FrameSaver® DSL

Models 9720, 9783, and 9788

User's Guide

Document No. 9700-A2-GB20-20

December 2002

PARADYNE®

Notice

Warranty, Sales, Service, and Training Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Internet:** Visit the Paradyne World Wide Web site at **www.paradyne.com**. (Be sure to register your warranty at **www.paradyne.com/warranty**.)
- **Telephone:** Call our automated system to receive current information by fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — Outside the U.S.A., call 1-727-530-2340

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to **userdoc@paradyne.com**. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Trademarks

Patent Notification

FrameSaver products are protected by U.S. Patents: 5,550,700 and 5,654,966. Other patents are pending.

Contents

3 Configuration Procedures

4 Configuration Options

5 Configuring the FrameSaver DSL Router

6 Security and Logins

7 Operation and Maintenance

8 Troubleshooting

9 Setting Up OpenLane for FrameSaver Device

About This Guide

Purpose and Intended Audience

This document contains information that applies to FrameSaver DSL (Digital Subscriber Line) 9720, 9783, and 9788 CSU/DSUs (Channel Service Unit/Data Service Units) and FrameSaver DSL routers running firmware release level 2.0.4 and above. Features slated for firmware release 2.1, such as Telnet capability, are described in this manual but may not be immediately available in all models.

It is intended for system designers, engineers, administrators, and operators who are familiar with the operation of digital data communications equipment and frame relay networks.

NOTE:

In this manual, CSU/DSU refers to the line termination capability of the DSL endpoint, and does not imply association with traditional T1 or DDS equipment.

Document Organization

Section	Description
Chapter 1, *About FrameSaver DSL Devices*	Identifies how FrameSaver DSL devices fit into Paradyne's Service Level Management (SLM) solution, and describes the unit's basic, unique, and advanced features.
Chapter 2, *User and Command Line Interfaces, and Basic Operation*	Shows how to navigate the menu-driven user interface and the router's Command Line Interface (CLI).
Chapter 3, *Configuration Procedures*	Shows how to access and save configuration options.
Chapter 4, *Configuration Options*	Describes the configuration options available for the devices.
Chapter 5, *Configuring the FrameSaver DSL Router*	Describes the FrameSaver DSL Router's interfaces and features, with sample router scenarios, and how to configure the router.

Section	Description
Chapter 6, *Security and Logins*	Provides procedures for controlling access to the device and setting up logins.
Chapter 7, *Operation and Maintenance*	Provides procedures to display device identification information and perform file transfers, as well as how to display and interpret status and statistical information.
Chapter 8, *Troubleshooting*	Provides device problem indicators, problem resolution, alarm conditions, troubleshooting, and test procedures.
Chapter 9, *Setting Up OpenLane for FrameSaver Device*	Identifies where installation and setup information is located and how FrameSaver devices are supported.
Chapter 10, *Setting Up Network Health for FrameSaver Device*	Describes setup of Concord's Network Health application to create reports for FrameSaver devices.
Appendix A, *Menu Hierarchy*	Contains a graphical representation of how the menu-driven user interface screens are organized.
Appendix B, *SNMP MIBs, Traps, and RMON Alarm Defaults*	Identifies the MIBs supported, lists the device's compliance with SNMP format standards and special operational trap features, describes the RMON-specific user history groups, and presents alarm and event defaults.
Appendix C, *Router CLI Commands, Codes, and Designations*	Describes the configuration options available on the FrameSaver DSL Router, and the minimum access level for each command.
Appendix D, *Router Command Line Summaries and Shortcuts*	Provides a summary of commands, with abbreviated syntax that can be entered, and the default setting for each command.
Appendix E, *Connectors, Cables, and Pin Assignments*	Shows the unit's rear panels, tells what cables are needed, and provides pin assignments for interfaces and cables.
Appendix F, *Technical Specifications*	Technical Specifications.
Appendix G, *Equipment List*	Equipment List.
Index	Lists key terms, acronyms, concepts, and sections.

A master glossary of terms and acronyms used in Paradyne documents is available on the World Wide Web at **www.paradyne.com**. Select *Library* → *Technical Manuals* → *Technical Glossary*.

