Express 6100/6120 **IDSL Router/Bridge**

Part Numbers 1200176L1/L4 Document Number 61200176L1-1B

July 2000



Trademarks:

DMS-100 is a trademark of Northern Telecom, Inc.

Ethernet is a trademark of Digital Equipment Corporation, Intel Corporation, and Xerox Corporation.

Expert ISDN (patent number 5,715,241) is a trademark of ADTRAN, Inc.

Macintosh is a registered trademark of Apple Computer, Inc.

Novell, NetWare, and Internetwork Packet Exchange (IPX) are registered trademarks of Novell, Inc.

Windows is a registered trademark of Microsoft Corporation. 5ESS is a registered trademark of LUCENT.



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

© 2000 ADTRAN, Inc. All Rights Reserved. Printed in U.S.A. FCC regulations require that the following information be provided in this manual:

- 1. This equipment complies with Part 68 of the FCC rules. On the bottom or side of this equipment is a label that ocntains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN), if applicable, for this equipment. If required, this information must be given to the telephone company.
- 2. The following information may be required when applying to your local telephone company for leased line facilities.

Service Type	REN/SOC	FIC	USOC
ISDN	6.0N	02IS5	RJ49C

- An FCC-compliant telephone cord and modular plug may be provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68-compliant. See installation instructions for details.
- 4. If this equipment causes harm to the telephone network, the telephone company may temporarily discontinue service. If possible, advance notification is given; otherwise, notification is given as soon as possible. The telephone company will advise the customer of the right to file a complaint with the FCC
- 5. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of this equipment; advance notification and the opportunity to maintain uninterrupted service are given.
- 6. If experiencing difficulty with this equipment, please contact ADTRAN (see inside back cover) for repair and warranty information. The telephone company may require this equipment to be disconnected from the network until the problem is corrected or until it is certain the equipment is not malfunctioning.
- 7. This unit contains no user serviceable parts.

To ADTRAN service personnel: For continued protection against risk of fire, replace F1 with the same type and rating of fuse only: .2A, 250V.

FEDERAL COMMUNICATIONS COMMISSION RADIO FRE-QUENCY INTERFERENCE STATEMENT:

This equipment has been tested and found to comply with the limits for a Class B 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 or TV reception. The user is encouraged to try to correct the interference by one or more of the following measures:

- 1. Reorient or relocate the receiving antenna.
- 2. Increase the separation between the equipment and receiver.
- 3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4. Consult the dealer or an experienced radio/TV technician for help.



Change or modifications to this unit not expressly approved by ADTRAN will void the user's authority to operate the equipment.

CANADIAN EMISSIONS REQUIREMENTS

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

Cet appareil nuerique respecte les limites de bruits radioelectriques applicables aux appareils numeriques de Class B prescrites dans la norme sur le materiel brouilleur: "Appareils Numeriques," NMB-003 edictee par le ministre des Communications.

CANADIAN EQUIPMENT LIMITATIONS

Notice: The Canadian Industry and Science Canada 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, 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). 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 water pipe 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 requirement that the total of the Load Numbers of all devices does not exceed 100.

IMPORTANT SAFETY INSTRUCTIONS

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons. The precautions are listed below.

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

SAVE THESE INSTRUCTIONS.

Limited Product Warranty

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

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

In no event will ADTRAN or its suppliers be liable to 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.

Table of Contents

Setting up the IDSL Line	Quick Start-1
Chapter 1 Understanding IDSL and the Express	
The Express 6100/6120	1-1
Applications	
Single User to Corporate LAN (Figure 1-3)	1-2
Frame Relay Connectivity to ADTRAN Frame	Port 144
(Figure 1-4)	1-2
Small Office/Home Office (SOHO) to Corpora	
(Figs 1-5 and 1-6)	
Routing and Bridging with the Express 6100/612	
Factory Default	
Bridging	
IP Routing	
IPX Routing	
Concurrent Routing And Bridging	
Network Address Translation Mode	
Front Panel	
Indicators	
Indicators	
Rear Panel	
Configuration	
Security	
security	10
Chapter 2 Installation	2-1
Chapter 3 Terminal Menu Operation and Struct	
Terminal Menu Structure	
Configuration	
Status	
Test	
Logs	
Utilities	
Navigating the Terminal Menus	
General Layout	
Menu Path	
Moving Around	

Submenus [+] or [DATA]	3-4
Activation Field <+>	. 3-4
Editable Data Field	. 3-5
Read-Only Field	
Navigation with the Keyboard	. 3-5
Security Levels	. 3-7
Configuration Menu	
System Info	
System Name	3-8
System Location	3-8
System Contact	3-9
Firmware Revision	3-9
System Uptime	3-9
Configuration/WAN	3-10
WAN/ISDN	3-10
ISDN/Clock Mode	3-10
IDSL/Channel Rate	3-11
IDSL/NEBEs	3-11
IDSL/FEBEs	3-11
WAN/L2 Protocol	3-11
Configuration/IP	3-12
IP/IP Address	3-12
IP/Subnet Mask	3-12
IP/Default Gateway	3-13
IP/Static Routes	3-13
Static Routes/Active	3-13
Static Routes/IP Address	3-13
Static Routes/Subnet Mask	3-13
Static Routes/Gateway	3-13
Static Routes/Hops	3-13
Static Routes/Private	3-14
IP/IP Router	3-14
IP Router/Mode	3-14
IP/RIP.	3-14
IP/NAT	3-15
NAT/DHCP Mode	3-15
NAT/DHCP Renewal Time	3-16
NAT/Web Server	3-16
NAT/Default IP	3-16
IP/DNS	3-16
· · · · · · · · · · · · · · · · · · ·	

DNS/Domain Name	
	3-17
	3-17
J	3-17
J	3-17
J	3-17
	3-18
0	3-19
IPX/Mode	3-19
IPX/Network	3-19
<i>J</i> 1	3-20
	3-20
	3-21
	3-21
0	3-21
	3-22
0 0	3-22
	3-22
O	3-23
	3-23
σ	3-23
0	3-23
O	3-23
WAN IPX Bridge/Frame Type	3-24
WAN IPX Bridge/Seed Status	3-24
0 00	3-24
6	3-25
	3-25
\mathcal{J}	3-26
\mathcal{J}	3-26
J	3-26
	3-26
	3-26
\boldsymbol{j}	3-26
	3-27
\mathcal{J}	3-27
	3-28
Filter Defines / Pattern Filter Defines	
Filter Defines /IPX Filter Defines	3-30

Configuration/Frame Relay	3-32
Frame Relay/Maintenance Protocol	3-33
Frame Relay/Polling Frequency	3-33
Frame Relay/DLCI Mapping	3-33
DLCI Mapping/Active	3-34
DLCI Mapping/DLCI	3-35
DLCI Mapping/IP Map	3-35
DLCI Mapping/IPX Map	3-37
DLCI Mapping/Bridge Map	3-38
DLCI Mapping/Filters	3-39
Configuration/PPP Profile	3-42
PPP Profile/Authentication	3-42
Authentication/Tx Method	3-42
Authentication/Tx Username	3-43
Authentication/Tx Password	3-43
Authentication/Rx Username	3-43
Authentication/Rx Password	3-43
PPP Profile/IP	3-43
IP/Mode	3-43
IP/NAT	3-44
IP/Route	3-44
IP/RIP	3-45
PPP Profile/IPX	3-46
IPX/Mode	3-46
IPX/Remote Network	3-46
IPX/Triggered	3-47
IPX/Type 20 Packets	3-47
PPP Profile/Bridge	3-47
Bridge/Mode	3-47
PPP Profile/PPP	3-48
PPP/VJ Compression	3-48
PPP/Max Config	3-48
PPP/Max Timer	3-48
PPP/Max Failure	3-48
PPP Profile/Filters	3-49
Filters/WAN-to-LAN (In)	3-49
Filters/In Exceptions	3-50
Filters/LAN-to-WAN (Out)	3-50
Filters/Out Exceptions.	3-51
Configuration/Management	3-51
Comiguration/Management	J-J2

Management/Telnet/Web	3-52
Telnet/Web/Server Access	3-52
Telnet/Web/User List	
Management/SNMP	3-54
SNMP Access	
SNMP/Communities	
SNMP/Traps	3-55
Management/Maint Port	3-55
Maint Port/Password Protect	3-55
Maint Port/Password	3-55
Maint Port/Baud Rate	3-56
Maint Port/Data Bits	3-56
Maint Port/Parity	3-56
Maint Port/Stop Bits	3-56
Configuration/Terminal Mode	3-56
Status Menu	3-57
Status/Sessions	3-57
Sessions/PPP Session	3-57
Sessions/Frame Relay	3-58
Frame Relay/Port	3-58
Frame Relay/DLCI Table	3-59
Sessions/Spanning Tree	3-60
Status/ARP Cache	3-60
	3-61
ARP Cache /MAC Address	3-61
	3-61
	3-61
Bridge Cache/MAC Address	3-61
	3-61
Bridge Cache/TTL	3-61
	3-61
IP Routes /IP Address	3-61
	3-62
IP Routes / Gateway	3-62
IP Routes /Port	3-62
IP Routes /Use	3-62
IP Routes/Flags	3-62
IP Routes/Hops	
IP Routes/TTL	
Status/IPX Routes	3-63

IPX Routes / Network	3-63
IPX Routes / Gateway	3-63
IPX Routes / Port	3-63
IPX Routes/Use	3-63
IPX Routes/Hops	3-63
IPX Routes/Ticks	3-64
IPX Routes/TTL	3-64
Status/IPX Servers	3-64
IPX Servers/Type	3-64
IPX Servers/Name	3-64
IPX Servers/Network	3-64
IPX Servers / Address	3-64
IPX Servers/Socket	3-64
IPX Servers/Hops	3-64
IPX Servers/TTL	3-65
Status/WAN Stats	3-65
Status/LAN Stats	3-65
Status/IP Stats	3-66
Test Menu	.3-68
Test Menu/Echo Request	3-68
Logs Menu	3-69
Logs/Sys log Host	3-69
Logs/PPP Log	3-70
PPP Log/Active	3-70
PPP Log/Wrap	3-70
PPP Log/Level	3-70
PPP Log/View	3-70
PPP Log/Clear	3-70
Logs/Connection Log	3-70
Connection Log/Active	3-71
Connection Log/Wrap	3-71
Connection Log/Level	3-71
Connection Log/View	3-71
Connection Log/Clear	3-71
Logs/Network Log	3-71
Network Log/Active	3-71
Network Log/Wrap	3-72
Network Log/Level	3-72
Network Log/View	3-72
Network Log/Clear	3-72

Utilities Menu		
Utilities/Ping 3		
Utilities/Telnet Client 3		
Utilities/Upgrade Menu 3-74		
Upgrade/Transfer Method		
Upgrade/TFTP Host		
Upgrade/Filename		
Upgrade/Status		
Upgrade/Start Transfer 3-75		
Upgrade/Abort Transfer 3-75		
Upgrade/TFTP Server 3-75		
Utilities/Exit		
Chapter 4 Specifications 4-1		
Specifications and Features 4-1		
Network Interface4-1		
Ethernet Interface (LAN)		
Display		
Environmental4-1		
Physical4-1		
Power		
Appendix A Loop Status Messages		
Appendix B Log Messages B-1		
Appendix C SNMP		
Appendix D Connector Pinouts		
Appendix E Terminal Mode Commands E-1		
Index Index-1		

List of Figures

Figure 1-1.	Express 6100
Figure 1-2.	Express 6120 1-1
	Single User to Corporate LAN 1-2
Figure 1-4.	Frame Relay Connectivity to ADTRAN
O	Frame Port 144 1-3
Figure 1-5.	SOHO to Corporate LAN (6100) 1-3
Figure 1-6.	SOHO to Corporate LAN (6120) 1-4
Figure 1-7.	Express 6100 Front Panel 1-7
	Express 6120 Front Panel 1-8
Figure 1-9.	Express 6100 Rear Panel 1-9
Figure 1-10.	Express 6120 Rear Panel 1-9
	Top Level Terminal Menu 3-3
Figure 3-2.	Configuration/System Info Screen 3-8
Figure 3-3.	Configuration/WAN Screen 3-10
	Configuration/IP Screen 3-12
	Configuration/IPX Screen 3-19
Figure 3-6.	Configuration/Bridge Screen 3-22
	Configuration/Security Screen 3-25
Figure 3-8.	Configuration/Frame Relay Screen 3-32
	Configuration/PPP Profile Screen 3-42
	$Configuration/Management\ Screen\\ 3\text{-}52$
	Status Screen
	Test Screen
	Logs Screen
Figure 3-14.	Utilities Screen

List of Tables

Table D-1.	IBM/AT Style EIA-232 Interface	D-1
Table D-2.	RJ-49C ISDN	D-1
Table D-3.	10BaseT Ethernet	D-2

Quick Startup Guide

SETTING UP THE IDSL LINE

The Express 6100/6120 works over leased or "dry" copper provided by the local telephone company. See *Specifications* on page 4-1 for specifications on maximum distance.

- Connect a VT 100 async terminal, or personal computer with a terminal emulator running 9600 N-8-1, to the MAINTENANCE port.
- 2. Hold down the **Control** key and press **R**; then press **Enter** to display the top menu.
- 3. Using the arrow keys and **Enter** key to navigate the menu, go to the **Configuration/WAN/ISDN** menu.
- 4. Set the rate of transfer that will be used. Both devices must be set at the same rate.
- 5. Use the left arrow key or the **Escape** key to go back up the menu tree. When asked to save ISDN parameters, type **y**.
- Connect the IDSL line to the RJ-45 jack labeled ISDN on the rear panel. See *Connector Pinouts* on page D-1 for connector pinouts.
- When the Loop LED(s) remain solid, the Express 6100/6120 is in synchronization.
- The Link LED will illuminate to indicate that PPP has successfully negotiated.

Chapter 1 Understanding IDSL and the Express 6100/6120

IDSL is leased mode ISDN. ADTRAN provides a full line of IDSL products that are the price/performance leaders in the industry.

THE EXPRESS 6100/6120

The Express 6100/6120 is a standalone device that links two Local Area Networks (LANs) using a high-speed DSL two-wire line. The Express 6100/6120 has a two-wire interface and operates up to 144 kbits per second.

Figure 1-1 on page 1-1 shows the Express 6100. Figure 1-2 on page 1-1 shows the Expess 6120. This router includes an integrated hub.

The 10BaseT connector operates at 10 Mbits per second half duplex and accepts standard Ethernet packets encapsulated using IEEE 802.3 or Ethernet II (DIX). The maintenance port can connect to any asynchronous terminal emulating a VT 100 terminal for configuration.

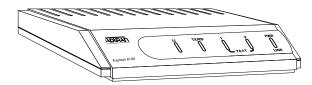


Figure 1-1. Express 6100

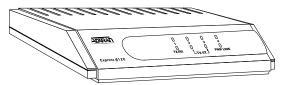


Figure 1-2. Express 6120

Applications

Single User to Corporate LAN (Figure 1-3)

- Telecommuter/Home Office Access to the corporate LAN
- Single device access
- User Datagram Protocol (UDP) broadcasts are "relayed" to corporate LAN.
- Client device can obtain the Internet Protocol (IP) address dynamically using Dynamic Host Configuration Protocol (DHCP).
- Compatible with popular central site LAN access devices

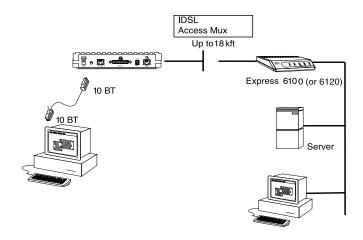


Figure 1-3. Single User to Corporate LAN

Frame Relay Connectivity to ADTRAN Frame Port 144 (Figure 1-4)

- Telecommuter/Home Office Access to the corporate LAN
- Access to any other router within the Frame Relay Network
- User Datagram Protocol (UDP) broadcasts are "relayed" to corporate LAN.
- FramePort 144 provides concentration of up to 96 IDSL interfaces into a single DS-1.

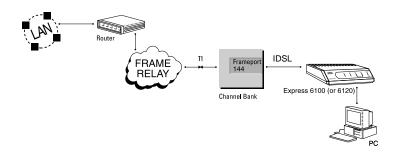


Figure 1-4. Frame Relay Connectivity to ADTRAN Frame Port 144

Small Office/Home Office (SOHO) to Corporate LAN (Figs 1-5 and 1-6)

- Connects the small office or home office to the corporate LAN
- Routes IP and Internet Packet Exchange (IPX) traffic from multiple devices to the corporate LAN
- Bridges all non-routed traffic (e.g., AppleTalk)
- Low cost alternative to buying a high-end router
- Compatible with popular central site LAN access devices

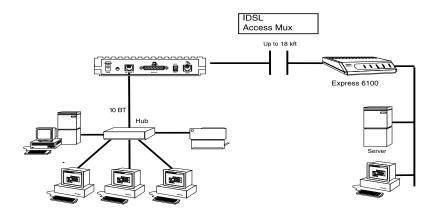


Figure 1-5. SOHO to Corporate LAN (6100)

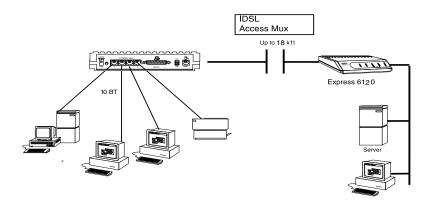


Figure 1-6. SOHO to Corporate LAN (6120)

The Express 6100/6120 provides the following basic functions:

- LAN Bridge: Bridging provides a point-to-point connection between two LANs. The bridge learning function scans the source and destination media access control (MAC) addresses of all packets on its local LAN and determines which packets should be transmitted over the IDSL link. Applications include connectivity between single user or small offices to corporate LANs.
- 2. **IP Router:** The Express 6100/6120 can function as an IP router using the Routing Information Protocol (RIP) for advertising and learning routes among other routers. Static routes may also be entered into the routing table.
- 3. **IPX Router:** IPX routers and services can be exchanged between the Express 6100/6120 and other devices using RIP and Service Advertising Protocol (SAP). Watchdog serialization filtering and spoofing can permit the ISDN to be idle during no application traffic periods.
- 4. Network Address Translation (NAT): Single networks can connect to the Internet with this function. The Express 6100/6120 translates outgoing IP packets over the IDSL to the IP router at the Internet Service Provider. Many popular Internet applications are supported.

