frame relay upgrade.) The central-site ATLAS terminates a full T1 (F-T1) frame relay connection from the XYZ service provider, and the internal router terminates the IP traffic. A TSU 100e with a router module is located at each of the two remote sites. To re-create this example, follow the process discussed below.

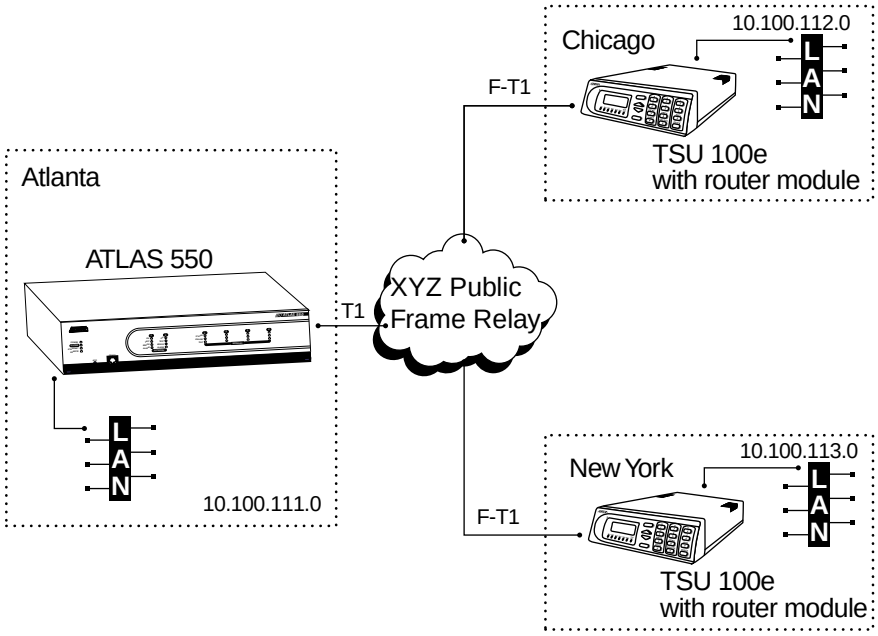


Figure D-2. IP Routing Network with ATLAS as the Central-Site Router

Step 1 From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG**, create the packet endpoint (see Figure D-3).

Figure D-3. Creating Packet Endpoint

Step 2 From **PACKET MANAGER/PACKET ENDPOINTS/CONFIG/SUBLINKS**, create the sublinks or DLCIs for frame relay (see Figure D-4).

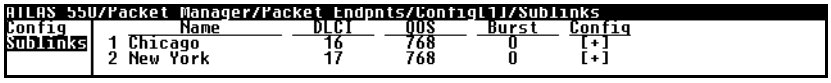


Figure D-4. Creating Sublinks

Step 3 From **PACKET MANAGER/PACKET CNCTS**, connect the IP traffic to the internal router (see Figure D-5).

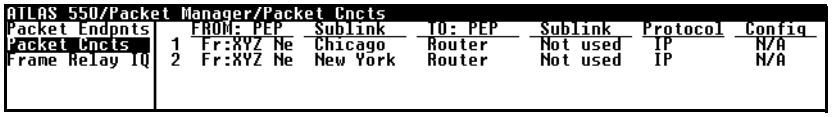


Figure D-5. Connecting IP Traffic to Internal Router

Step 4 From **DEDICATED MAPS/CREATE/EDIT MAPS/CONNECTS**, attach the packet endpoint to the appropriate physical interface (see Figure D-6).

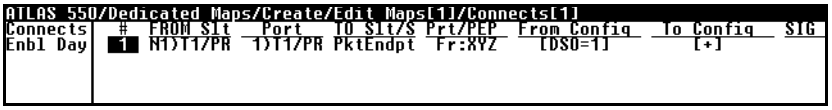


Figure D-6. Connecting Endpoints to Physical Interface

Step 5 From **ROUTER/IP/INTERFACES**, enable routing on the two interfaces. See Figure D-7.