Product-Related Documents

Document Number	Document Title
Paradyne FrameSaver Documentation:	
9000-A2-GB20	*Configuring Frame Relay Service Over DSL*
9000-A2-GK43	*FrameSaver SLV Activation Instructions*
9700-A2-GL10	*FrameSaver DSL CSU/DSU, Models 9783 and 9788, Quick Reference*
9700-A2-GL11	*FrameSaver DSL Router, Models 9783 and 9788, Quick Reference*
9720-A2-GN10	*FrameSaver DSL 9720 CSU/DSU Installation Instructions*
9783-A2-GN10	*FrameSaver DSL 9783 CSU/DSU Installation Instructions*
9783-A2-GN11	*FrameSaver DSL 9783 Router Installation Instructions*
9788-A2-GN10	*FrameSaver DSL 9788 CSU/DSU Installation Instructions*
9788-A2-GN11	*FrameSaver DSL 9788 Router Installation Instructions*
Paradyne Hotwire Documentation:	
8000-A2-GB26	*Hotwire MVL, ReachDSL, RADSL, IDSL, and SDSL Cards, Models 8310, 8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*
8335-A2-GB20	*Hotwire ATM Line Cards, Models 8335, 8355, 8365, and 8385, User's Guide*
8820-A2-GN20	*Hotwire 8820 GranDSLAM Installation Guide*
Paradyne OpenLane NMS Documentation:	
7800-A2-GB30	*OpenLane SLM Reports Reference Guide*
7800-A2-GB32	*OpenLane SLM Administrator's Guide*
7800-A2-GZ46	*OpenLane SLM Oracle Database Administration Instructions*
NetScout Documentation:	
2930-170	*NetScout Probe User Guide*
2930-610	*NetScout Manager/Plus User Guide*
2930-620	*NetScout Manager/Plus & NetScout Server Administrator Guide*
2930-788	*NetScout Manager Plus Set Up & Installation Guide*
Concord Communications Documentation:	
09-10010-005	*Network Health User Guide*
09-10020-005	*Network Health Installation Guide*
09-10050-002	*Network Health – Traffic Accountant Reports Guide*
09-10070-001	*Network Health Reports Guide*

Complete Paradyne documentation for this product is available at **www.paradyne.com**. Select *Library* → *Technical Manuals*.

To order a paper copy of this manual:

- Within the U.S.A., call 1-800-PARADYNE (1-800-727-2396)
- Outside the U.S.A., call 1-727-530-8623

Conventions Used

Convention	Interpretation
[ ]	Brackets indicate an optional element.
{ }	Braces indicate a required entry.
|	Vertical bars separate mutually exclusive elements. Enter one element only.
[{ }]	Braces within brackets indicate a required choice within an optional element.
Italics	Entry is a variable, which must be supplied by the operator.
Bold	Entry, or the minimum characters that can be entered, must be typed as shown
x.x.x.x	32-bit IP address and mask information where *x* is an 8-bit weighted decimal notation.
xx:xx:xx:xx:xx:xx	MAC address information, where *x* is a hexadecimal notation.
Main Menu → Status	Menu selection indicates a selection sequence to be made from a menu (e.g., select Status from the Main Menu).
Text highlighted in blue	A hyperlink to additional information when viewing this manual online. Click on the highlighted text.

About FrameSaver DSL Devices

1

This chapter includes the following:

System Overview

The Paradyne system solution consists of:

- FrameSaver® DSL (Digital Subscriber Line) CSU/DSU (Channel Service Unit/Data Service Unit)
- FrameSaver DSL Router
- Hotwire® ATM (Asynchronous Transfer Mode) Line Card in the Hotwire GranDSLAM, or with another vendor's DSLAM (Digital Subscriber Line Access Multiplexer)

  Call Paradyne for compatible DSLAMs (see *Warranty, Sales, Service, and Training Information* in the front of this document for the phone number).
- OpenLane® SLM (Service Level Management) System

This solution controls network costs by providing increased manageability, monitoring, and diagnostics to identify and troubleshoot problems more quickly. FrameSaver DSL devices operate with other FrameSaver devices, and are also compatible with Concord Communication's Network Health software.

FrameSaver DSL Features

Based upon the model ordered, or whether the device has been upgraded to Service Level Verifier (SLV) capability, FrameSaver DSL devices have the Diagnostic Feature Set or Advanced SLM Feature Set, each providing different levels of intelligence for monitoring, managing, and reporting performance of the device.

For features specific to the DSL CSU/DSU or router, see *CSU/DSU-Specific Features* and *Router-Specific Features*.

CSU/DSU-Specific Features

The following features only apply to the DSL CSU/DSU:

- **Two Interfaces.** Provides two interfaces for traffic:
  - Synchronous DTE port for user data
  - Ethernet Interface for management data
- **Upstream Pipelining.** Provides pipelining capability into the Wide Area Network (WAN) for reduced latency, where groups of bytes are transmitted as soon as they are received, rather than waiting for the entire frame to be collected before sending.
- **LMI Protocol Support.** Automatically detects and initializes the Local Management Interface (LMI) protocol type on the user data port.

Router-Specific Features

The following features only apply to the DSL router:

- **Ethernet Interface.** Supports user data and management traffic. An LED is also provided to view the status of the interface.
- **In-Band Router Management.** Permits the router to be managed via customer data PVCs and EDLCIs by assigning an IP address for router management that is different from the IP address generally used for the network interface.
- **Inverse ARP for User Data.** Provides Inverse ARP (Address Resolution Protocol) support for user data, as well as management data. The router responds to Inverse ARP requests, and can acquire the IP address of a FrameSaver device at the far end of a customer PVC. ARP information is retained for both customer data and management data.