 PPP or Frame Relay: The layer two protocol used to transfer packets can be PPP or Frame Relay (RFC 1490). PPP allows a point-to-point connection, whereas Frame Relay can provide up to ten permanent virtual circuits.

Routing and Bridging with the Express 6100/6120

The Express 6100/6120 is a Router and Transparent Learning Bridge. Its features can be easily configured and used once several basic concepts are understood.

Factory Default

The Express 6100/6120 comes from the factory configured for MAC Bridging with no filters or connection information defined. An IP address of 10.0.0.1 with a network mask of 255.255.255.0 is preloaded. The factory default layer two configuration is Auto Detect, which automatically detects PPP or Frame Relay.

Bridging

In Bridge Mode, the Express 6100/6120 can be used to connect two LAN segments. In this mode, all protocols are supported because they are transported across the IDSL link at the MAC layer. The Spanning Tree Algorithm can be used to guarantee a loop-free topology. MAC addresses are "learned" by each Express 6100/6120 to prevent non-WAN packets from being bridged.

IP Routing

The Express 6100/6120 operates as an IP router when the **Configuration/IP/IP Router/Mode** option is configured to **On**. In PPP mode, the Express 6100/6120 uses an IP unnumbered WAN interface; the IP address and mask assigned to the unit's LAN interface apply to all routing and IP operations for the unit. In Frame Relay mode, each PVC can be specified as numbered or unnumbered links. If a default gateway is specified on the network of the Ethernet interface, the unit attempts to reach the gateway through that interface. If no default gateway is specified (i.e., 0.0.0.0) the WAN interface becomes the de-

fault gateway (recommended for remote applications when there are no other routers on the remote LAN).

IPX Routing

Network routes and services are learned and advertised using Novell's RIP and SAP.

Concurrent Routing And Bridging

The Express 6100/6120 can route IP and IPX as well as bridge non-IP/IPX packets simultaneously. The PPP profile will by default negotiate PPP network protocols to support the transmission and reception of IP, IPX, and Bridge packets. If the PPP peer does not accept a protocol, the Express 6100/6120 will fall back to any combination of routing and bridging.

Network Address Translation Mode

NAT is a special mode of operation in which the Express 6100/6120 obtains a dynamically assigned IP address from the peer router (typically an Internet Service Provider). This allows a network of computers to appear as a single IP address.

NAT is enabled if the layer-two protocol is PPP and the PPP profile has the IP parameter **NAT** set to **Yes**, or the layer two protocol is Frame Relay and a DLCI mapping has the **IP Map/Nat** parameter set to **Yes**. The network computer's IP stack may use DHCP to request an IP address, default gateway address, and domain name server addresses from the Express 6100/6120.

Front Panel

Figure 1-7 shows the front panel of the Express 6100. The indicators are divided into LAN functions, WAN functions, and Test functions.

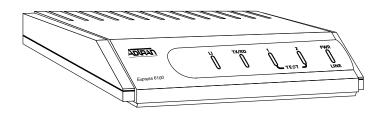


Figure 1-7. Express 6100 Front Panel

	rigate i 7. Express of our font i and
Indicators	-
TX/RX	Flashes when transmitting and receiving data on the 10BaseT connector.
LI	Link integrity. Illuminates when there is a good connection between the Express 6100 and the Hub/NIC card.
PWR	Flashes when the IDSL link (pins 4 and 5 on RJ-45) is not in sync. Solid when in sync.
TEST 1, 2	Illuminates solid when either PPP or Frame Relay has an active connection. Flashes when trying to establish a PPP or Frame Relay connection.

Figure 1-8 shows the front panel of the Express 6120.

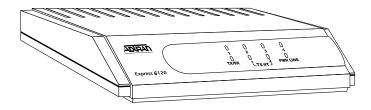


Figure 1-8. Express 6120 Front Panel

	gaxp
Indicators	
TX/RX	Flashes when transmitting and receiving data on the 10BaseT connector.
1, 2, 3, 4	Link integrity. Illuminates when there is a good connection between the Express 6120 and the Hub/NIC card.
PWR	Flashes when the IDSL link (pins 4 and 5 on RJ-45) is not in sync. Solid when in sync.
TEST 1, 2	Illuminates solid when either PPP or Frame Relay has an active connection. Flashes when trying to establish a PPP or Frame Relay connection.

Rear Panel

The Express 6100/6120 has one RJ-45 jack, labeled **ISDN**, on the rear panel for network connection (see Figure 1-9 on page 1-9 and Figure 1-10 on page 1-9).

The **OFF/ON** switch block is for factory default and firmware downloading. With switch 1 in the up or **OFF** position, the Express 6100/6120 will immediately go into a download mode when power is enabled. Switch 1 must be in the down or **ON** position in order to boot up normally. Switch 2 in the up or **OFF** position will force the entire configuration to be factory defaulted.

The Express 6100/6120 transfers data up to 144 kbps over a two-wire facility. This type of service is a permanent connection between endpoints or between the unit and the Frame Relay cloud. It is sometimes referred to as a leased connection, a dedicated connection, a "nailed-up" connection, or a private circuit. Leased connection or leased line is used in this manual to represent these types of services.

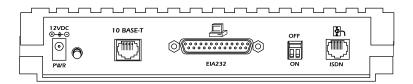


Figure 1-9. Express 6100 Rear Panel

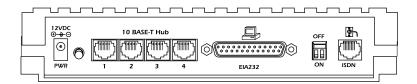


Figure 1-10. Express 6120 Rear Panel

Configuration

The Express 6100/6120 is configured using a menu-based interface. This interface can be accessed via the maintenance port using any asynchronous VT 100 terminal or personal computer running a terminal emulation program, or via IP using a Telnet client program or web browser. To use the Telnet interface or web browser, the Express 6100/6120 must first have an IP address programmed into it via the maintenance port. The factory default is 10.0.0.1.

Security

Security on network devices is a major concern for almost anyone with a network. The Express 6100/6120 provides many tools for securing the local network from hostile users. Connections can be authenticated using passwords. A RADIUS client can also be used.

The Telnet and web browser configuration can also be protected using the same authentication methods. Each menu item in the Express 6100/6120 has a security level associated with it. A Telnet session is assigned a privilege level which determines which menu items are accessible to the Telnet client. See *Security Levels* on page 3-7 for more information on menu security levels.

Filters can be defined to prevent certain addresses or protocols from being transferred from LAN-to-WAN, WAN-to-LAN, or WAN-to-WAN.

As already mentioned, a web browser can be used to configure the Express 6100/6120. This is accomplished by entering <code>http://10.0.0.1</code> on any Windows Internet Explorer browser. If the Express 6100/6120's IP address has been changed from the factory default, then 10.0.0.1 should be replaced by that address.

Chapter 2 Installation

After unpacking the unit, immediately inspect it for possible shipping damage. If damage is discovered, file a claim immediately with the shipping carrier; then contact the ADTRAN Repair and Return department.

IDSL NETWORK CONNECTION

The Express 6100/6120 supports leased operation. A single RJ-49C modular jack labeled **ISDN** on the rear panel provides connection to the network. Leased operation mode supports dedicated 2B1Q data service at rates up to 144 kbps by using a nailed up circuit, or a permanent connection between endpoints.

See *Connector Pinouts* on page D-1 for ISDN network connector pin assignments.

6100 LOCAL AREA NETWORK CONNECTION

The Express 6100 has a single 10BaseT connection port that provides half duplex 10 Mbps operation over a 4-wire twisted pair. Other types of Ethernet interfaces (i.e., AUI, 10Base2, etc.) can be accommodated by obtaining an appropriate converter.

6120 LOCAL AREA NETWORK CONNECTION

The Express 6120 has an integrated hub with four 10BaseT connection ports. Each port can provide half duplex 10 Mbps operation over a 4-wire twisted pair. All four 10BaseT connection ports are the same and are treated equally by the Express 6120.

To connect to an NIC you will need a straight-through cable. To connect to another hub you will need an Ethernet crossover cable, unless the hub you are connecting to has a crossover switch. See *Connector Pinouts* on page D-1 for 10BaseT connector pin assignments.

Chapter 3 Terminal Menu Operation and Structure

TERMINAL MENU STRUCTURE

The Express 6100/6120 uses a multilevel menu structure containing both menu items and data fields. All menu operations and data display in the terminal menu window. The Express 6100/6120 is shipped in the Factory Default configuration. Connect any VT 100 or VT 220 type terminal emulator to the maintenance port. The default rate is 9600 baud 8-N-1. The terminal emulator can flow the Express 6100/6120 off using software flow control. Hardware flow control is not used.

The opening menu (the Main menu, or top-level menu) is the access point to all other operations. Each Main menu item has several functions and submenus to identify and access specific parameters. Figure 3-1 on page 3-3 shows the top-level terminal menu.



To edit items in the terminal menus, you must have the appropriate security level. Each menu description in this section indicates the required security level required for write access. The maintenance port is always at security level 0, giving full access to all configuration items.

The Main menu contains the following options.

> CONFIGURATION

The **Configuration** menu provides options to set up the operational configuration for the Express 6100/6120. See the section *Configuration Menu* on page 3-8 for detailed information on the available options.

> STATUS

The **Status** menu provides options to review and monitor the status of the Express 6100/6120 system. See the section *Status Menu* on page 3-57 for detailed information on the available options.

> TEST

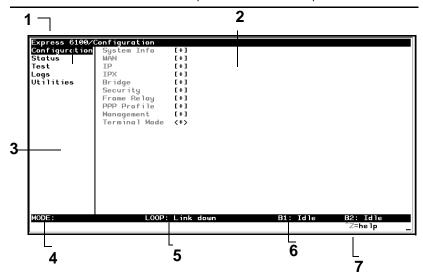
The **Test** menu can be used for performing diagnostic testing of the Express 6100/6120. See the section *Test Menu* on page 3-68 for detailed information on the tests available.

> LOGS

The **Logs** menu can be used for viewing the operational logs for the Express 6100/6120. See the section *Logs Menu* on page 3-69 for detailed information on the available options.

> UTILITIES

The **Utilities** menu provides tools for system diagnostics and upgrading the Express 6100/6120. See the section *Utilities Menu* on page 3-73 for detailed information on the available options.



Menu Path Describes the current position in the terminal menu structure. **Right Pane** Lists available submenus. Additional submenus available through this pane are indicated by the [+] and [DATA] symbols. 3 Left Pane Lists available menus. 4 Mode Describes current operating mode. 5 Loop Status Displays current status of IDSL line. **Rate Status** Displays current rate of connection. **Navigation** Displays list of characters you can use to navi-Help gate the terminal menus (press Control-Z).

Figure 3-1. Top Level Terminal Menu

NAVIGATING THE TERMINAL MENUS

The following sections provide information on how to navigate through the terminal menus.

General Layout

When you first start a terminal mode session, the screen shown in Figure 3-1 on page 3-3 displays. The screen is divided into left and right panes. The left pane shows the current list of submenus, while the right pane shows the contents of a selected submenu.

Menu Path

The top line of the display shows this session's current position (path) in the menu tree. Figure 3-1 on page 3-3 shows the top menu level with the cursor on the Configuration submenu, so the path display shows **Express 6100/Configuration**.

Moving Around

Press **Tab** or the right arrow key to move the cursor from the left pane to the right pane. Press **Tab** or the left arrow key to move the cursor from the right pane back to the left pane. Use the up and down arrows to move around within each pane. Press **Enter** to activate a menu. Press the left arrow key or the **Escape** key to go back up the menu. The following options display throughout the menus.

Submenus [+] or [DATA]

Menus that display [+] or [DATA] indicate that more items are available when selected.

Activation Field <+>

Menus that display <+> indicate that an action is to be taken, such as activating a test.

Editable Data Field

A highlighted menu item indicates that you can enter data in that field.

Read-Only Field

An underlined field is a display field that contains read-only information.

Navigation with the Keyboard

You can use different keystrokes to navigate through the terminal menu. Press **Control-Z** to activate a pop-up screen with the available keystrokes. The following section provides a list of the available keystrokes and the results:

General Navigation

Н	Returns	ta tha	hama	coroon
н	Refurns	to the	$n \cap m \in$	screen

J Jumps between two menu items. Press J while on a menu item of interest, and you will jump back to the main screen. Go to another menu item of interest, Press J, and you will jump back to the screen that was displayed the first time you pressed J. Press J anytime you want to jump between these items.

Arrow Keys Selects items and moves between the left and right panes. The left arrow key allows you to go back up the menu.

.....

Enter Activates an item or moves into submenu.

Escape Cancels an edit. Allows you to go back up the menu.

Also will dismiss the pop-up help screens.

Tab Moves between the left and right panes.

A Moves to the top of a screen.Z Moves to the bottom of a screen.

Backspace Ascends one menu level.

Session Management

- Control-L Logs out of the session.
- **Control-S** Invalidates the password entry and returns to the login screen. The Password prompt will display.
- **Control-R** Refreshes the screen. To save time, only the portion of the screen that has changed is refreshed. This option should be necessary only if the display picks up incorrect characters.

Configuration

- **F** Restores factory default settings. This setting restores the factory defaults based on the location of the cursor. Entire submenus can be factory defaulted.
- C Copies selected items to the clipboard. The amount of information you can copy depends on the cursor location when you press C. For example, 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 Num field in the Frame Relay Mapping screen, all of the information associated with the Map entry is copied.
- P Pastes the item stored in the clipboard, if the information in compatible. You must confirm all pastes except those to a single editable field.
- > For certain types of fields, when you paste information into the field, the value increments by 1.
- For certain types of fields, when you paste information into the field, the value decrements by 1.
- I Inserts a new item in a list. For example, add a new item to the Connection List by pressing I while the cursor is over the index number.
- D Deletes a list item. For example, delete an item from the Connection List by pressing D while the index number is active.

Security Levels

Each menu item on the configuration screens has an associated security level. The security level ranges from 0 (highest security level) to 5 (lowest security level). This level determines whether a Telnet session can access that menu item. The Telnet session is assigned a security level set by the user. Passwords can only be accessed as security level 0. The maintenance port is always at security level 0.

The security levels are assigned as follows:

Level

- O Access all parameters including passwords
- 1 Access all parameters except passwords
- 2 Access all parameters except passwords and authentication methods
- 3 Access all parameters except passwords, authentication methods, and IDSL parameters
- 4 Access only test and status menus
- 5 Access status menus only

> CONFIGURATION MENU

» System Info

The **System Info** menu provides basic information about the unit and displays data fields for editing information. *Figure 3-2* displays the submenus available under this menu item.



Figure 3-2. Configuration/System Info Screen

»» System Name

Write security: 3; Read security: 5

Provides a user-configurable text string for the name of the Express 6100/6120. This name can help distinguish between different installations. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an under bar). The system name is also used for PPP authentication and IPX service name.

»» System Location

Write security: 3; Read security: 5

Provides a user-configurable text string for the location of the Express 6100/6120. This helps to keep track of the physical location of the unit.

You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an under bar).

»» System Contact

Write security: 3; Read security: 5

Provides a user-configurable text string for the contact name. This field can contain a name, phone number, or e-mail address of a person responsible for the Express 6100/6120. You can enter up to 31 alphanumeric characters in this field, including spaces and special characters (such as an under bar).

»» Firmware Revision

Read security: 5

Displays the current firmware revision level of the Express 6100/6120. This field is a read-only field.

»» System Uptime

Read security: 5

Displays the length of time the Express 6100/6120 has been running since power up or reset. This field is a read-only field.

» Configuration/WAN

The **WAN** menu is used to set up the ISDN parameters for the Express 6100/6120. *Figure 3-3* shows the **WAN** menu.



Figure 3-3. Configuration/WAN Screen

»» WAN/ISDN

Write security: 2; Read security: 5

Selects the mode the IDSL line is in.

ISDN/Clock Mode

Write security: 2; Read security: 5

The Express 6100/6120 can only operate as a slave.

IDSL/Channel Rate

Write security: 2; Read security: 5

Determines the rate at which data is transferred over the IDSL link. Possible rates are 64K, 128K, and 144K.

IDSL/NEBEs

Read security: 5

This contains the number of Near-End-Block-Errors (NEBEs) that have been detected by the Express 6100/6120's IDSL circuitry. Continuous errors can indicate a line problem, but a burst at one time is normal.

IDSL/FEBEs

Read security: 5

This contains the number of Far-End-Block-Errors (FEBEs) that have been detected by the IDSL circuitry on the other end of the link. Continuous errors can indicate a line problem, but a burst at one time is normal.