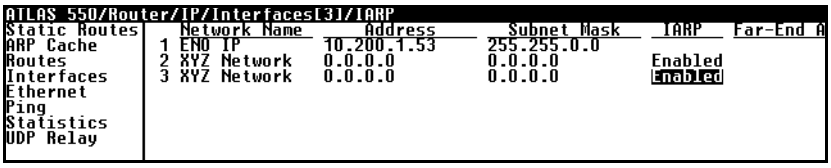


Figure D-7. Enabling Routing

Appendix E Troubleshooting

Power-up Self Test Fails

Modules seated improperly, module failure

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

System Timing Source Unlocked
(Displayed on Terminal Interface, “System Status”)

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

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

Cannot establish Telnet session with ATLAS 550

Max Telnet sessions set to 0, IP address of ATLAS 550 does not match remote host IP address

- Verify that the Ethernet connection is in place, check IP addresses programmed in ATLAS 550 and in the Telnet client, verify that session timeout value is not set too low.
- Verify the link is up via the Ethernet LED.

Cannot pass data from T1 interface to V.35 port

Misconfiguration, improper cabling

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

Switched calls are not working

Misconfiguration

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

Cannot communicate with ATLAS 550 using VT-100 connected to the Control/Chain In Port

Misconfiguration, improper cabling

- Check cabling, verify that the Control / Chain In port rate matches that of the attached terminal.

Frame relay link is down.

Cabling problem.

- **T1**
  - Check the ports' alarm status.
  - If the T1 is experiencing LOS, ensure the cable is plugged in.
  - If the cable is plugged in, ensure the pinout is correct. Refer to the *ATLAS User Manual* for a correct pinout.
- **Nx**
  - Check DTE port signals and verify that DTR and RTS are active.
  - If signals are inactive, verify V.35 cable is connected to correct port.
  - If cable is connected, verify external DTE is powered on.

Packet endpoint not mapped

- From **PACKET MANAGER/PACKET ENDPNTS/STATUS**, verify that the packet endpoint indicates that a physical port is mapped.

Signaling mismatch

- From **PACKET MANAGER**, verify that the Signaling type matches that provided by the carrier and the external DTE.

Timers not configured

- Verify that frame relay counters and timers are configured as specified by the frame relay provider. (Counters and timers do not normally need to be adjusted.)

Link is active, but data is not passing.

DLCI is not active

- Verify in the **PACKET MANAGER/PACKET ENDPNTS/PERFORMANCE** menu that the DLCI shows active. If the DLCI is listed inactive and the packet endpoint is configured as User side of UNI, the frame relay network has not activated this DLCI.

No data on DLCI

- Verify in the **PACKET MANAGER/PACKET ENDPNTS/PERFORMANCE** menu that the DLCI shows receive packets. If there are no packets received, verify that external equipment is configured to transmit data on this DLCI.
- Verify in the **PACKET MANAGER/PACKET CNCTS** menu that this DLCI is mapped.

Appendix F Acronyms and Abbreviations

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

PBX	private branch exchange
PRI	Primary Rate ISDN
PSTN	public switched telephone network
SNMP	simple network management protocol
RBS	robbed bit signaling
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	time division multiplexing
TFTP	Trivial File Transfer Protocol
TSU	terminal service unit
WAN	wide area network

Appendix G Glossary

10/100BaseT Ethernet connection
The ATLAS 550 RJ-48C port that provides Ethernet LAN connection for TFTP, SNMP, andTelnet.

A-Law
PCM coding method as defined by the ITU-T. It is a companding standard for converting between analog and digital in a PCM system. A-Law is mainly used in Europe. µ-Law is the North American equivalent.

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

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

Annex A
Standard for frame relay signaling as defined by the International Telecommunication Union Telecommunication in publication Q.933-A.

Annex D
Standard for frame relay signaling as defined by the American National Standards Institute (ANSI) in publication T1.617-D.