»» WAN/L2 Protocol

Write security: 3, Read security: 5

This parameter specifies the layer 2 data link layer transport used. When selected as PPP, the Express 6100/6120 will negotiate PPP over the IDSL interface. This is used mainly for campus wiring applications. Parameters for controlling the PPP negotiation are in the Configuration/PPP Profile menu. Frame Relay should be selected when the Express 6100/6120 is connected to a Frame Relay switch. The Configuration/WAN/Frame Relay menu is used for controlling the Frame Relay parameters. When Auto Detect (def) is selected, the Express 6100/6120 will look at the incoming packets in order to determine what layer 2 protocol to use.

» Configuration/IP

The IP menu is used to set up the IP parameters for the Express 6100/6120. Any general IP-related configuration item is under this menu. *Figure 3-4* shows the IP menu.

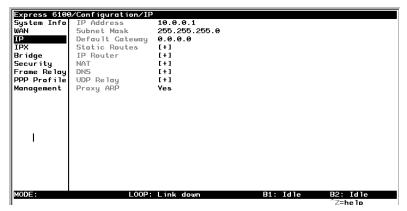


Figure 3-4. Configuration/IP Screen

»» IP/IP Address

Write security: 2; Read security: 5

The IP address assigned to the Express 6100/6120's Ethernet port is set here. This address must be unique within the network. Factory default is 10.0.0.1.

»» IP/Subnet Mask

Write security: 2; Read security: 5

The IP network mask to be applied to the Express 6100/6120's Ethernet port is set here. Factory default is 255.255.255.0.

»» IP/Default Gateway

Write security: 3; Read security: 5

The default gateway is used by the Express 6100/6120 for sending IP packets whose destination address is not found in the route table. If this address is all zeros, then the first WAN connection becomes the default gateway.

»» IP/Static Routes

Static Routes can be inserted under this menu.

Static Routes/Active

Write security: 4; Read security: 5

Adds this static route entry to the IP routing table when set to **Yes** (def) and removes it (if it was previously added) if set to **No**.

Static Routes/IP Address

Write security: 4; Read security: 5

This is the IP address of the host or network address of the device being routed to.

Static Routes/Subnet Mask

Write security: 4; Read security: 5

This mask determines the bits in the previous IP address that are used. If this is to be a host route, it must be set to all ones (255.255.255.255).

Static Routes/Gateway

Write security: 4; Read security: 5

This is the IP address of the router to receive the forwarded IP packet.

Static Routes/Hops

Write security: 4; Read security: 5

This is the number of router hops required to get to the network or host. Maximum distance is 15 hops.

Static Routes/Private

Write security: 4; Read security: 5

When set to **No**, the Express 6100/6120 will advertise this static route using RIP. Otherwise, setting to **Yes** means that the route is kept private.

»» IP/IP Router

The IP router is configured under this menu as follows.

IP Router/Mode

Write security: 3; Read security: 5

When this option is set to On, the Express 6100/6120 will advertise and listen to routes from other IP routers. If Off (def), the route table is still used but only static routes are used for routing IP packets and only the Ethernet port is used. IP packets can be sent over the WAN, but only when bridged.

IP/RIP

Write security: 3; Read security: 5

The Routing Information Protocol (RIP) is supported by the Express 6100/6120. The following parameters are required for setting up the mode on the Ethernet port:

RIP/Mode

Write security: 3; Read security: 5

This option turns RIP **On** or **Off** (def).

RIP/Protocol

Write security: 3; Read security: 5

Version can be V1 (def) or V2.

RIP/Method

Write security: 3; Read security: 5

Split Horizon Only routes not learned on the Ethernet port

are advertised.

Poison Reverse All routes are advertised, including routes (def) learned from the Ethernet port. These routes

are poisoned.

None All routes are advertised, including routes

learned from the Ethernet port. No attempt is

made to poison these routes.

RIP/Direction

Write security: 3; Read security: 5

Tx and Rx (def) RIP advertisements are transmitted and lis-

tened to on the Ethernet port.

Tx only RIP advertisements are transmitted and not

listened to.

Rx only RIP advertisements are listened to but not

transmitted.

RIP/V2 Secret

Write security: 0; Read security: 0

This is a text string used to authenticate advertised routes.

»» IP/NAT

The Network Address Translation general parameters are set up under this menu.

NAT/DHCP Mode

Write security: 3; Read security: 5

When this option is set to **On**, the Express 6100/6120 acts as a DHCP server and will dynamically assign IP, network mask, default gateway, and DNS addresses to any device which transmits a broadcast DHCP request. The addresses assigned are based on the Express 6100/6120's own IP address and will be within the same network.

This mode is most commonly used with the NAT functionality. The default is **Off**.

NAT/DHCP Renewal Time

Write security: 3; Read security: 5

This is the number of hours that the DHCP server should allow the device before it is required to send a new DHCP request. The default is 15 hours, and 0 represents an infinite lease.

NAT/Web Server

Write security: 3; Read security: 5

This is the IP address of a web server on the Ethernet network. When an active NAT connection is made to the Internet, any HTTP, FTP, or SMTP server requests from the WAN are translated and sent to this web server. Normally, communication across NAT must be initiated from the LAN side of the Express 6100/6120. Web Server allows a single machine on the NAT side to be accessed from the Internet side of NAT. This provides outside access to a web server, mail, or ftp server.

NAT/Default IP

This is the IP address used by the Express 6100/6120 for Network Address Translation when nothing is assigned during the PPP negotiation when PPP mode is active or when nothing is specified in the DLCI Mapping's Link IP Address.

»» IP/DNS

The Domain Name Server parameters used by the Express 6100/6120 are specified here. The DNS server addresses can be exchanged between PPP peers. When a connection occurs and IPCP is negotiated, the Express 6100/6120 will get the DNS server addresses from the PPP peer. If the configured DNS server addresses (Server 1 and Server 2) are all zeros, the addresses from the PPP peer are used. In NAT mode, the PPP peer's DNS addresses are always used. The DNS addresses set in Server 1 and Server 2 are offered to a PPP peer if requested.

DNS/Domain Name

Write security: 3; Read security: 5

This is a text string used to represent the domain name used by the Express 6100/6120.

DNS/Server 1

Write security: 3; Read security: 5

This is the IP address for the primary DNS device. It is the first server that domain name requests are sent.

DNS/Server 2

Write security: 3; Read security: 5

This is the IP address for the secondary DNS device. It is used as a back-up in case the primary address does not respond to the request.

»» IP/UDP Relay

The Express 6100/6120 can be configured as a relay agent for UDP broadcast packets. Normally, a router will not forward UDP broadcast packets. However, many network applications use UDP broadcasts to configure addresses, host names, and other information. If hosts using these protocols are not on the same network segment as the servers providing the information, the client programs will not receive a response without enabling the UDP relay agent.

UDP Relay/Mode

Write security: 3; Read security: 5

When this option is set to **On** (def), the Express 6100/6120 will act as a relay agent.

UDP Relay/UDP Relay List

Up to four relay destination servers can be specified in this list.

UDP Relay List/Relay Address

Write security: 3; Read security: 5

This is the IP address of the server that will receive the relay packet.

UDP Relay List/UDP Port Type

Write security: 3; Read security: 5

Standard The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time

when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123). NBNS (NetBIOS Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and

BootP.

Specified When set, the UDP port (1 to 65535) can be specified

in the UDP Port columns. (up to a maximum of three

per server)

UDP Relay List/UDP Ports 1, 2, and 3

Write security: 3; Read security: 5

UDP Port 1, UDP Port 2, and UDP Port 3 are used for specifying UDP ports to be relayed. These fields only apply when **UDP Port Type** is set to **Specified**.

»» IP/Proxy ARP

Write security: 4; Read security: 5

This feature allows the network portion of a group of addresses to be shared among several physical network segments. The ARP protocol itself provides a way for devices to create a mapping between physical (i.e., Ethernet) addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a "proxy" for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned to it. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to **Yes** (def), when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, the Express 6100/6120 will answer the request with its own hardware ad-

dress. If set to No, the Express 6100/6120 will only respond to ARP requests received for its own IP address.

» Configuration/IPX

The IPX menu is used to set up the IPX parameters for the Express 6100/6120. Any general IPX-related configuration item can be found under this menu. *Figure 3-5* shows the IPX menu.

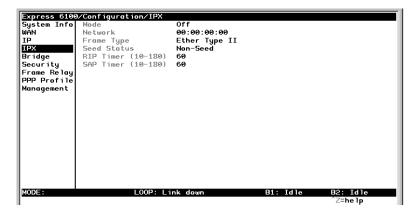


Figure 3-5. Configuration/IPX Screen

»» IPX/Mode

Write security: 2; Read security: 5

When this option is set to **On**, the Express 6100/6120 will route IPX. Setting it to **Off** (def) will disable all IPX functionality.

»» IPX/Network

Write security: 2; Read security: 5

The IPX network address for the Ethernet port is set here. This is an eight-digit hexadecimal value that uniquely identifies the network segment of the Ethernet port. Accidental selection of an IPX network which is already in use on another network segment may cause hard-to-diagnose problems. IPX network numbers should be carefully tracked.

»» IPX/Frame Type

Write security: 2; Read security: 5

The Express 6100/6120 supports all four defined IPX frame types. The possible frame types are: **Ether Type II** (def), **Ether 802.3 (Raw)**, or **Ether SNAP** (802.2 SNAP). Only one frame type can be used at one time.

»» IPX/Seed Status

Write security: 2; Read security: 5

The seed status defines what the Express 6100/6120 is to do with the network information on the selected frame type during startup. There are three possible seeding selections specified:

Seed

The Express 6100/6120 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, the Express 6100/6120 will use the configured IPX network number for the Ethernet segment.

Non-Seed (def)

The Express 6100/6120 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, the Express 6100/6120 will wait indefinitely until a number is sent by another router on the Ethernet segment.

Auto-Seed

The Express 6100/6120 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, the Express 6100/6120 will auto-generate a valid number using its routing tables.

»» IPX/RIP Timer

Write security: 3; Read security: 5

This value specifies how often the Express 6100/6120 sends out IPX RIP packets on the network segment attached to the Ethernet port. The RIP packets sent contain routing information about the networks for which this Express 6100/6120 is responsible. The default value is 60 seconds.

»» IPX/SAP Timer

Write security: 3; Read security: 5

This value specifies how often the Express 6100/6120 sends out IPX SAP (Service Access Protocol) packets on the network segment attached to the Ethernet port. The SAP packets sent contain information about the services (such as servers, printers, etc.) for which this Express 6100/6120 is responsible. The default value is 60 seconds.

» Configuration/Bridge

The Bridge menu is used to set up the bridge parameters for the Express 6100/6120. The bridging function runs at the Media Access Control (MAC) level which allows any protocol packets that run over Ethernet to be forwarded. Bridging can run concurrently with the IP and IPX routing. However, certain rules apply for when packets are bridged across a WAN connection. When IP routing is active, IP packets (which include ARP packets) are not bridged. When IPX routing is active, IPX packets are not bridged. Also, the WAN IP Bridge and WAN IPX Bridge menus allow the WAN connection to bridge packets to the Express 6100/6120 but get routed as soon as they arrive at the unit. Figure 3-6 shows the Bridge menu.



Figure 3-6. Configuration/Bridge Screen

»» Bridge/Mode

Write security: 2; Read security: 5

When this option is set to On (def), the Express 6100/6120 bridge function will be enabled. Setting it to Off will disable all bridge functionality.

»» Bridge/WAN IP Bridge

When IP routing is active, the Express 6100/6120 will allow another WAN device to bridge IP packets to it using PPP BCP. Normally, two IP routers would negotiate PPP IPCP to exchange IP packets. However, if a device can only support PPP BCP, IP packets are encapsulated by the device as bridge packets. The Express 6100/6120 can treat the WAN IP Bridge as a virtual Ethernet port connected only to a WAN device which has negotiated PPP BCP. This menu allows the IP parameters for this virtual Ethernet to be set up.

WAN IP Bridge/Network

Write security: 2; Read security: 5

This is the IP address of the virtual Ethernet port.

WAN IP Bridge/Netmask

Write security: 2; Read security: 5

This is the network mask to be applied to the virtual Ethernet port.

WAN IP Bridge/Triggered

Write security: 2; Read security: 5

When set to **Yes**, only IP RIP updates are sent when the routing table has changed. When set to **No** (def), updates are sent periodically.



RIP version, method, and direction are determined by the Ethernet parameters set in the Configuration/IP/IP Router/RIP menu.

WAN IP Bridge/Proxy ARP

If this option is set to **Yes** (def), the Express 6100/6120 will proxy ARP on the bridge IP port. See the section *IP/Proxy ARP* on page 3-18 for an explanation of the proxy ARP function.

»» Bridge/WAN IPX Bridge

When IPX routing is active, the Express 6100/6120 will allow another WAN device to bridge IPX packets to it using PPP BCP. Normally, two IPX routers would negotiate PPP IPXCP to exchange IPX packets. However, if a device can only support PPP BCP, IPX packets are encapsulated by the device as bridge packets. The Express 6100/6120 can treat the WAN IPX Bridge as a virtual Ethernet port connected only to a WAN device which has negotiated PPP BCP. This menu allows the IPX parameters for this virtual Ethernet to be set up.

WAN IPX Bridge/Network

Write security: 2; Read security: 5

This is the network address of the virtual Ethernet port. See *IPX/Network* on page 3-19 for an explanation of the IPX network number.

WAN IPX Bridge/Frame Type

Write security: 2; Read security: 5

This is the frame type used for the virtual Ethernet port. See *IPX/Frame Type* on page 3-20 for an explanation of the IPX frame type.

WAN IPX Bridge/Seed Status

Write security: 2; Read security: 5

This is the seed status used for the virtual Ethernet port. See *IPX/Seed Status* on page 3-20 menu for an explanation of the IPX seed status.

WAN IPX Bridge/Triggered

Write security: 2; Read security: 5

When set to Yes, only IPX RIP and SAP updates are sent when the routing or service table has changed. When set to No (def), updates are sent periodically.



RIP and SAP periodic rates set for the Ethernet port (see IPX/RIP Timer on page 3-21 and IPX/SAP Timer on page 3-21) are used for the WAN IPX bridge port.

» Configuration/Security

The **Security** menu is used to set up the authentication parameters needed to authenticate PPP connection. Also, the filter defines are placed under this menu. Figure 3-7 shows the Security menu.



Figure 3-7. Configuration/Security Screen

»» Security/Authentication

Write security: 1; Read security: 2

The method used for authenticating the PPP peer is selected here. The possible values are:

None (def) No attempt is made to authenticate the PPP peer. **Radius** The Express 6100/6120 will act as a RADIUS client and authenticate the PPP peer using the RA-

DIUS server. The Radius server parameters must

be set up properly for this to work.

The PPP profile is used to authenticate the PPP **PPP Profile**

peer.

See Configuration/PPP Profile on page 3-42 for more information on authenticating.

»» Security/Radius Server

The parameters for the radius server are configured in this menu. The RADIUS server can be used for authenticating a PPP peer (if defined under **Security/Authentication**) and for Telnet server sessions.

Radius Server/Primary Server

Write security: 1; Read security: 2

This is the IP address of the first RADIUS server that the Express 6100/6120 should attempt to communicate with when authenticating a PPP peer.

Radius Server/Secondary Server

Write security: 1; Read security: 2

This is the IP address of the back-up RADIUS server that the Express 6100/6120 should attempt to communicate with when the primary server does not respond.

Radius Server/UDP Port

Write security: 1; Read security: 2

This is the UDP port that the Express 6100/6120 should use when communicating with the RADIUS server. The default is 1645, which is the commonly used port.

Radius Server/Secret

Write security: 0; Read security: 1

The RADIUS server and Express 6100/6120 share this text string, which is used by the RADIUS sever to authenticate the Express 6100/6120 that is the RADIUS client. The factory default is not to use a secret.

Radius Server/Retry Count

Write security: 1; Read security: 2

This is the number of times the Express 6100/6120 should send a request packet to the RADIUS server without a response before giving up. If the

number of attempts to communicate with the primary server is equal to the retry count, the secondary server (if defined) is tried. If the secondary server does not respond within the retry count, the PPP peer (or Telnet session) is not authenticated and is dropped. The default is 5.

»» Security/PPP

Write security: 1; Read security: 2

The PPP peer can be authenticated using three standard methods: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Protocol) and EAP (Extensible Authentication Protocol). The strength of the authentication is determined in the order EAP, CHAP, followed by PAP, where EAP is the strongest and PAP is the weakest. PAP is a clear-text protocol, which means it is sent over the PPP link in a readable format. Care must be taken not to allow highly sensitive passwords to become compromised using this method. CHAP and EAP use a one-way hashing algorithm which makes it virtually impossible to determine the password. EAP has other capabilities which allow more flexibility than CHAP.

The following selections are possible:

PAP, CHAP or EAP (def)	The Express 6100/6120 will ask for EAP during the first PPP LCP negotiation and allow the PPP peer to negotiate down to CHAP or PAP.
CHAP or EAP	The Express 6100/6120 will ask for EAP during the first PPP LCP negotiation and allow the PPP peer to negotiate down to CHAP but not PAP.
EAP	The Express 6100/6120 will only allow EAP to be negotiated. If the PPP peer is not capable of doing EAP, then the connection will not succeed

»» Security/Filter Defines

The Express 6100/6120 can filter packets based on certain parameters within the packet. The method used by the Express 6100/6120 allows the highest flexibility for defining filters and assigning them to a profile. The filters are set up in two steps: (1) defining the packet types, and (2) adding them to a list under the PPP profile or DLCI map. See

the section *DLCI Mapping/Filters* on page 3-39 for examples of how to set up filter profiles. This menu is used to define the individual filter defines based on packet type.