ANSI T1.617-D (Annex D)
See Annex D.

ARP
Address Resolution Protocol. A protocol that maps an IP address to an ethernet MAC address.

ANSI T1.617-D (Annex D)
See Annex D.

ATLAS 550
A bandwidth management system which functions as a central site multiplexer. (See also *Integrated Access System*.)

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

B8ZS
Bipolar eight zero substitution. In a T1 carrier system, a specific eight bit pattern containing two deliberate bipolar violations which replaces eight consecutive customer zero bits.

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

BECN
Backward Explicit Congestion Notification. Sent to the device generating excessive frame relay traffic as a means to slow down the flow of data to the network. Compare with FECN.

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

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

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

Burst
A sporadic increase in a transmission.

Bursty traffic
Traffic that alternates between steady transmission and short bursts of high transmission.

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

CIR
Committed Information Rate. The guaranteed bandwidth available for customer data under normal circumstances.

Companding
The process of compressing and expanding a signal.

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

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

CS
See CTS.

CSU
Channel Service Unit. A device that functions similarly to a modem except that the CSU works with digital signals rather than analog signaling.

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

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

DACS
Digital Access Cross-Connect System. An architecture that allows the cross-connecting of several T1 circuits; that is, any DS0 on any T1 circuit can be groomed to any other DS0 on any of the other T1 circuits in the system.

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

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

DHCP
Dynamic Host Configuration Protocol. Allows dynamic IP address allocation.

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

DID
Direct Inward Dial. Digits received or transmitted that allow the attached equipment to further route a call.

Digital Access Cross-Connect System
See *DACS*.

Discard Eligible (DE)
A flag that can be set to indicate to the network that if excess traffic is received, this frame can be discarded if necessary.

DLCI
Data Link Connection Identifier. Identifies each virtual circuit within a shared physical channel.

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

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

DSU
Data Service Unit. A device used with a CSU to support digital communications by converting signals. (See also CSU.)

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

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

Dual Nx56/64 Module
(Nx is pronounced "en-by.") One of the ATLAS 550 option modules. The Dual Nx56/64 Module provides two synchronous V.35 DTE ports, each of which can operate at any rate that is a multiple of 56 or 64 kbps, up to 2.048 Mbps.

Dual T1/PRI Module
One of the ATLAS 550 option modules. The Dual T1/PRI Module provides two channelized T1 or Primary Rate ISDN (PRI) interfaces. Each interface can operate independently in DS-1 or DSX-1 mode, and any port can serve as the primary or backup timing source for the entire system.

E1 circuit
European equivalent to the T-1 with a capacity of 2.048 Mbps. An E1 can handle 32 voice channels with each conversation being digitized at 64 kbps.

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

FECN
Forward Explicit Congestion Notification. Sent to the device receiving data from the frame relay network to indicate that there is congestion in the receive direction. The receiving DTE device should take action to slow down traffic from the remote end. Compare with BECN.

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

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

FRAD
Frame Relay Access Device. Any equipment that provides a connection between a frame relay network and a LAN.

Frame Relay
A subset of the X.25 packet switching protocol that allows for efficient transmission of data by utilizing many virtual circuits on a single physical interface.

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

Full Status Poll
A poll that occurs each N391 polls and reports the status of each PVC. During this poll the frame relay switch can also notify the user side of the UNI of any creation or deletion of frame relay PVCs.

G.723.1
ITU-specified voice compression algorithm.

Groom
The assignment and redistribution of any DS0 on any T1 circuit to any other DS0 on any on the T1 circuits in a DACS.

Group of Four
The Frame Relay Consortium, composed of Cisco Systems, DEC, Nortel, and StrataCom, which defined an interface for the UNI.

HDLC
High Level Data Link Control. A generic link-level communications protocol developed by the International Organization for Standardization (ISO). HDLC manages synchronous code-transparent, serial information transfers over a link connection.

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

IAD
Integrated Access Device. A network access device that provides many services from a single platform. The ATLAS 550 is an IAD.