Filter Defines /MAC Filter Defines

Write security: 2; Read security: 3

The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of the Express 6100/6120 are defined here. Up to 32 MAC defines can be specified.

Name	Identifies the filter entry
Src Addr	48-bit MAC source address used for comparison. (hexadecimal format)
Src Mask	Bits in the MAC source address which are compared. (hexadecimal format)
Dest Addr	48-bit MAC destination address used for comparison. (hexadecimal format)
Dest Mask	Bits in the MAC destination address used for comparison. (hexadecimal format)
MAC Type	16-bit MAC type field used for comparison. (hexadecimal format)
Type Msk	Bits in the MAC type field used for comparison.

Filter Defines /Pattern Filter Defines

Write security: 2; Read security: 3

The pattern filter is applied to bridge packets only. That is, any packet which is forwarded by the bridge functionality of the Express 6100/6120. Up to 32 pattern defines can be specified.

(hexadecimal format)

Name	Identifies the filter entry
Offset	Offset from beginning of packet of where to start the pattern comparison
Pattern	64 bits used for comparison. (hexadecimal format)
Mask	Bits in the pattern to be compared. (hexadecimal format)

Filter Defines /IP Filter Defines

Write security: 2; Read security: 3

The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.

Name Identifies the filter entry

IP Src IP address compared to the source address.

(dotted decimal format)

Src Mask Bits which are used in the source comparison.

(dotted decimal format)

IP Dest IP address compared to the destination ad-

dress. (dotted decimal format)

Dest Mask Bits which are used in the destination compar-

ison. (dotted decimal format)

Src Port IP source port number used for comparison

Range: 0 to 65535. (decimal format)

Src Port Cmpr Type of comparison that is performed

means ports equal to
 mot = means port not equal to
 means port greater than
 means port less than

None means the source port is not compared

Dst Port IP destination port number used for compari-

son Range: 0 to 65535. (decimal format)

Dst Port Cmpr Type of comparison that is performed

means ports equal to
 mot = means port not equal to
 means port greater than
 means port less than

None means the destination port is not compared

Proto Protocol used for comparison. Range: 0 to

255. (decimal format)

Proto Cmpr Type of comparison that is performed

means protocols equal to
 mot = means protocols not equal to
 means protocols greater than
 means protocols less than

None means the protocol is not compared

TCP Est

Yes only when TCP established
No only when TCP not established

Ignore ignore TCP flags

Filter Defines /IPX Filter Defines

Write security: 2; Read security: 3

The IPX filter defines apply to any IPX packet whether it is routed or bridged. Also, any IPX encapsulation type will be accounted for. Up to 32 IPX defines can be specified.

Name Identifies the filter entry (15 characters

max)

Src Net 32-bit source network address

Src Mask Bits in the source network address which

are compared. (hexadecimal format)

Dest Net 32-bit destination network address

Dest Mask Bits in the destination network address

which are compared. (hexadecimal for-

mat)

Src Socket 16-bit value which is the source socket.

Range: 0-65535.

Src Socket Comp Type of comparison that is performed:

means socket equal to
 not = means socket not equal to
 means socket greater than
 means socket less than

None no comparison is done on source socket

Dest Socket 16-bit value which is the destination sock-

et.

Range: 0-65535.

Dest Socket Comp Type of comparison that is performed:

means socket equal to
 not = means socket not equal to
 means socket greater than
 means socket less than

None no comparison is done on destination

socket

Type 8-bit value which is the IPX type

Type Comp Type of comparison that is performed:

means type equal to
 not = means type not equal to
 means type greater than
 means type less than

None no comparison is done on IPX type

» Configuration/Frame Relay

Frame Relay is a connection-oriented service requiring circuits to be configured by your carrier to establish a physical link between two or more locations. Multiple virtual circuits (which appear as virtual point-to-point links) can be run through the same physical connection.

There are two types of virtual circuits supported in Frame Relay: Permanent Virtual Circuits (PVC) and Switched Virtual Circuit (SVC). PVCs are like dedicated point-to-point private lines. Since the physical connection is always there in the form of a leased line, call setup and tear down is done by a carrier via a network management system. SVCs require setup and tear down and are generally not available from Frame Relay carriers. Virtually all Frame Relay communications is done using PVCs. The Express 6100/6120 supports PVCs only.

A number called the Data Link Connection Identifier (DLCI) identifies each virtual circuit within a shared physical channel.

Figure 3-8 shows the Frame Relay menu.



Figure 3-8. Configuration/Frame Relay Screen

»» Frame Relay/Maintenance Protocol

Write security: 3, Read security: 5

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

Annex D (def) This is an ANSI standard and is the most com-

monly used standard in the US.

Annex A This is the CCITT European standard.

LMI This was developed by a vendor consortium

and is also known as the "consortium" management interface specification. It is still used

by some carriers in the U.S.

Static This should be selected when there is no Frame

Relay switch in the circuit. The DLCIs are assigned in the DLCI Mapping and must be the same for the device it will communicate with.

»» Frame Relay/Polling Frequency

Write security: 3, Read security: 5

This parameter is the interval that the Express 6100/6120 polls the Frame Relay switch using the maintenance protocol selected above. The Express 6100/6120 is required to poll the Frame Relay switch periodically to determine whether the link is active. The value is in seconds and ranges from 5 to 30 seconds with a default of 15 seconds.

»» Frame Relay/DLCI Mapping

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

When empty and a maintenance protocol other than static is used, the Express 6100/6120 will poll the switch to determine which DLCIs are

active. These active DLCIs will attempt to determine the IP and IPX addresses on the other end of the virtual circuit using Inverse ARP (IARP). If there is a response, the network learned will be added to the router tables and the virtual circuit will be treated as an unnumbered interface. Bridge connections are made using bridge group 1.

When more than one DLCI mapping is listed, the Express 6100/6120 will try to match the DLCIs learned from the Frame Relay switch with the DLCI values in the map. If there is a match, the protocols specified in the map are used. However, if an active DLCI is not in the list, it looks for an entry that has 0 in the DLCI field. This entry is considered the default entry to use when no match occurs. If this default entry is not present, the Express 6100/6120 falls back to using IARP (as discussed in the previous paragraph) to determine the protocols to use with that particular virtual circuit. If a static maintenance protocol is used, at least one DLCI mapping must be specified.



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



To delete an unused profile, use the **D** key when the cursor is over the number in the **Num** column. Once deleted, the profile is gone permanently as soon as the DLCI Mapping is saved. Items may be deleted when **DEL** appears below the status bar.

DLCI Mapping/Active

Write security: 3, Read security: 5

When this parameter is set to **Yes** (def), the mapping is used to determine the protocols used. If set to **No**, the Express 6100/6120 will ignore the virtual circuit with this DLCI.

DLCI Mapping/DLCI

Write security: 3, Read security: 5

This is the DLCI associated with this virtual circuit. This value can range from 16 to 1007.

DLCI Mapping/IP Map

Write security: 3, Read security: 5

This menu represents the IP protocol mapping that is to take place for this DLCI.

IP Map/Active

Write security: 3, Read security: 5

When this is set to **Yes** (def), the Express 6100/6120 will attempt to transport IP packets for this DLCI. A setting of **No** means that no IP traffic or route will be exchanged.

IP Map/IARP

Write security: 3, Read security: 5

When this is set to **Yes** (def), the Express 6100/6120 will send Inverse ARP packets to determine the IP address on the other end of the virtual circuit. If the IARP is responded to, a route is placed in the IP route table. A setting of **No** means that the route address is to be assigned statically using the **IP Map/Far-End IP Address** parameter. The Express 6100/6120 will always respond to Inverse ARP requests.

IP Map/Far-End IP Address

Write security: 3, Read security: 5

This is the IP address of the device on the other end of the virtual circuit. When this DLCI becomes active, the Express 6100/6120 will add a route in the IP routing table.

IP Map/IP Netmask

Write security: 3, Read security: 5

The IP network mask to apply to the **Far-End IP Address** and **Link IP Address** is specified here.

IP Map/Link IP Address

Write security: 3, Read security: 5

The virtual circuit may require an IP address to be specified at this DLCI interface. This is called a numbered interface. This address is used by the Express 6100/6120 to respond to Inverse ARP requests. If this IP address is left as 0.0.0.0, the link is treated as unnumbered and the Express 6100/6120 responds to the Inverse ARP with its Ethernet IP address.

IP Map/RIP Protocol

Write security: 3, Read security: 5

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

IP Map/RIP Method

Write security: 3, Read security: 5

The way the RIP protocol sends out its advertisements is specified here:

None All routes in the router table are adver-

tised out this virtual circuit with no modi-

fication of the metrics.

Split Horizon (def) Only routes not learned from this particu-

lar virtual circuit are advertised.

Poison Reverse All routes are advertised, but the routes

learned from this port are "poisoned"

with an infinite metric.

IP Map/RIP Direction

Write security: 3, Read security: 5

This parameter allows the direction at which RIP advertisements are sent and listened to be specified.

Tx and Rx (def) RIP advertisements are periodically trans-

mitted and are listened to on this virtual cir-

cuit.

Tx Only RIP advertisements are periodically trans-

mitted but are not listened to on this virtual

circuit.

Rx Only RIP is not transmitted on this virtual circuit

but they are listened to.

IP Map/NAT

The Express 6100/6120 can perform Network Address Translation over a PVC. Setting this option to **On** will cause the Express 6100/6120 to translate between the Ethernet addresses and the configured **Link IP Address**. Only one PVC may be used for translation at one time. If more than one IP Map is configured for NAT, the first PVC which is activated becomes the NAT port.

DLCI Mapping/IPX Map

This menu represents the IPX protocol mapping that is to take place for this DLCI.

IPX Map/Active

Write security: 3, Read security: 5

When this is set to **Yes** (def), the Express 6100/6120 will attempt to transport IPX packets for this DLCI. A setting of **No** means that no IPX traffic or route will be exchanged.

IPX Map/IARP

Write security: 3, Read security: 5

When this is set to **Yes** (def), the Express 6100/6120 will send Inverse ARP packets to determine the IPX network on the other end of the virtual circuit. If the IARP is responded to, a route is placed in the IPX route table. A setting of **No** means that the IPX network is to be assigned to the link statically using the IPX Map/Link Network parameter. The Express 6100/6120 will always respond to Inverse ARP requests.

IPX Map/Link Network

Write security: 3, Read security: 5

This is the IPX network of the link or of the other device's LAN. When this DLCI becomes active, the Express 6100/6120 will add a route to this network in the IPX routing table. This address is also used by the Express 6100/6120 to respond to Inverse ARP requests. If this IPX address is left as 0, the link is treated as unnumbered and the Express 6100/6120 responds to the Inverse ARP with its Ethernet IPX address.

DLCI Mapping/Bridge Map

This menu is used to permit bridging of packets over this DLCI. Each DLCI or virtual circuit must be assigned a bridge group. The bridge group treats all virtual circuits as one circuit. Bridge packets destined to be transmitted out a particular bridge group are copied and transmitted individually out each DLCI in the bridge group. However, incoming bridge packets received from one DLCI are not retransmitted out the other DLCIs in the same bridge group. Any device in the bridge group must transmit to each DLCI. This requires a fully meshed circuit, meaning each device has a virtual circuit to each other.

Bridge Map/Active

Write security: 3, Read security: 5

When this is set to **Yes** (def), the Express 6100/6120 will bridge packets to and from this DLCI. Bridge packets are any packets that are not IP or IPX packets except when the router is turned off, in which case

that particular router's protocol packets are bridged. A setting of No means that no bridging will occur.

Bridge Map/Bridge Group

Write security: 3, Read security: 5

The bridge group that this DLCI is part of is specified here as **Group** 1 or **Group 2**. These groups correspond to the spanning tree protocols Bridge Group 1 and Bridge Group 2.

DLCI Mapping/Filters

The Express 6100/6120 can block packets in and out of a PVC port by use of the filters. They are set up in two steps: 1) define the types of packets that would be of interest in the Configuration/Security/Filter **Defines** menu, and 2) set up the filter type and combination of defines that will cause a packet block.

Filters/In from PVC

Write security: 2; Read security: 5

The packets which come into the Express 6100/6120 via this PVC can be filtered in three ways:

Disabled Turns off packet input filtering. No incoming packets from this PVC are blocked. (def) All incoming packets from this PVC are blocked **Block All** except as defined in the Filters/In Exceptions

Forward All All incoming packets from this PVC are not blocked except as defined in the Filters/In Ex-

ceptions list.

Filters/In Exceptions

Write security: 2; Read security: 5

This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

Active	Turns this entry active when set to On .
Туре	Selects the filter define list to reference:
MAC	from the Configuration/Security/Filter Defines/MAC Filter Defines list.
Pattern	from the Configuration/Security/Filter Defines/Pattern Filter Defines list.
IP	from the Configuration/Security/Filter Defines/IP Filter Defines list.
IPX	from the Configuration/Security/Filter Defines/IPX Filter Defines list.
Filter List Name	Selects between filters defined in the list.
Next Oper	The next operation to use to combine with the next filter in the list:
END	the last filter to combination.
AND	logically AND this filter with the next filter in the list
OR	logically OR this filter with the next filter in the list.

Filters/Out to PVC

Write security: 2; Read security: 5

The packets which transmit out this PVC from the Express 6100/6120 can be filtered in three ways:

Disabled (def) Turns off packet output filtering. No outgo-

ing packets to this PVC are blocked.

Block All All outgoing packets to this PVC are blocked

except as defined in the Filters/Out Excep-

tions list.

Forward All All outgoing packets to this PVC are not

blocked except as defined in the Filters/Out

Exceptions list.

Filters/Out Exceptions

Write security: 2; Read security: 5

This is a list of up to 32 filter entries. The setup is exactly the same as the **Filter/In Exceptions** list.

Maintenance DLCI

The Express 6100/6120 can be configured from the WAN without having to preset a DLCI mapping or IP address. This value is the DLCI number used to open an IP session by the Express 6100/6120. Any IP packet arriving from the PVC is assumed to be for the Express 6100/6120's IP stack. The destination address in the packet is assigned as the PVC's link IP address. The source address is used to add a host route in the routing table. The default is 901, but any legal DLCI number can be used.

BECN Timeout

This value is expressed in milliseconds and represents the amount of time the Express 6100/6120 will stop transmitting over a PVC which received a packet with the BECN bit set. The default is 1.5 seconds.

» Configuration/PPP Profile

The Express 6100/6120 uses the PPP profile to specify the profile used when connected using PPP. *Figure 3-9* shows the PPP profile menu.

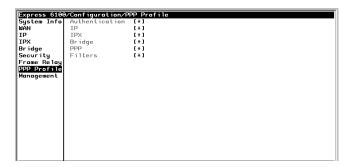


Figure 3-9. Configuration/PPP Profile Screen

»» PPP Profile/Authentication

The authentication menu contains the required parameters for the authentication of the PPP peer and for being authenticated by the PPP peer. Authentication is applied between the Express 6100/6120 and the PPP peer as follows:

Authentication/Tx Method

Write security: 2; Read security: 3

This parameter specifies how the Express 6100/6120 is to be authenticated by the PPP peer. There are four possible selections. See *Security/PPP* on page 3-27 for an explanation of the three PPP standard authentication types.

None (def) The connection will not allow the PPP peer to authenticate it.

PAP, CHAP or The connection can be authenticated using

EAP PAP, CHAP or EAP.

CHAP or EAP The connection can be authenticated using

CHAP or EAP only.

EAP The connection will only allow authentica-

tion by the peer using EAP.

Authentication/Tx Username

Write security: 1; Read security: 3

This is the username that is used when being authenticated by the PPP peer.

Authentication/Tx Password

Write security: 0; Read security: 1

This is the password or secret that is used when being authenticated by the PPP peer.

Authentication/Rx Username

Write security: 1; Read security: 3

This is the username used to authenticate the PPP peer.

Authentication/Rx Password

Write security: 0; Read security: 1

This is the password or secret that is used to authenticate the PPP peer.

»» PPP Profile/IP

The IP menu contains the parameters for exchanging IP data with the PPP peer.

IP/Mode

Write security: 3; Read security: 5

Setting to **On** will permit this connection profile to negotiate PPP IPCP with the PPP peer for exchanging of IP packets. The default is **Off**.

IP/NAT

Write security: 3; Read security: 5

The Express 6100/6120 can perform Network Address Translation. This feature is most widely used when connecting to the Internet. The Ethernet network can consist of private network numbers. When this profile is connected, all IP addresses on the Ethernet side are translated into the one real IP address negotiated with the PPP peer (ISP). Multiple stations on the Ethernet side can access the Internet simultaneously. See the section IP/NAT on page 3-15 for more global options. Setting this option to $\bf On$ will cause the Express 6100/6120 to perform NAT. In the $\bf Off$ (def) position, the unit will route across the connection normally.

IP/Route

The IP parameters are configured in this menu. Usually the Express 6100/6120 will automatically discover the PPP peer's networks using PPP IPCP and/or RIP.

Route/IP/Net

Write security: 3; Read security: 5

The PPP peer's IP address or network can be set here, if known. Leaving this at 0.0.0.0 means that the Express 6100/6120 will determine the PPP peer's IP and network using the PPP IPCP.

Route/Netmask

Write security: 3; Read security: 5

This network mask is applied to the **IP/NET** address for determining the PPP peer's network. If left as 0.0.0.0, a standard network mask is used.

Route/Force IP

Write security: 3; Read security: 5

When set to **Yes**, the Express 6100/6120 will force the PPP peer to use the IP address in the **IP/Net** for this profile as its WAN IP address. Normally this is set in the **No** (def) position.