IARP
Inverse Address Resolution Protocol. Used for resolving the protocol address when the hardware address is known.

ICMP
Internet Control Message Protocol. Specified in RFC-292 to provide diagnostic functions.

Integrated Access System
A chassis-based product that supports a number of end-user applications on the subscriber side and a number of carrier interfaces on the trunk side. The ATLAS 550 is an Integrated Access System designed to provide significant wide-area cost savings through the consolidation of voice, data, fax, and video.

IP
Internet Protocol. A protocol which provides for transmitting blocks of data between hosts identified by fixed-length addresses.

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

ITU-T Q.933-A (Annex A)
See Annex A.

IXC
IntereXchange Carrier. Phone companies that connect LECs.

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

LAN
Local area network. A group of computers and peripheral devices connected by a communications channel, limited by distance.

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

LEC
Local Exchange Carrier. Provides local access to public data and phone networks.

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

Link Integrity Poll
A poll that occurs each T391 seconds to determine the state of the connection to the frame relay switch.

LLC2
Logical Link Control Type 2. Upper portion of the Data Link layer (layer 2) that handles flow control and error control.

LMI
Standard published by the Frame Relay Consortium in 1990 to create a defined interface on the UNI. The Consortium was composed of Cisco Systems, DEC, Nortel, and StrataCom, and is commonly referred to as the Group of Four. LMI has become a generic term to indicate the type of frame relay signaling used and could be used to mean Annex A or Annex D.

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

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

MAC Address
Data link address that is unique for every device that gets connected to a LAN. Devices on the LAN use these addresses to update routing tables.

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

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

µ-Law
A companding standard for converting between analog and digital in a PCM system. µ-Law is mainly used in North America. A-Law is the European equivalent.

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

N391
Defines how many link integrity polls occur before a full status poll. One out of the number defined in N391 is a full status poll. Default is 6.

N392
Defines how many bad polls can occur within an N393 window before the link is declared down.

N393
Defines the number of polls that make up the window used by N392 to determine if a link is operational.

NNI
A standard interface between two frame relay switches.

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

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

Octal FXO Module
One of the ATLAS 550 option modules. The Octal FXO provides eight analog interface to a system or PBX.

Octal FXS Module
One of the ATLAS 550 option modules. The Octal FXS provides eight 2-wire interface that can operate in the PLAR, Tandem, or FXS mode to provide analog voice.

option modules
Any optional, hot-swappable module that can be added to the ATLAS 550 system for a variety of applications.

OSI
Open System Interconnection. It is a standard defined by ISO and the ITU-T to allow interoperability between equipment of different vendors.

overbooking
ATLAS 550 feature that reduces telecommunications expenses by allowing you to over-subscribe switched bandwidth for situations where simultaneous access to the network by every subscriber is not required.

Packet
A transmission that contains both control information and data.

Packet Endpoint
A virtual port within the ATLAS 550 that a specified physical port terminates its data into for further routing by the system.

Packet Switching
A method of routing packets that avoids congestion and minimizes delivery time.

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

PCM
Pulse Code Modulation. The most common method for encoding analog voice into a digital bit stream.

PIV
Port/PVC Interval. Think of this as a resource meter. The ATLAS 550 can track up to 10,000 PIVs. The PIV is derived from the Max Number of Days and Max Number of Intervals selected by the user. Changing one affects the other.

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

PVC
Permanent Virtual Circuit. Virtual circuit within the frame relay network that has all bandwidth parameters permanently defined upon ordering the circuit.

QOS
Quality of service. A means of guaranteeing available bandwidth under normal operating conditions.

Quad BRI/U Module
One of the ATLAS 550 option modules. The Quad BRI/U Module provides four basic rate ISDN U interfaces, each capable of operating in NT or LT mode.

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

RIP
Routing Information Protocol. A protocol used to exchange routing information among a set of computers connected by a LAN. RIP uses hop count as a routing metric.