Link IP

This is the IP address that is assigned to the PPP link when using numbered links. By default, no address is assigned and the PPP link is unnumbered.

IP/RIP

The RIP parameters can be adjusted from their defaults under this menu.

RIP/Mode

Write security: 3; Read security: 5

The Express 6100/6120 performs RIP over the WAN connection when this is set to On.

RIP/Protocol

Write security: 3; Read security: 5

The Express 6100/6120 performs version 1, V1 (def), or version 2, V2, of RIP on this WAN connection.

RIP/Method

Write security: 3; Read security: 5

Split Horizon Only routes not learned on the WAN con-

nection are advertised.

Poison Reverse All routes are advertised, including routes (def)

learned from the WAN connection. These

routes are poisoned.

None All routes are advertised, including routes

> learned from the WAN connection. No attempt is made to poison these routes.

RIP/Direction

Write security: 3; Read security: 5

Tx and Rx (def) RIP advertisements are transmitted and

listened to on the WAN connection.

Tx only RIP advertisements are transmitted and

not listened to.

Rx only RIP advertisements are listened to but not

transmitted.

RIP/Triggered

Write security: 3; Read security: 5

When set to **Yes**, only IP RIP updates are sent when the routing table has changed and learned routes are not "aged." When set to **No** (def), updates are sent periodically.

»» PPP Profile/IPX

The IPX menu contains the parameters for exchanging IPX data with the PPP peer.

IPX/Mode

Write security: 3; Read security: 5

Setting to **On** will permit this connection profile to negotiate PPP IPX-CP with the PPP peer for exchanging of IPX packets.

IPX/Remote Network

Write security: 3; Read security: 5

A non-zero value in this remote network number will allow the Express 6100/6120 to add a route to the PPP peer's network to the routing table.

The Express 6100/6120 normally will treat the WAN network as an unnumbered link. This is usually referred to as being a "half-router." However, a PPP peer which wants to assign a network address to the WAN link can do so, in which case the Express 6100/6120 will go into "full-router" mode.

IPX/Triggered

Write security: 3; Read security: 5

When set to **Yes**, only IPX RIP and SAP updates are sent when the routing or service table has changed and learned routes are not "aged." When set to **No** (def), updates are sent periodically based on the RIP and SAP timers set in **Configuration/IPX/RIP Timer** and **Configuration/IPX/SAP Timer**.

IPX/Type 20 Packets

Write security: 3; Read security: 5

For certain protocol implementations, like NetBIOS, to function in the NetWare environment, routes must allow a broadcast packet to be propagated throughout the IPX networks. The Type 20 IPX packet is used specifically for this purpose. This causes special handling of this packet by the Express 6100/6120. When a router receives this type of packet, it rebroadcasts it across all interfaces except the one it is received on and includes the network number of that interface in the data portion of the packet. The IPX Router Specification from Novell notes that Type 20 packets should not be propagated across slower links with bandwidths of less than 1Mbps (like ISDN). However, when set to **Pass** (def), the Express 6100/6120 will allow these packets to propagate over the WAN connection. This facilitates dial-on-demand applications. When set to **Block**, all Type 20 packets are not propagated across the WAN connection.

»» PPP Profile/Bridge

The Bridge menu contains the parameters needed for exchanging bridged packets with the PPP peer.

Bridge/Mode

Write security: 3; Read security: 5

When set to **On** (def), the Express 6100/6120 will attempt to negotiate PPP BCP with the PPP peer. Bridging can be used even in route mode only if the PPP peer cannot support certain PPP protocols for that particular routing protocol. See *Bridge/WAN IP Bridge* on page 3-22 and *Bridge/WAN IPX Bridge* on page 3-23 for further details.

»» PPP Profile/PPP

The Express 6100/6120 supports the IETF standards for the Point-to-Point Protocol. The PPP state machine running in the Express 6100/6120 can be fine-tuned to support many applications that can be employed. The configurable items under this menu can be changed from their default values for special cases.

PPP/VJ Compression

Write security: 3; Read security: 5

When this item is set to On, the Express 6100/6120 will perform TCP/IP header compression known as Van Jacobson compression to the PPP peer. Normally, this is not necessary over ISDN connections and can be set to Off (def) to disable it.

PPP/Max Config

Write security: 3; Read security: 5

This value is the number of unanswered configuration-requests that should be transmitted before giving up on a call. The possible values are 5, 10 (def), 15 and 20.

PPP/Max Timer

Write security: 3; Read security: 5

This value is the number of seconds to wait between unanswered configuration-requests. The possible values are $1 \sec$, $2 \sec$, (def), $3 \sec$, $5 \sec$, and $10 \sec$.

PPP/Max Failure

Write security: 3; Read security: 5

Due to the nature of PPP, configuration options may not be agreed upon between two PPP peers. This value is the number of configuration-naks that should occur before an option is configuration-rejected. This allows a connection to succeed that might otherwise fail. The possible values are 5 (def), 10, 15 and 20.

»» PPP Profile/Filters

The Express 6100/6120 can block packets in and out of a WAN port by use of the filters. They are set up in two steps: 1) define the types of packets that would be of interest in the **Configuration/Security/Filter Defines** menu, and 2) set up the filter type and combination of defines that will cause a packet block.

Filters/WAN-to-LAN (In)

Write security: 2; Read security: 5

The packets which come into the Express 6100/6120 can be filtered in three ways:

Disabled (def) Turns off packet input filtering. No incoming

packets are blocked.

Block All All incoming packets from the WAN are

blocked except as defined in the Filters/In Ex-

ceptions list.

Forward All All incoming packets from the WAN are not

blocked except as defined in the Filters/In Ex-

ceptions list.

Filters/In Exceptions Write security: 2; Read security: 5

This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

Active	Turns this entry active when set to On.
Туре	Selects the filter define list to reference:
MAC	from the Configuration/Security/Filter Defines/MAC Filter Defines list.
Pattern	from the Configuration/Security/Filter Defines/Pattern Filter Defines list.
IP	from the Configuration/Security/Filter Defines/IP Filter Defines list.
IPX	from the Configuration/Security/Filter Defines/IPX Filter Defines list.
Filter List Name	Selects between filters defined in the list.
Next Oper	The next operation to use to combine with the next filter in the list:
Next Oper END	
-	the next filter in the list:

Filters/LAN-to-WAN (Out) Write security: 2; Read security: 5

The packets which come out toward the WAN from the Express 6100/6120 can be filtered in three ways:

Disabled (def) Turns off packet output filtering. No outgo-

ing packets are blocked.

Block All All outgoing packets to the WAN are blocked

except as defined in the Filters/Out Excep-

tions list.

Forward All All outgoing packets to the WAN are not

blocked except as defined in the Filters/Out

Exceptions list.

Filters/Out Exceptions

Write security: 2; Read security: 5

This is a list of up to 32 filter entries. The setup is exactly the same as the Filter/In Exceptions list.

» Configuration/Management

The Express 6100/6120 can be managed using Telnet, Simple Network Management Protocol (SNMP), or the maintenance port. See *SNMP* on page C-1 for a description of the MIBs supported by the Express 6100/6120. Each of the three methods can be protected using authentication. *Figure 3-10* shows the Configuration/Management menu.



Figure 3-10. Configuration/Management Screen

»» Management/Telnet/Web

Any Telnet client application can bring up a session to the Express 6100/6120's Telnet server using the standard Telnet TCP port. Only one session is supported at a time. All sessions require a user name and password.

Telnet/Web/Server Access

Write security: 2; Read security: 5

This option must be set to \mathbf{On} (def) to access the Express 6100/6120 via Telnet or via a web browser. Turning it \mathbf{Off} means that access is denied.

Telnet/Web/User List

Up to four users can be configured for access to the Express 6100/6120. Each user can be assigned a privilege and time out.

User List/Name

Write security: 1; Read security: 3

A text string of the user name for this session.

User List/Authen Method

Write security: 1; Read security: 3

The user can be authenticated in two ways:

Password The Password field is used to authenticate the us-

er.

Radius The Radius client is used for authenticating the

user.

User List/Password

Write security: 0; Read security: 3

When the authenticating method is password, this text string is used for the password.

User List/Idle Time

Write security: 1; Read security: 3

When set to non-zero, the session is automatically logged out when no activity occurs for this amount of time. The range is 0 to 255 and is in minutes. The default is 10 minutes, and a setting of 0 will never time-out the session. When a timeout occurs during an edit session, all changes are saved.

User List/Level

Write security: 0; Read security: 1

This is the security level privilege that is assigned for this user. See *Security Levels* on page 3-7 for an explanation of what those levels imply. Level 0 is the default.

»» Management/SNMP

The Express 6100/6120 is an SNMP agent. It can respond to Get-Requests, Set-Requests, and generate traps. These two lists set up the manager, communities, and levels. See *SNMP* on page C-1 for more information on SNMP.

SNMP Access

Write security: 3; Read security: 5

When set to No, SNMP access is denied. When set to On (def), the Express 6100/6120 will respond to SNMP managers based on the following lists.

SNMP/Communities

This list is used to set up to eight SNMP communities' names that the Express 6100/6120 will allow. Factory default sets the community "public" with "Get" privileges.

Communities/Name

Write security: 1; Read security: 3

This is a text string for the community name.

Communities/Privilege

Write security: 1; Read security: 3

The access for this manager can be assigned three levels.

None No access is allowed for this community or manag-

er.

Get Manager can only read items.Get/Set Manager can read and set items.

Communities/Manager IP

Write security: 1; Read security: 3

This is the IP address of SNMP manager. If set to 0.0.0.0, any SNMP manager can access the Express 6100/6120 for this community.

SNMP/Traps

The Express 6100/6120 can generate SNMP traps. See *SNMP* on page C-1 for trap types supported. This list allows up to four managers to be listed to receive traps.

Traps/Manager Name

Write security: 2; Read security: 4

This is the text string describing the name of the entry. It is intended for easy reference and has no bearing on the SNMP trap function.

Traps/Manager IP

Write security: 2; Read security: 4

This is the IP address of the manager that is to receive the traps.

»» Management/Maint Port

The Express 6100/6120 has an EIA-232 connector on the back of the unit. The setup for that port is under this menu.

Maint Port/Password Protect

Write security: 0; Read security: 1

When set to No, the maintenance port is not password protected. When On (def), the Express 6100/6120 will prompt for a password upon startup.

Maint Port/Password

Write security: 0; Read security: 1

This is the text string that is used for comparison when password protecting the maintenance port. By default, no password is entered.



The security level for the maintenance port is always set to 0. This gives full access to all menus.

Maint Port/Baud Rate

Write security: 5; Read security: 5

This is the asynchronous rate that the maintenance port will run. The possible values are 300, 1200, 2400, 4800, 9600 (def), 19200, 38400, 57600, 115200.

Maint Port/Data Bits

Write security: 5; Read security: 5

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

Maint Port/Parity

Write security: 5; Read security: 5

This is the asynchronous parity that the maintenance port will run. The possible values are **None** (def), **Odd**, or **Even**.

Maint Port/Stop Bits

Write security: 5; Read security:5

This is the stop bit used for the maintenance port. The possible values are 1 (def), 1.5 or 2.

» Configuration/Terminal Mode

This is an activator which places the Express 6100/6120 terminal session into a command prompt mode. All menu options are accessible during this mode. See *Terminal Mode Commands* on page E-1 for the command structure and command list. Type **exit** to leave the terminal mode and return to the menus.

> STATUS MENU

The Express 6100/6120's Status menu contains comprehensive status and diagnostic information used in verifying configuration and identifying problems. The menus are divided into protocol types and sessions. *Figure 3-11* shows the Status menu.

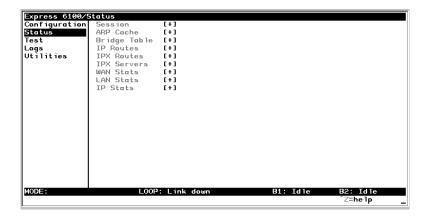


Figure 3-11. Status Screen

» Status/Sessions

This menu contains the current status of all sessions and spanning tree ports.

»» Sessions/PPP Session

Read security: 5

This menu reflects the results of PPP negotiations, user name, time connected, and data rates for the session.

PPP Links Reflects LCP layer active

BCP Shows UP if PPP Bridge Control Proto-

col has negotiated successfully

IPCP	Shows UP if PPP IP Control Protocol
------	-------------------------------------

has negotiated successfully

IPXCP Shows UP if PPP IPX Control Protocol

has negotiated successfully

Up Time Displays how long the call has been

connected

Tx Pkts Number of packets transmitted **Rx Pkts** Number of packets received Tx Bytes Number of bytes transmitted **Rx Bytes** Number of bytes received

Tx Rate Current application data transmission

Rx Rate Current application data reception rate

»» Sessions/Frame Relay

Frame Relay/Port

Shows Frame Relay statistics for the WAN port.

Port Index Always displays 0

Displays "up" when the Express 6100/ Signal State

6120 is communicating with the Frame

Relay switch; otherwise displays

"down"

Tx Frames Total packets transmitted out **Rx Frames** Total packets received from port Tx Bytes Total bytes transmitted out port **Rx Bytes** Total bytes received from port **Tx Throughput** Current transmit rate for port **Rx Throughput** Current receive rate for port Signal Tx Frames Number of Frame Relay signalling

packets transmitted out port

Signal Rx Frames Number of Frame Relay signalling

packets received from port

Drop Unknown DLCI Number of frames received that were

not associated with any known PVC

Drop Invalid DLCI Number of frames received that had il-

legal DLCIs

Frame Relay/DLCI Table

The status of all virtual circuits is displayed here.

DLCI The DLCI that is associated with this virtual

circuit.

State The state of the virtual circuit:

Inactive means the circuit exists but has been deacti-

vated by the Frame Relay switch.

Exists means the circuit exists at this point and

should be activated soon.

Active means the circuit is fully active.

Off means the circuit has been turned off by the

DLCI mapping active selection.

Tx Frames Number of Frame Relay packets that have

been transmitted via this DLCI.

Rx Frames Number of Frame Relay packets that have

been received via this DLCI.

Tx Bytes Number of Frame Relay bytes that have been

transmitted via this DLCI.

Rx Bytes Number of Frame Relay bytes that have been

received via this DLCI.

IP Sublfc The IP router port assigned for this DLCI.

Possible ports are fr0, fr1, ..., fr9. None

means that this DLCI not used for routing IP.

IPX Sublfc The IPX router port assigned for this DLCI.

Possible ports are fr0, fr1, ..., fr9. None means that this DLCI not used for routing IPX.

Bridge Group The bridge group that this DLCI belongs to

(Group 1 or Group 2). None means that this

DLCI is not used for bridging.

Tx Throughput Current transmit rate of this DLCI **Rx Throughput** Current receive rate of this DLCI

De Count Number of packets received on this DLCI

with the De bit set

Cr Count Number of packets received on this DLCI

with the Cr bit set

Becn Count Number of packets received on this DLCI

with the Becn bit set

Fecn Count Number of packets received on this DLCI

with the Fecn bit set

»» Sessions/Spanning Tree

Read security: 5

When Bridge mode and Spanning Tree mode are active, this reflects the current state of the LAN and WAN ports. The following can appear:

Off Appears when Spanning Tree mode is disabled

Disabled Port is not connected (for WAN) or disabled in

configuration

Listening Port is in the listening state **Learning** Port is in the learning state

Forwarding Port is in the forwarding state with the follow-

ing possible properties:

root is the root port designated is designated port

Blocking Port is in the blocked state

» Status/ARP Cache

Read security: 5

This lists the contents of the Express 6100/6120's ARP table. All resolved cache entries time out after 20 minutes. Unresolved entries time out in 3 minutes.

»» ARP Cache/IP Address

IP address used for resolving MAC address.

»» ARP Cache /MAC Address

Ethernet address resolved (0=no resolution).

»» ARP Cache/Time

Minutes since entry was first entered.

» Status/Bridge Table

Read security: 5

This lists the contents of the Express 6100/6120's bridge table.

»» Bridge Cache/MAC Address

Ethernet address for device learned.

»» Bridge Cache/Port

Port device learned from: **LAN**, **WAN0**, or **WAN1**. **WAN0** and **WAN1** represent Bridge Group 1 and Bridge Group 2, respectively.

»» Bridge Cache/TTL

Seconds until address is removed from table.

» Status/IP Routes

Read security: 5

This lists the contents of the Express 6100/6120's IP router table.

»» IP Routes /IP Address

Network or host destination address.

»» IP Routes /Netmask

Network mask applied to the destination address.

»» IP Routes /Gateway

Host or router to receive this packet.

»» IP Routes /Port

Port gateway is located on:

local	sent directly to the Express 6100/6120 router
eth0	Express 6100/6120's ethernet port
wan0	Express 6100/6120's first PPP bundle
fr 0 fr 9	Express 6100/6120 is connected up to 10 DLCIs

»» IP Routes /Use

Number of times the Express 6100/6120 has referenced the route.

»» IP Routes/Flags

Important tags associated with this route entry:

- **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 (updates only when table changes)

»» IP Routes/Hops

Number of routers that must go through to get to destination. Ranges from 0-15 or 16 for infinite (can't get there from here).

»» IP Routes/TTL

Seconds until address is removed from table or "zombied." Value of 999 means route is static.

» Status/IPX Routes

Read security: 5

This lists the contents of the Express 6100/6120's IPX router table.

»» IPX Routes /Network

Network destination address.

»» IPX Routes /Gateway

Node or Ethernet address of gateway to receive this packet.

»» IPX Routes /Port

Port gateway is located on

local	sent directly to the Express 6100/6120 router
eth0	Express 6100/6120's ethernet port
wan0	Express 6100/6120's first PPP bundle
fr 0 fr 9	Express 6100/6120 is connected up to 10 DLCIs

»» IPX Routes/Use

Number of times the Express 6100/6120 has referenced the route.

»» IPX Routes/Hops

Number of routers that must go through to get to destination. Ranges from 0-15 or 16 for infinite (can't get there from here).

»» IPX Routes/Ticks

Router determined value for representing time packets take to reach the network destination. One tick is equivalent to one-eighteenth of a second.

»» IPX Routes/TTL

Seconds until address is removed from table. Value of 999 means route is static.

» Status/IPX Servers

Read security: 5

This lists the contents of the Express 6100/6120's IPX server table.

»» IPX Servers/Type

The server type

»» IPX Servers/Name

The server name

»» IPX Servers/Network

The server network address

»» IPX Servers /Address

The servers node address

»» IPX Servers/Socket

The servers socket address

»» IPX Servers/Hops

Number of routers that must go through to get to server. Ranges from 0-15 or 16 for infinite.

»» IPX Servers/TTL

Seconds until address is removed from table. Value of 999 means server is static.

» Status/WAN Stats

Read security: 5

This menu contains generic WAN statistics on HDLC hardware port.

HDLC Port

Tx Bytes total number of raw bytes sent out HDLC port 1
Rx Bytes total number of raw bytes received in HDLC

port 1

Rx CRCs total number of CRC errors detected on HDLC

port 1

Clear Counts When activated, clears all WAN stat counts

» Status/LAN Stats

Read security: 5

This menu contains statistics for the Ethernet port.

Tx PacketsPackets transmitted out the Ethernet portRx PacketsPackets received from the Ethernet portTx ErrorsTotal transmit errors encountered on

Ethernet port

Single Collisions total single collisions before successful

transmission

Multiple total multiple collisions before successful

Collisions transmission

Excessive total collisions that resulted in packet be-

Collisions ing dropped

Deferred total packets deferred due to collisions

Transmissions

Carrier Sense total carrier sense errors encountered (no

Errors link integrity)

Rx Errors Total packets received in error and

dropped

CRCs total packets detected with CRC errors

Giants total packets received that were greater

than 1518 bytes

Runts total packets received that were less

than 64 bytes

Rx Collisions total collision occurred during reception

Clear Counts When activated, clears all LAN Stat

counts.

» Status/IP Stats

Read security: 5

This menu contains IP statistics that can be useful when diagnosing problems. All are taken from the SNMP MIB-2 variables.

Active TCP connections

Bad header packets

Bad IP addresses

Bad protocol discards

Clear Counts - clears all IP stats

Datagrams discarded

Default TTL

Disassembled fragments

Discarded routing entries

Errorfree discards

Failed fragments

ICMP messages received

ICMP messages sent

ICMP packet errors

ICMP redirected messages

ICMP specif if errors

ICMP timeouts received

IP datagrams reassembled

IP datagrams received

IP datagrams sent

IP reassembly failures

IP reassembly timeout

No application at dest. port

Routeless discards

Sent datagrams to upper layers

Successful fragments

TCP current connections

TCP failed attempts

TCP passive connections

TCP segments received

TCP segments sent

Total forwarded datagrams

Total IP fragments

Total TCP resets

Total TCP retransmits

UDP bad packets

UDP datagrams received

UDP datagrams sent

> TEST MENU

The Express 6100/6120's Test menu contains built-in tests that can be used to diagnose problems. *Figure 3-12* shows the Test menu screen.

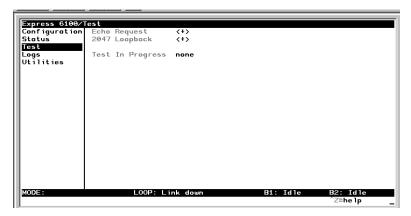


Figure 3-12. Test Screen

The following tests can be run:

» Test Menu/Echo Request

Write security: 4, Read security: 5

When activated, the echo request test will begin sending continuous PPP echo request packets to any open LCP ports. Results are displayed on the screen. This is not used in the Frame Relay mode.

> LOGS MENU

The Logs menu contain logs displaying important information about the running condition of the Express 6100/6120. The logs can be set to capture diagnostics of error conditions only by way of a log level. The levels are divided up as follows:

- level 0 Fatal event (causes reset)
- level 1 Critical event
- level 2 Error event
- level 3 Warning event
- level 4 Notify event
- level 5 Informational event
- level 6 Debugging event

Figure 3-13 shows the Logs menu. The three logs available are listed after the figure.

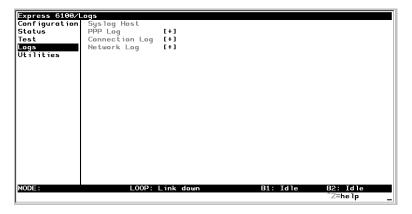


Figure 3-13. Logs Screen

» Logs/Sys log Host

Set this to the IP address or domain name (if DNS configured) of the sys log host device. All log events are sent to this device.

» Logs/PPP Log

Information pertaining to the PPP negotiation and authentication will be logged here.

»» PPP Log/Active

When set to **Yes** (def), PPP events below or equal to the log level are logged into the log.

»» PPP Log/Wrap

When set to **Yes** (def), new PPP events will overwrite old PPP events when the log is full. All logging will stop when the log is full and set to **No**.

»» PPP Log/Level

In order to log events, they must be at or below this level. Range is 0 to 6. The default is 3.

»» PPP Log/View

This menu displays the log list. The fields are as follows:

Date/Time Date and time event occurred.

Level Level associated with this event (0-6).

Message Text message for this event. If message is too long

to fit on the line, another event appears below it

continuing the message.

»» PPP Log/Clear

This clears the log when activated.

» Logs/Connection Log

Information pertaining to the connection over the IDSL link.

»» Connection Log/Active

When set to **Yes** (def), connection events below or equal to the log level are logged into the log.

»» Connection Log/Wrap

When set to **Yes** (def), new connection events will overwrite old connection events when the log is full. All logging will stop when the log is full and set to **No**.

»» Connection Log/Level

To log events, they must be at or below this level. Range is 0 to 6. The default is 3.

»» Connection Log/View

This menu displays the log list. The fields are as follows:

Date/Time Date and time event occurred.

Level Level associated with this event (0-6).

Message Text message for this event. If message is too long

to fit on the line, another event appears below it

continuing the message.

»» Connection Log/Clear

This clears the log when activated.

» Logs/Network Log

Information pertaining to the routing protocols is placed in this log.

»» Network Log/Active

When set to **Yes** (def), call events below or equal to the log level are logged into the log.

»» Network Log/Wrap

When set to **Yes** (def), new Network events will overwrite old Network events when the log is full. All logging will stop when the log is full and set to **No**.

»» Network Log/Level

To log events, they must be at or below this level. Range is 0 to 6. The default is 3.

»» Network Log/View

This menu displays the log list. The fields are as follows:

Date/Time Date and time event occurred.

Level Level associated with this event (0-6).

Message Text message for this event. If message is too long

to fit on the line, another event appears below it

continuing the message.

»» Network Log/Clear

This clears the log when activated.

> UTILITIES MENU

The Express 6100/6120 has utilities embedded in it to help in managing and testing the network and to facilitate software upgrades. *Figure 3-14* shows the Utilities menu.

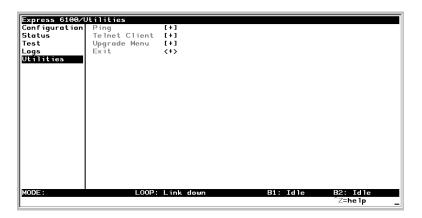


Figure 3-14. Utilities Screen

» Utilities/Ping

Write security: 4; Read security: 5

The ping menu is used to send ICMP ping messages to hosts. The following items are under this menu:

Start/Stop	Activator to start and cancel a ping test.
Host Address	IP address or domain name (if DNS is configured) of device to receive the ping
Size	Total size of ping to send. Range is 40 (def) to 1500 bytes.
# of Packets	Total packets to send every two seconds
# of Transmits	Total packets sent (read only)
# of Receives	Total packets received (read only)
% Loss	Percentage loss based on ping returned form host (read only)

» Utilities/Telnet Client

Write security: 4; Read security: 5

The Telnet menu can be used to activate the Telnet client function in the Express 6100/6120.

Host IP address or domain name (if DNS is configured)

of Telnet server. By default, the standard TCP server port is used. However, a nonstandard port can be specified here with the IP address or domain name

separated by a colon (:).

Activate Starts Telnet client function. The key combination

Control] cancels the session.

» Utilities/Upgrade Menu

Write security: 2; Read security: 3

The Express 6100/6120's firmware can be upgraded using this menu.

»» Upgrade/Transfer Method

The two methods for upgrading are **TFTP** and **XMODEM**. **TFTP** requires a TFTP server running somewhere on the network. The Express 6100/6120 starts a TFTP client function which gets the upgrade code from the TFTP server. Selecting **XMODEM** will load the upgrade code through the maintenance port using any PC terminal emulator with xmodem capability.

»» Upgrade/TFTP Host

This is required when the transfer method is TFTP. It is the IP address or domain name (if DNS is configured) of the TFTP server.

»» Upgrade/Filename

This is required when the transfer method is TFTP. It is the case-sensitive file name which is the upgrade code.

»» Upgrade/Status

This appears when TFTP is used. It displays the status of the transfer as it happens. Any error or success message will be displayed here.

»» Upgrade/Start Transfer

This activator is used when the configurable items in this menu are complete.



Once started, the Express 6100/6120 will prompt for erasing the flash. When the flash is erased and the upgrade transfer fails, do not turn off the unit. Retry the transfer until successful. Otherwise, if power is removed before upgrade has finished, the upgrade will have to occur from the maintenance port using XMODEM. If this happens, set a PC terminal emulation program to 9600 baud and attach to the Express 6100/6120's maintenance port. Press Return to display a simple terminal menu for upgrading. This menu appears when the flash code has been erased or is corrupt. The menu will also appear if you power up with the back panel switch one in the up position.

»» Upgrade/Abort Transfer

Use this activator to cancel any TFTP transfer in progress.

»» Upgrade/TFTP Server

Setting this to **Yes** allows another Express 6100/6120 to upgrade its code using TFTP client. This, in effect, turns on the Express 6100/6120 TFTP server function and allows its code to be "cloned." Setting to **No** (def) will deny any request from TFTP clients.

» Utilities/Exit

Write security: 5; Read security: 5

Activating this feature will exit the terminal session from the maintenance port or Telnet. It is equivalent to the key combination **Control L**.

Chapter 4 Specifications

SPECIFICATIONS AND FEATURES

This section lists the standard specifications and features incorporated in the Express 6100/6120.

Network Interface

- RJ-45 for IDSL two-wire service
- Signal Format: 2B1Q
- Max distance per loop: 15 kft at 26 AWG

Ethernet Interface (LAN)

Ethernet/IEEE 802.3 10BaseT

Display

Available through terminal interface or Telnet session

Environmental

- Operating Temperature: 0 50 °C
- Storage Temperature: 20 70 °C
- Relative Humidity: Up to 95% non-condensing

Physical

- Dimensions: 1 1/2" H x 6 1/2" W x 4" D
- Weight: 9.5 oz.

Power

120 VAC, 60 Hz, 8 W typical

Appendix A Loop Status Messages

The Express 6100/6120 displays current loop status of the IDSL on the bottom center line of the terminal screen. The following messages are defined:

Connected

This is seen when the Express 6100/6120 IDSL layer 1 is up. The rate is determined by what it is configured for under **Configuration/WAN/IDSL/Rate**.

Echo: Tx: X Rx: Y

The current transmit and receive count for the PPP echo request test.

Layer 1 up

The Express 6100/6120's IDSL layer 1 is up.

Link down

The IDSL link is not synchronized.

Link In Sync

The IDSL link is synchronized but layer 1 is not up.

NET EOC LOOPBACK

Express 6100/6120 has received an IDSL EOC loopback command from the far end.

RINGING

An incoming call is ringing.

Rate Status Messages

Displays the rate at which the connection has been established. \\

Appendix B Log Messages

The Express 6100/6120 Logs menu contains messages of events that occur. The definitions for some of those log messages are as follows:

PPP LOG MESSAGES

BCP <X> down

level 5

Bridge Control Protocol port <X> has been dropped between Express 6100/6120 and PPP peer.

BCP <X> up

level 5

Bridge Control Protocol port <X> has been successfully negotiated between Express 6100/6120 and PPP peer.

CCP <X> down

level 5

Compression Control Protocol port <*X*> has been dropped between Express 6100/6120 and PPP peer.

CCP <X> up

level 5

Compression Control Protocol port <X> has been successfully negotiated between Express 6100/6120 and PPP peer.

CHAP authen failed

level 3

The PPP peer has rejected the Express 6100/6120's username and/or password used for authenticating. Check to make sure the Configuration/Connection List/Authentication parameters Tx Method, Tx Username, and Tx Password are correct.

EAP authen failed

level 3

The PPP peer has rejected the Express 6100/6120's username and/or password used for authenticating. Check to make sure the Configuration/Connection List/Authentication parameters Tx Method, Tx Username, and Tx Password are correct.

IPCP <X> down

level 5

IP Control Protocol port <X> has been dropped between Express 6100/6120 and PPP peer.

IPCP <X> up

level 5

IP Control Protocol port <X> has been successfully negotiated between Express 6100/6120 and PPP peer.

IPXCP <X> down

level 5

IPX Control Protocol port <X> has been dropped between Express 6100/6120 and PPP peer.

IPXCP <X> up

level 5

IPX Control Protocol port <X> has been successfully negotiated between Express 6100/6120 and PPP peer.

LCP <X> down

level 5

Link Control Protocol port <X> has been dropped between Express 6100/6120 and PPP peer.

LCP <X> up

level 5

Link Control Protocol port <X> has been successfully negotiated between Express 6100/6120 and PPP peer.

Link is looped back

level 3

The Express 6100/6120 has dialed a location which is looping back all data. Essentially, it has negotiated PPP with itself.

Negot not converging

level 2

Negotiation of the LCP layer is unattainable due to misconfiguration or the Express 6100/6120 or PPP peer is requiring authentication and the other is refusing.

No IP addr for peer

level 2

The Express 6100/6120 cannot continue the connection because there was no IP address received from the PPP peer or it was not set in **Configuration/Connection List/IP/Route/IP/Net** parameter.

No Response from peer

level 2

The Express 6100/6120 has dialed or answered a call and no PPP negotiation packets were seen.

PAP authen failed

level 3

The PPP peer has rejected the Express 6100/6120's username and/or password used for authenticating. Ensure that the Configuration/Connection List/Authentication parameters Tx Method, Tx Username, and Tx Password are correct.

Peer failed CHAP authen

level 3

The PPP peer's reported CHAP username and/or password does not match the Express 6100/6120's parameters. This is most likely caused by PPP peer sending an incorrect username and/or password. Make sure the **Configuration/Connection List/Authentication** parameters **Rx Username** and **Rx Password** are correctly entered. Also, if using RADIUS, check that the server is configured and running properly.

Peer failed EAP authen

level 3

The PPP peer's reported EAP username and/or password does not match the Express 6100/6120's parameters. This is most likely caused

by PPP peer sending incorrect username and/or password. Make sure the **Configuration/Connection List/Authentication** parameters **Rx Username** and **Rx Password** are correctly entered. Also, if using RADIUS, check that the server is configured and running properly.

Peer failed PAP authen

level 3

The PPP peer's reported PAP username and/or password does not match the Express 6100/6120's parameters. This is most likely caused by PPP peer sending incorrect username and/or password. Make sure the **Configuration/Connection List/Authentication** parameters **Rx Username** and **Rx Password** are correctly entered. Also, if using RADIUS, check that the server is configured and running properly.

Peer refused authen

level 3

The PPP peer would not allow the Express 6100/6120 to authenticate it using the method set in **Configuration/Security/PPP**.

Peer refused SpanTree

level 4

The PPP peer would not participate in the Spanning Tree protocol. This is a warning message only. Bridging will still occur across the WAN port so care must be taken that no loop topologies exist across the connection.

PPPtx[x] ...

level 6

Advance debugging decode of transmitted PPP configuration packets.

PPPrx[x] ...

level 6

Advanced debugging decode of received PPP configuration packets.

CALL LOG MESSAGES

Power Up - last down cause: <reason>

level 0 (displayed as level 1 after the unit is reset)

This is the <reason> for the last reset. Most are caused by internal errors. Possible reasons are:

Bus Error - Bad address occurred on the internal bus

Kernel error - General operating system error

No SBCs - Mail resources used up or lost

Router stack error - Fatal error in protocol stack

general panic - general error

no rip - rip tasks could not start

out of memory - out of available memory

out of TCP ports - all TCP ports are used up

unknown error - unknown fatal error has occurred

Set timer error - Cannot set real-time clock

Software Watch Dog Reset - Software watchdog was not updated

NETWORK LOG MESSAGES

Attempting to add bad IP iface route: ifnum=<inter> dest=<ip>

level 4

An IP address <ip> could not be used for the interface number <inter>.

DHCP couldn't alloc mem

level 1

A DHCP response could not be generated due to memory allocation problems.

DHCP response sent

level 4

A DHCP response was successfully sent to requesting device.

DHCP socket failed

level 1

Internal error occurred when attempting to start DHCP server.

DHCP: Host not added to ARP table

level 2

The DHCP server could not add requesting host to ARP table.