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

Router
An interface which finds the best path between two networks. Routers forward packets from one network to another, based on network layer information.

Routing Metric
The method by which a routing algorithm determines that one route is better than another. This information is stored in routing tables. Such tables include reliability, delay bandwidth, load, MTUs, communication costs, and hop count.

SNA
Systems Network Architecture. Network architecture developed by IBM in the 1970s.

SNMP
Simple Network Management Protocol. A control and reporting scheme widely used to manage devices from different vendors. SNMP operates on top of the Internet protocol.

SVC
Switched Virtual Circuit. Virtual circuit within the frame relay network that is created only when needed. Bandwidth parameters are defined each time the circuit is created.

synchronous
1. The condition occurring when two events happen in a specific time relationship with each other, both under control of a master clock.

2. A method of data transmission requiring the transmission of timing pulses to keep the sender and receiver synchronized in their communication used to send blocks of information. Synchronous data transmission is used in high speed data circuits because there is less overhead than asynchronous transmission of characters which contain two extra bits per character to affect timing.

T1 circuit
Also T-1. A digital transmission link with a capacity of 1.544 Mbps. T1 uses two pairs of normal twisted wires. T1 normally can handle 24 voice conversations with each conversation being digitized at 64 kbps. With more advanced digital voice encoding techniques, it can handle more voice channels. T1 is a standard for digital transmission in North America.

T1 Network Interface Module
One of the ATLAS 550 network interface modules. The T1 Network Interface Module (NIM) provides a single channelized T1 or PRI interface. It can operate in DS-1 or DSX-1 mode and can serve as the primary or backup timing source for the entire system.

T391
Defines the time in seconds between frame relay link integrity polls.

T392
Defines the time in seconds the frame relay switch will wait for a poll from the user before declaring the poll bad.

TBOP
Transparent Bit Oriented Protocol. ADTRAN proprietary method for transmitting HDLC traffic across a frame relay network.

TCP
Transmission Control Protocol. Connection oriented protocol that provides error control of IP traffic.

TCP/IP
Transmission Control Protocol/Internet Protocol. A set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, and terminal emulation.

TDM
Time Division Multiplexing. A method for sending two or more signals over a common transmission path by assignment the path sequentially to each signal, each assignment being for a discrete time interval.

Telco
Telephone company.

Telnet
A terminal emulation protocol, part of the TCP/IP suite of protocols, that provides remote terminal-connection services. (See also *VT-100*.)

TFTP
Trivial File Transfer Protocol. A simplified version of the TCP/IP file transfer protocol that does not include password protection or user-directory capability.

TIA 464A
Telecommunication Industry Association's standard for DTMF detection and generation.

Transparent BOP
See TBOP

trunk
A direct line between two telephone switching centers.

TSU
T1 Service Unit.

UDP
User Datagram Protocol. Connectionless protocol defined by RFC 768 for transmission of data without acknowledgment or error control.

UNI
User to Network Interface. Defines the interface between the CPE and the frame relay providers switch.

VCOM Module
One of the ATLAS 550 option modules. The Voice Compression (VCOM) Module can provide 8, 16, 24, or 30 compressed voice channels to implement voice over frame relay in the ATLAS 550.

Voice Compression
A means of reducing the bandwidth required for transmission of voice traffic with minimal impact on the quality of the voice.

VT-100
A non-intelligent terminal or terminal emulation mode used for asynchronous communications. Used to configure the ATLAS 550.

WAN
Wide Area Network. A network that connects users across large distances.

XMODEM
An error-correcting file transfer, data transmission protocol used to transmit files between PCs. The XMODEM protocol sends information in128 byte blocks of data. Some sums (check sums) are done on

each block and the result is sent along with the block. If the result does not check out at the other end, the computer at the other end sends a request (a NAK-negative acknowledgment) to retransmit that block again. If the block checks out, the computer send ACK (an acknowledgment). In this way, relatively error-free transmissions can be accomplished.

Index

D

E

F

S

T

U

V

W

Y

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 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 # _____