Installing bad default route: ifnum=<inter> metric=<hops> gw=<ip>

level 6

The Express 6100/6120 did not install a default route because the <inter> or <hops> was zero.

Rejecting packet with Source Routing option - src=<srcip> dest=<destip>

level 4

The Express 6100/6120 has dropped a source routed IP packet due to invalid parameters.

setmask: local IP iface(0), not done

level 6

Debug error used in determining router stack problems.

syslog: bad host

level 2

Syslog function cannot use host name or IP set in **Configuration/ Logs/Syslog Host**.

syslog: no port

level 2

Syslog function cannot open port to send Log entries.

TEL: Telnet Session Closed

level 4

Telnet server session has been closed.

telclient bad host

level 2

Telnet client could not use host name or IP address set in **Configuration/Utilities/Telnet Client/Host**.

telclient bad init

level 2

Telnet client could not initialize a session.

Telnet Client: Clr TCBF_BUFFER flag failed

level 6

Debugging message related to Telnet client function.

Telnet Client: Set TCBF_DONTBLOCK flag failed

level 6

Debugging message related to Telnet client function.

Telnet Client socket failed

level 2

Telnet client function could not open TCP socket.

Telnet server connect to <ip>

level 4

Telnet server has connected to Telnet client with IP address <ip>.

Telnet Session Closed

level 4

Telnet server has closed connection.

Telnet Session failed, error <errnum>

level 2

Telnet server could not connect to Telnet client due to error.

TELNETD: accept failed

level 2

Telnet server could not open TCP socket to incoming Telnet client.

TELNETD: Set TCPC_LISTENQ failed

level 6

Debugging message related to Telnet server function.

TELNETD: Clr TCBF_BUFFER flag failed

level 6

Debugging message related to Telnet client function.

TELNETD: could not obtain peer ip

level 2

Telnet server function could not get IP address of Telnet client.

TELNETD: Session failed, error

level 2

A Telnet server session has failed because of an error.

TELNETD: Set TCBF_DONTBLOCK flag failed

level 6

Debugging message related to Telnet client function.

TELNETD: SOCKET creation error

level 2

Telnet server could not be started due to TCP socket error.

TFTP: can't get to host

level 2

TFTP client could not get to host.

TFTP client: unable to open port

level 2

TFTP client function could not open a UDP port.

TFTP: error rcvd - <message>"

level 2

Received error with <message> from TFTP server.

TFTP: lost communication

level 2

Lost communication to TFTP client or server during transfer.

TFTP server: unable to open port

level 2

TFTP server function could not open a UDP port.

Appendix C SNMP

UNDERSTANDING SNMP

As Local Area Network (LAN) environments became standardized over the past ten years, multi-vendor equipment grew with competition. It became necessary to manage the various vendor equipment from a single control console. Thus, the Simple Network Management Protocol (SNMP) emerged as the *de facto* standard for managing commercial Transmission Control Protocol/Internet Protocol (TCP/IP) networks.

The term *SNMP* broadly refers to the message protocols used to exchange information between the network and the managed devices, as well as to the structure of network management databases. SNMP has three basic components:

- Network Manager: This 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: This 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 connected.
- MIB: This is an index to the organized data within a network device. It defines the operating parameters that can be controlled or monitored.

When requesting the network manager to retrieve or modify a particular piece of information about a network device, the network manager transmits the request to that network device. The agent in that device interprets the incoming request, performs the requested task, and sends its response to the network manager. The network manager.

er collects all the data from the various network devices and presents it in a consistent form.

Using SNMP Version 1, the network manager can issue three types of commands:

- **GetRequest**: This command retrieves a single item or the first in a series from a network device.
- **GetNextRequest**: This command retrieves the next item in a series from a network device.
- SetRequest: This command writes information to a network device.

The network device issues two types of messages:

- **GetResponse**: This message is the response to a network manager **GetRequest** or **GetNextRequest** command.
- **Trap**: This is an unsolicited message issued by a network device to report an operational anomaly or an alarm condition to the network manager.

These messages are typically encased within informational packets and transported over the LAN or WAN.

SNMP EMBEDDED AGENT

The Express 6100/6120 supports the following groups from MIB-II: (RFC 1213)

- System Group
- UDP Group
- Interfaces Group
- ICMP Group
- Address Translation Group
- IP Group
- TCP Group

Also, the Ethernet transmission MIB is supported (RFC 1643).

The following manager requests are supported:

- Get object
- Get next object
- Set object

Communities

The Express 6100/6120 permits up to eight communities to be defined. The privilege level of each community can be set. The default community is public with read-only privileges. When the IP address is all zeros, any manager of the community can access the Express 6100/6120.

Traps

Up to four hosts can be set to receive traps. Each host entry requires an IP address of the manager.

Trap types supported are: cold start, link up, link down, and authentication failure.

Appendix D Connector Pinouts

Table D-1. IBM/AT Style EIA-232 Interface

	Pin	Name	I/O	Description
	1	CD	N/C	Carrier Detect
	2	RD	0	Receive Data
()	3	TD	I	Transmit Data
<i>></i>	4	DTR	N/C	Data Terminal Ready
	5	GND	N/A	Signal Ground
	6	DSR	N/C	Data Set Ready
	7	RTS	I	Request to Send
	8	CTS	0	Clear to Send
	9	RI	N/C	Ring Indicator

I = Input, O = Output, N/A = Not Applicable, N/C = Not Connected

Table D-2. RJ-49C ISDN

ISDN	Pin	Description
///////\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	4	Ring
\/	5	Tip

Table D-3. 10BaseT Ethernet

6100	Pin	Signal
	1	RX1
10BT 	2	RX2
	3	TX1
	6	TX2
6120		·
10BT	1	TX1
	2	TX2
	3	RX1
	6	RX2

Appendix E Terminal Mode Commands

The Express 6100/6120 supports a command line interface. All menu options are configurable and readable from the terminal mode. Additional commands are also available.

MENU COMMANDS

Every menu item in the menu structure can be accessed through the terminal mode interface. Terminal commands are as follows:

top_menu sub_menu1 sub_menu2 ... config_item

Each config_item is entered as shown below.

TYPE:	ENTERED AS:
string	printable characters within double quotes
password	printable characters within double quotes
IP address	xx.xx.xx.xx (09) separated by '.'
Hex	xx:xx:xx:xx (09,af) separated by ':'
enum	sub-string or [#index]
unsigned	digits (09)
date	mm-dd-yyyy
time	hh:mm:ss
date/time	mm-dd-yyyy hh:mm:ss
activator	read only
list	followed by index with first record being 1
array	followed by index with first record being 1

One of the following key words must be used first:

KEYWORD:	GOES DIRECTLY TO:
info	Configuration/System Info menu.
idsl	Configuration/WAN/IDSL menu.
ip	Configuration/IP menu.
ipx	Configuration/IPX menu.
bridge	Configuration/Bridge menu.
security	Configuration/Security menu.
ррр	Configuration/PPP Profile menu.
telnet	Configuration/Management/Telnet menu.
snmp	Configuration/Management/SNMP menu.
maint	Configuration/Management/Maint menu.
status	Configuration/Status menu.
test	Configuration/Test menu.
logs	Configuration/Logs menu.
util	Configuration/Utilities menu.
frame	Configuration/WAN/Frame Relay menu

Some examples are listed below:

telnet user 1 name "guest"	sets user name for Telnet user list entry 1 to "guest"
test 2047	starts 2047 test
status ip 1 gateway	returns the gateway address for IP route table entry 1

ADDITIONAL COMMANDS

Other commands available from the terminal mode are listed below:

save	Saves the configuration to non-volatile RAM (flash).
mac	Returns the MAC address for the Express 6100/6120.
version	Returns the firmware version and routing stack version.
reset	Resets the unit.
exit	Leaves terminal mode and returns to menus.
download	Downloads complete configuration to the terminal screen for capture.

DOWNLOAD/UPLOADING CONFIGURATION

The Express 6100/6120's configuration can be captured to a text file using the download command. The text file can be edited if required. Upload of the configuration can be accomplished by sending the text file to the Express 6100/6120 in terminal mode. A baud rate of 9600 is strongly recommended when uploading. As soon as the upload has been completed, type **save** to save the new configuration to flash. A **reset** command or power cycle 10 seconds after the save command is recommended to ensure that the new configuration is complete.

Acronyms

AEP AppleTalk Echo Protocol

AMI Alternate Mark Inversion

ARP Address Resolution Protocol

B (Channel) A 64 kbps digital information channel

BCP Bridge Control Protocol

BONDING Bandwidth On Demand Interoperability

Group

BOOTP Bootstrap Protocol

BPDU Bridging Protocol Data Unit

bps Bits per second
Bps Bytes per second
BRI Basic Rate Interface
CA Call Appearance

CCP Compression Control Protocol

CCITT Consultative Committee for International

Telegraphy and Telephony

CD Carrier Detect

CPE Customer Premises Equipment
CRC Cyclic Redundancy Check

CSMA/CD Carrier Sense Multiple Access Collision

Detect

DHCP Dynamic Host Configuration Protocol

DLCI Data Link Connection Identifier
DMS Digital Multiplex Switching
DTE Data Terminal Equipment

DTMF Dual Tone Multi-Frequency

EKTS Electronic Key Telephone Service

ESS Electronic Switching System

FAX Facsimile

FEBE Far End Block Errors
FTP File Transfer Protocol

ICMP Internet Control Message Protocol

ID Identification

IETF Internet Engineering Task Force

I/O Input/Output
IP Internet Protocol

IPCP Internet Protocol Control Protocol
IPX Internetwork Packet Exchange

Integrated Injected LogicIECInter-Exchange Carrier

ISDN Integrated Services Digital Network

ISO International Standardization

Organization

ISP Internet Service Provider

kbps Kilobits per second

kHz Kilohertz

LAN Local Area Network
LCP Link Control Protocol
LDN Local Directory Number
MAC Media Access Control

MIB Management Information Base

MP Multilink Protocol

MRU Maximum Receivable Unit

MRRU Maximum Receivable Reconstructable

Unit

NBP Name Binding Protocol
NEBE Near End Block Errors
NIC Network Interface Card

NI-1 National ISDN-1

NT Network Termination
PBX Private Branch Exchange

PC Personal Computer

PING Packet InterNet Groper

POTS Plain Old Telephone Service

PPP Point-to-Point Protocol
PRI Primary Rate Interface
RFC Request For Comments

RIP Routing Information Packet, Routing

Information Protocol

RTMF Routing Table Maintenance Protocol

SAP Service Advertising Protocol

SNMP Simple Network Monitoring Protocol SPCS Stored Program Controlled Switching

System

SPID Service Profile Identifier

TCP Transmission Control Protocol
TEI Terminal Endpoint Identifier
TFTP Trivial File Transfer Protocol
UDP User Datagram Protocol
WAN Wide Area Network

ZIP Zone Information Protocol

Glossary

10Base2

IEEE 802.3 specification, similar to Ethernet, using thin coaxial cable that runs at 10 Mbps, with a maximum distance of 185 meters per segment. Also known as Thin Ethernet or Thinwire Ethernet.

10BaseT

IEEE 802.3 specification, using unshielded twisted-pair cabling and running at 10 Mbps.

AEP

AppleTalk Echo Protocol. Allows a node on an AppleTalk network to send a packet to another node and in return, receive an echoed copy of the packet.

B-Channel

64 kbps bearer channel used for voice, circuit, or packet switched data.

bearer service

As defined by CCITT standards, a type of telecommunication service that provides the capability for the transmission of information between user-to-network interfaces. Bearer services defined for ISDN are circuit mode and packet mode.

BOOTP

The Bootstrap Protocol allows a network node to determine certain startup information such as its IP address.

Bridge

A data communications device that connects two or more networks. A bridge stores and forwards complete packets between the networks. Bridges operate at the data-link layer of the OSI model.

CCITT

Consultative Committee on International Telephony and Telegraphy. A body of the International Telegraph Union (ITU) which prepares recommendations, commonly referred to as international standards, to resolve technical telegraph and telephone problems.

central office (CO)

In telephony, the phone company switching facility or center, usually a Class 5 end office, at which subscribers local loops terminate. Handles a specific geographic area, identified by the first three digits of the local telephone number. Usually the facilities of the local BOC.

CSMA/CD

Carrier Sense Multiple Access Collision Detect. A channel access mechanism where devices check the channel for a carrier before transmitting. If no carrier is sensed for the specified period of time, the device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays their retransmissions for a random length of time. CSMA/CD is used by Ethernet and IEEE 802.3.

D-channel

The ISDN channel that carries signalling information to control the call setup, teardown, or invocation of supplementary services. The D-Channel may also be used to provide packet mode data service.

DDS

Dataphone Digital Service. AT&T private line service for transmitting data over a digital system. The digital transmission system transmits electrical signals directly, instead of translating the signals into tones

of varied frequencies as with traditional analog transmission systems. Digital techniques provide more efficient use of transmission facilities, resulting in lower error rates and costs than analog systems.

digital hub

Designated office where DDS channels are interconnected and where synchronous network timing, testing access, and additional service features are provided.

Ethernet

A local area network used for connecting computers, printers, workstations, a terminals, servers, etc., within the same building or campus. Ethernet operates over twisted wire and coaxial cable at speeds up to 10 Mbps. Ethernet specifies a CSMA/CD.

four-wire circuits

Telephone lines using two wires for transmitting and two wires for receiving, offering much higher quality than a 2-wire circuit. All long distance circuits are 4-wire. Almost all local phone lines and analog phones are 2-wire.

group 4

A high-speed (56 kbps) facsimile protocol specific to ISDN.

hop count

A routing metric used to measure the distance between a source and a destination. Particularly used by RIP.

hub

(1) Communications center, (2) Major routing station for connecting channels, (3) DDS connecting center.

IEEE

Institute of Electrical and Electronic Engineers. Professional organization that defines network standards. IEEE LAN standards are the predominant LAN standards today and include protocols similar or virtually equivalent to Ethernet and Token Ring.

IEEE 802.1d

An algorithm used to prevent bridging loops by creating a spanning tree.

IEEE 802.2

An IEEE LAN protocol that specifies an implementation of the LLC sublayer of the data link layer. It handles errors, framing, flow control, network layer (Layer 3) service interface, and is used in LANs.

IEEE 802.3

A physical layer standard specifying a linear bus network LAN with a CSMA/CD access method on a bus topology. Ethernet follows the 802.3 standard, transmitting at 10 megabits per second. This is the most common local area network specification. Physical variations of IEEE 802.3 include 10Base2 and 10BaseT.

in-band signalling

Signalling made up of tones which pass within the voice frequency band and are carried along the same circuit as the talk path being established by the signals. Virtually all signalling (request for service, dialing, disconnect, etc.) in the U.S. is in-band signalling. Most of that signalling is MF (Multi-Frequency) dialing. The more modern form of signalling is out-of-band.

interexchange carrier

Since divestiture, any carrier registered with the FCC authorized to carry customer transmissions between LATAs interstate, or if approved by a state public utility commission, intrastate. Includes carri-

ers such as AT&T Communications, Satellite Business Systems, GTE Telenet, GTE Sprint, and MCI.

information element

The name for the data fields within an ISDN Layer 3 message.

interworking

Communication between two types of networks or end equipment. This may or may not involve a difference in signalling or protocol elements supported.

Internet Protocol

A TCP/IP protocol describing software that tracks the Internet address of nodes, routes outgoing message, and recognizes incoming messages. Used in gateways to connect networks at OSI network Level 3 and above.

IPX

Internetwork Packet Exchange. A Novell NetWare protocol used to move information across networks.

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.

jabber

An error condition in which a network device continually transmits garbage onto the network. In IEEE 802.3, a data packet whose length exceeds that prescribed in the standard.

jitter

The slight movement of a transmission signal in time or phase that can introduce errors and loss of synchronization for high-speed synchronous communications. See phase jitter.

LATA

Local Access and Transport Area. One of 161 local telephone serving areas in the United States, generally encompassing the largest standard statistical metropolitan areas. Subdivisions established as a result of the AT&T divestiture that now distinguish local from long distance service. Circuits with both end-points within the LATA (intraLATA) are generally the sole responsibility of the local telephone company, while circuits that cross outside the LATA (interLATA) are passed on to an interexchange carrier.

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.

Media Access Control (MAC)

As defined by the IEEE, the lower of the two sublayers of the OSI reference model data link layer. The MAC sublayer is concerned with media access issues, such as whether token passing or contention is used.

message

The Layer 3 information that is passed between the CPE and SPCS for signalling.

multipoint line

A communications line having multiple cable access points.

Name Binding Protocol (NBP)

The AppleTalk transport-level protocol that translates a character string name into the internet address of the corresponding socket client; NBP enables AppleTalk protocols to understand user-defined zones and device names by providing and maintaining translation tables that map these names to corresponding socket addresses.

NAT

Network Address Translation occurs at the borders of stub domains. Its purpose is to translate the IP address of passing packets by changing all references of one IP address to another. Translation is performed as per RFC 1631.

netmask

A 32-bit bit mask which shows how an Internet address is to be divided into network, subnet, and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion (as determined by the address's class), and the subnet field should be contiguous with the network portion.

non-ISDN line

Any connection from a CPE to a SPCS that is not served by D-Channel signalling.

non-ISDN trunk

Any trunk not served by either SS7 or D-Channel signalling.

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.

phase jitter

In telephony, the measurement in degrees out-of-phase that an analog signal deviates from the reference phase of the main data-carrying signal. Often caused by alternating current components in a telecommunications network.

point-to-point protocol (PPP)

An implementation of TCP/IP which is intended for transmission using telephone lines. PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

poison routes

Routes which have an infinite metric which to other routers means the network for the route is inaccessible.

PRA

Primary Rate Access. Connects high-capacity CPE, such as PBXs, to the network. In the US, this is composed of twenty-three 64 kbps channels and one 64 kbps D-channel. Also known as Primary Rate Interface (PRI).

RIP

Routing Information Protocol. A protocol used to exchange routing information among a set of computers connected by a LAN. RIP uses hop counts as a routing metric.

router

An interface which finds the best route 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 one route is better than another. This information is stored in routing tables. Such ta-

bles include reliability, delay bandwidth, load, MTUs, communication costs, and hop count. \\

RS-232-C

An EIA-specified physical interface with associated electrical signal-ling between DCE and DTE. The most commonly employed interface between computer devices and modems.

RTMP

Routing Table Maintenance Protocol. The AppleTalk protocol used to establish and maintain the routing information that is required by internet routers in order to route datagrams from any source socket to any destination socket in the internet. Using RTMP, internet routers dynamically maintain routing tables to reflect changes in internet topology.

service advertising protocol (SAP)

An IPX protocol through which network resources such as servers become known to clients.

serving area

Region surrounding a broadcasting station where signal strength is at or above a stated minimum. The geographic area handled by a telephone central office facility. Generally equivalent to a LATA.

SNMP

Simple Network Management Protocol. SNMP provides a means to monitor and set network configuration and runtime parameters.

spanning tree

A loop-free subset of the topology of a network.

SPCS

Stored Program Controlled Switch. A digital switch that supports call control, routing, and supplementary services provision under software control. All ISDN switches are SPCSs.

spoofing

Spoofing reduces the required bandwidth by having devices, such as bridges or routers, answer for the remote devices. This causes the remote LAN to appear as if it is still connected to the LAN device even though it is not. The spoofing saves the WAN bandwidth, because no packet is ever sent out on the WAN.

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 effect timing.

T1

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.

TA

Terminal Adaptor. A DCE that connects to the ISDN S-Interface and enables non-ISDN terminal equipment to communicate over the ISDN.

TE1

Terminal Equipment Type 1. ISDN-compatible terminals.

Telnet

The TCP/IP standard protocol for remote terminal connection service. Telnet allows a user at one site to interact with a remote timesharing system at another site as if the user's terminal were connected directly to the remote machine.

TCP/IP

Transmission Control Protocol/Internet Protocol. A set of protocols developed by the Department of Defense to link dissimilar computers across many kinds of networks.

twisted pair

Two wires twisted around each other to reduce induction (interference) from one wire to the other. Several sets of twisted pair wires may be enclosed in a single cable. Twisted pair is the normal cabling from a central office to your home or office, or from your PBX to your office phone. Twisted pair wiring comes in various thicknesses. As a general rule, the thicker the cable is, the better the quality of the conversation and the longer cable can be and still get acceptable conversation quality. However, the thicker it is, the more it costs.

2B+D

The Basic Rate Interface (BRI) in ISDN. A single ISDN circuit divided into two 64 kbps digital channels for voice or data and one 16 kbps channel for low speed data (up to 9,600 baud) and signalling. 2B+D is carried on one or two pairs of wires depending on the interface, the same wire pairs that today bring a single voice circuit into your home or office. See ISDN.

23B+D

In ISDN, also known as the Primary Rate Interface. A circuit with a wide range of frequencies that is divided in twenty-three 64 kbps

paths for carrying voice, data, video, or other information simultaneously. It bears a remarkable similarity to today's T1 link, except that T1 carries 24 voice channels. In ISDN, 23B+D gives twenty-three channels and one D channel for out-of-band signalling. However, in T1, signalling is handled in-band. See ISDN.

two-wire circuit

A transmission circuit composed of two wires, signal and ground, used to both send and receive information. In contrast, a 4-wire circuit consists of two pairs. One pair is used to send and one pair is used to receive. All trunk circuits (long distance) are 4-wire. A 4-wire circuit delivers better reception, but also costs more. All local loop circuits (those coming from a Class 5 central office to the subscriber's phone system) are 2-wire, unless a 4-wire circuit is requested.

U-interface

A twisted pair subscriber loop that connects the NT1 reference point to the ISDN network, as defined in the I.411 Recommendation. This interface provides Basic Rate Access with an operating frequency of 160 kbps and an information rate of 144 kbps. Under U.S. regulations, this also marks the line of demarcation between customer-owned equipment and the public network.

ZIP

Zone Information Protocol. The AppleTalk session-layer protocol used to maintain and discover the internet-wide mapping of network number ranges to zone names.

Zombie Routes

Routes that have been identified by the router to be deleted. They remain in the router's route table for a specified amount of time with an infinite metric so that all other routers will learn of this router's intention to delete them.

Index

Numerics	bridging 1-5
10baseT interface D-2	concurrent routing and bridg-
A	ing 1-6
ADTRAN frame port 144 1-2	demand 1-5
agent C-1, C-3	C
applications	call log messages B-6
frame relay connectivity to	channel rate 3-11
ADTRAN frame port144 1-2	CHAP 3-42
single user to corporate LAN	clock mode 3-10
1-2	command line interface E-1
SOHO to corporate LAN 1-3	command prompt mode 3-56
ARP cache 3-60	commands E-3
authentication 3-25, 3-42	communities C-3
PPP peer 3-42	communities/manager IP 3-55
authentication/Rx password 3-	communities/name 3-54
43	communities/privilege 3-54
authentication/Rx username 3-	concurrent routing and bridg-
43	ing 1-6
authentication/Tx method 3-42	configuration 1-9
authentication/Tx password 3-	downloading/uploading E-3
43	configuration menu 3-2, 3-8
authentication/Tx username 3-	configuration/bridge 3-21
43	configuration/frame relay 3-32
auto detect 1-5, 3-11	configuration/IP 3-12
В	configuration/IPX 3-19
baud rate 3-56	configuration/management 3-
BECN timeout 3-41	52
bridge 3-47	configuration/management
bridge map/active 3-38	menu 3-52
bridge map/bridge group 3-39	configuration/PPP profile 3-42
bridge menu 3-21	configuration/security 3-25
bridge mode 1-5	configuration/system info 3-8
bridge table 3-61	configuration/terminal mode
bridge/mode 3-22, 3-47	3-56
bridge/WAN IP bridge 3-22	configuration/WAN 3-10
bridge/WAN IPX bridge 3-23	connection LAN 2-1

. 1	Til C D o
connection list profile	Ethernet interface D-2
deleting 3-34	Ethernet interface (LAN) 4-1
connection log 3-70	Express 6100
connection log/active 3-71	front panel 1-7
connection log/clear 3-71	indicators 1-7
connection log/level 3-71	Express 6100/6120
connection log/view 3-71	configuration 1-9
connection log/wrap 3-71	functions provided by 1-4
connector pinouts D-1	installation 2-1
corporate LAN 1-2, 1-3	overview 1-1
D	rear panel 1-8
data bits 3-56	security 1-10
default 1-5	terminal menu structure 3-1
default gateway 3-13	Express 6120
demand bridging 1-5	front panel 1-8
demand routing 1-5	indicators 1-8
DHCP mode 3-15	F
display 4-1	factory default 1-5
DLCI mapping 3-33	features 4-1
DLCI mapping/active 3-34	FEBE 3-11
DLCI mapping/bridge map 3-38	FEBEs 3-11
DLCI mapping/DLCI 3-35	filter
DLCI mapping/filters 3-39	setting up 3-27
DLCI mapping/IP map 3-35	filter defines 3-27
DLCI mapping/IPX map 3-37	filter defines /IP filter defines 3-
DLCI table 3-59	29
DNS 3-16	filter defines /IPX filter defines 3-
DNS server 3-16	30
DNS/domain name 3-17	filter defines /MAC filter defines
DNS/server 1 3-17	3-28
DNS/server 2 3-17	filter defines /pattern filter de-
domain name 3-17	fines 3-28
download/uploading configura-	filters 3-39, 3-49
tion E-3	filters/in exceptions 3-40, 3-50
E	filters/LAN-to-WAN (out) 3-51
EAP 3-42	filters/out exceptions 3-41, 3-51
echo request 3-68	filters/Out to PVC 3-41
EIA-232 interface D-1	firmware revision 3-9
embedded agent C-3	frame relay 1-5, 3-32
environmental specifications 4-1	frame relay connectivity to ADT-
chynonnenai specifications 4-1	

RAN frame port144 1-2	IP routing 1-5
frame relay/DLCI mapping 3-33	IP stats 3-66
frame relay/DLCI table 3-59	IP/default gateway 3-13
frame relay/maintenance proto-	IP/DNS 3-16
col 3-33	IP/IP address 3-12
frame relay/polling frequency 3-	IP/IP router 3-14
33	IP/mode 3-43
frame relay/port 3-58	IP/NAT 3-15, 3-44
frame type 3-20	IP/proxy ARP 3-18
front panel 1-7, 1-8	IP/RIP 3-14, 3-45
front panel indicators 1-7, 1-8	IP/route 3-44
G	IP/static routes 3-13
GetNextRequest C-2	IP/subnet mask 3-12
I	IP/UDP relay 3-17
IDSL 1-1	IPX filter defines 3-30
network connection 2-1	IPX map/active 3-37
overview 1-1	IPX map/IARP 3-38
setting up the line Quick Start-1	IPX map/link network 3-38
IDSL/channel rate 3-11	IPX menu 3-19
IDSL/FEBEs 3-11	IPX router 1-4
IDSL/NEBES 3-11	IPX routes 3-63
indicators 1-7, 1-8	IPX routing 1-6
installation 2-1	IPX servers 3-64
interface	IPX/frame type 3-20
Ethernet 4-1	IPX/mode 3-19, 3-46
network 4-1	IPX/network 3-19
IP filter defines 3-29	IPX/remote network 3-46
IP map/active 3-35	IPX/RIP timer 3-21
IP map/far-end IP address 3-35	IPX/SAP timer 3-21
IP map/IARP 3-35	IPX/seed status 3-20
IP map/IP netmask 3-36	IPX/triggered 3-47
IP map/link IP address 3-36	IPX/type 20 packets 3-47
IP map/NAT 3-37	ISDN
IP map/RIP direction 3-37	jack 1-8
IP map/RIP method 3-36	ISDN jack Quick Start-1
IP map/RIP protocol 3-36	ISDN/clock mode 3-10
IP menu 3-12	L
IP router 1-4, 3-14	L2 protocol 3-11
IP router/mode 3-14	LAN bridge 1-4
IP routes 3-61	LAN connection 2-1
11 10465 0 01	

LAN stats 3-65 LEDs 1-7, 1-8 line mode Quick Start-1 link IP 3-45 log messages B-1 logs menu 3-2, 3-69 logs/connection log 3-70 logs/network log 3-71 logs/PPP log 3-70 logs/sys log host 3-69 loop status messages A-1 M MAC addresses 1-4 MAC bridging 1-5 MAC filter defines 3-28 maint port/baud rate 3-56 maint port/parity 3-56 maint port/parity 3-56 maint port/password 3-55 maint port/stop bits 3-56 maint port/stop bits 3-56 maint port/stop bits 3-56 maintenance DLCI 3-41 maintenance port 3-55 maintenance protocol 3-33 management 3-52 management/SNMP 3-54 management/Telnet 3-52	NAT/DHCP renewal time 3-16 NAT/web server 3-16 NEBE 3-11 NEBES 3-11 network address translation 1-4, 1-6 network connection IDSL 2-1 network device GetResponse C-2 network interface 4-1 network log 3-71 network log messages B-7 network log/clear 3-72 network log/clear 3-72 network log/view 3-72 network log/view 3-72 network log/wrap 3-72 network manager C-1 GetRequest C-2 none 3-15 O OFF/ON switch 1-8 overview Express 6100/6120 1-1 P packets filtering 3-27 PAP 3-42
55	none 3-15
maint port/stop bits 3-56	
	OFF/ON switch 1-8
-	Express 6100/6120 1-1
	P
menu commands E-1	parity 3-56
navigating 3-4, 3-5	password 3-53, 3-55
structure 3-1	pattern filter defines 3-28 physical specifications 4-1
MIB C-1	ping 3-73
mode 1-5	poison reverse 3-15, 3-45
N	polling frequency 3-33
NAT 1-4, 3-15, 3-16	power requirements 4-1
NAT mode 1-6	PPP 1-5, 3-27, 3-48
NAT/Default IP 3-16	PPP log 3-70
NAT/DHCP mode 3-15	PPP log messages B-1

PPP log/active 3-70	RJ-49C interface D-1
PPP log/clear 3-70	route/force IP 3-44
PPP log/level 3-70	route/IP/net 3-44
PPP log/view 3-70	route/netmask 3-44
PPP log/wrap 3-70	routing
PPP peer 3-16	concurrent routing and bridg-
PPP profile 3-42	ing 1-6
PPP profile/authentication 3-42	demand 1-5
PPP profile/bridge 3-47	IP 1-5
PPP profile/filters 3-49	IPX 1-6
PPP profile/IP 3-43	Rx only 3-15
PPP profile/IPX 3-46	S
PPP profile/PPP 3-48	SAP 1-4, 1-6
PPP/max config 3-48	SAP timer 3-21
PPP/max failure 3-48	security 1-10
PPP/max timer 3-48	security levels 3-1, 3-7
PPP/VJ compression 3-48	security menu 3-25
proxy ARP 3-18	security/authentication 3-25
\mathbf{Q}	security/filter defines 3-27
quick startup guide Quick Start-1	security/PPP 3-27
R	security/radius server 3-26
radius 3-53	seed status 3-20
radius server 3-26	sessions 3-57
radius server/primary server 3-	sessions/frame relay 3-58
26	sessions/PPP session 3-57
radius server/retry count 3-26	sessions/spanning tree 3-60
radius server/secondary server	SetRequest C-2
3-26	signal format 4-1
radius server/secret 3-26	SNMP 3-54, C-1
radius server/UDP port 3-26	SNMP access 3-54
rear panel 1-8, 1-9	SNMP/communities 3-54
RIP 1-4, 1-6, 3-14, 3-45	SNMP/traps 3-55
RIP timer 3-21	SOHO (small office - home office)
RIP/direction 3-15, 3-46	1-3
	spanning tree 3-60
RIP/method 3-15, 3-45 RIP/mode 3-14, 3-45	spanning tree algorithm 1-5
RIP/protocol 3-14, 3-45	specifications 4-1
RIP/triggered 3-46	environmental 4-1
RIP/V2 secret 3-15	physical 4-1
	power 4-1
RJ11 interface D-1	Power 1-1

split horizon 3-15, 3-45 static routes/active 3-13 static routes/hops 3-13 static routes/IP address 3-13 static routes/IP address 3-14 static routes/subnet mask 3-13 static routes/subnet mask 3-13 status menu 3-2, 3-57 status/ARP cache 3-60 status/bridge table 3-61 status/IP routes 3-61 status/IP stats 3-66 status/IPX routes 3-63 status/IPX routes 3-63 status/IPX servers 3-64 status/LAN stats 3-65 status/WAN stats 3-65 status/WAN stats 3-65 stop bits 3-56 subnet mask 3-12 switches OFF/ON 1-8 TO HUB/TO NIC 1-8 system contact 3-9 system info menu 3-8 system location 3-8 system uptime 3-9 T Telnet 1-10, 3-52 Telnet client 3-74 Telnet/server access 3-52 Telnet/user list 3-52 terminal menu commands E-1 navigating 3-4, 3-5	test menu/echo request 3-68 TFTP 3-74 TFTP host 3-74 TO HUB/TO NIC switch 1-8 transfer methods 3-74 trap C-2 traps C-3 traps/manager IP 3-55 traps/manager name 3-55 Tx and Rx 3-15 Tx methods 3-42 Tx only 3-15 type 20 packets 3-47 U UDP port type 3-18 UDP relay list 3-17 UDP relay list/relay address 3-18 UDP relay list/UDP port type 3-18 UDP relay list/UDP port type 3-18 UDP relay list/UDP port type 3-18 UDP relay list/UDP port s 1, 2, 3 3-18 UDP relay/mode 3-17 UDP relay/UDP relay list 3-17 upgrade menu 3-74 upgrade/abort transfer 3-75 upgrade/filename 3-74 upgrade/start transfer 3-75 upgrade/transfer method 3-74 user list 3-52 user list/authen method 3-53 user list/idle time 3-53
commands E-1	user list/authen method 3-53

utilities menu 3-2, 3-73 utilities/exit 3-75 utilities/ping 3-73 utilities/Telnet client 3-74 utilities/upgrade menu 3-74 **V**

VJ compression 3-48

W

WAN IP bridge 3-22 WAN IP bridge proxy ARP 3-23 WAN IP bridge/netmask 3-23 WAN IP bridge/network 3-22 WAN IP bridge/triggered 3-23 WAN IPX bridge 3-23 WAN IPX bridge/frame type 3-24
WAN IPX bridge/network 3-23
WAN IPX bridge/seed status 3-24
WAN IPX bridge/triggered 3-24
WAN menu 3-10
WAN stats 3-65
WAN/ISDN 3-10
WAN/L2 protocol 3-11
web 1-10
web browser 1-10
X
xmodem 3-74

Product Support Information

Presales Inquiries and Applications Support

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

Applications Engineering (800) 615-1176

Sales (800) 827-0807

Post-Sale Support

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

Technical Support (888) 4ADTRAN

Repair and Return

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

CAPS Department (256) 963-8722

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

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

RMA # _____