- **CLI Access and Configuration.** Provides a router Command Line Interface (CLI), along with the menu-driven user interface, for configuring and managing the router. It is accessed from the Main Menu via a direct COM port connection or Telnet.

  The following features are configurable using the CLI:

  — NAT (Network Address Translation) support provides the means to bind IP addresses in a private network to addresses in a public, or global, network for transparent routing between the two domains on all PVCs. Up to 30 NAT pools are supported.

  — Routing table configuration permits configuration of static routes. Up to 32 entries can be made.

  — IP forwarding to forward multicast IP packets and customer datagrams.

  — Filtering on the Ethernet and frame relay interfaces, configurable from the CLI access list, allows the router to filter MAC frames and prevent unwanted inbound connections. Two filter access lists are supported per interface, one for the transmit and one for the receive direction.

  The following protocol is supported:

  — DHCP (Dynamic Host Configuration Protocol) support for dynamic allocation of IP addresses and automatic cleanup when a subinterface is deleted, as well as allowing multiple IP address ranges for DHCP deny capability. The DHCP server and relay cannot be enabled at the same time. Up to 253 DHCP clients can be supported. One DHCP pool of addresses, and one IP address range per pool is supported.

Diagnostic Feature Set

The following feature set is common to all FrameSaver DSL devices. It provides basic FrameSaver frame relay and diagnostic capability, which includes the following features:

- **Easy Installation.** When AutoBaud is used, no configuration is required. SNMP options may be modified to provide security and enable traps.
- **Frame Relay Aware Management.** Supports diagnostic and network management features over the frame relay network. The device's frame relay capability also supports:
  - — Inband management channels over the frame relay network using dedicated PVCs.
  - — Unique nondisruptive PVC (Permanent Virtual Circuit) diagnostics.
  - — Real-time end-to-end connectivity test and latency snapshots.
  - — Troubleshooting DLCI for service provider remote management.
  - — Basic frame relay statistics.
  - — Committed Information Rate (CIR) monitoring on a PVC basis.
  - — Multiple PVCs on an interface.
  - — Multiplexing management PVCs with user data PVCs.
  - — Multiplexing multiple PVCs going to the same location onto a single network PVC.
- **Router-Independence.** Remote access to diagnostics, performance monitoring, PVC-based in-band network management, and SNMP connectivity are not dependent upon external routers, cables, or LAN adapters.
- **Security.** Provides multiple levels of security to prevent unauthorized access to the unit.
- **Dual Flash Memory.** Allows software upgrades while the unit is running. Two software loads can be stored and implemented at the user's discretion.
- **Auto-Configuration**. Provides the following automatic configuration features:
  - — CIR Determination – Recalculates the committed rate measurement interval (T_c) and excess burst size (B_e) when a DLCI's CIR changes.
  - — Excess Burst Size (B_e) and Committed Burst Size (B_c) are recalculated when Committed Burst Size B_c (Bits) is set to CIR. The committed rate measurement interval (T_c) is recalculated when Committed Burst Size B_c (Bits) is set to Other.
- **Configurable FTP Transfer Rate.** Allows control of the transmit rate used for downloading from the FrameSaver unit and uploading user history statistics to an NMS (Network Management System) via the COM port connection or a management PVC. This allows the data to be transferred as a background task using the standard File Transfer Protocol (FTP) over extended periods of time using low bandwidth.

- **Multiplexed PVCs.** Provides a method of multiplexing management data with customer data transparently over a single PVC (Permanent Virtual Circuit) when FrameSaver devices are at each end of the circuit. This feature also makes it possible to run nondisruptive PVC tests.
- **Maximum Number of PVCs and Management PVCs Supported.** Provides the following number of PVCs. All models provide two dedicated management PVCs.

Model #	Product	PVCs
Diagnostic Feature Set		
9720-A1-211 9783-A1-211 9788-A1-211	FrameSaver DSL 9720 Remote CSU/DSU FrameSaver DSL 9783 Remote CSU/DSU FrameSaver DSL 9788 Remote CSU/DSU	8 8 64
9783-A1-213	FrameSaver DSL 9783 Central Site CSU/DSU	64
9783-A1-214 9788-A1-214	FrameSaver DSL 9783 Router FrameSaver DSL 9788 Router	8
Advanced SLM Feature Set		
9720-A1-221 9783-A1-221 9788-A1-221	FrameSaver DSL 9720 Remote CSU/DSU with SLM FrameSaver DSL 9783 Remote CSU/DSU with SLM FrameSaver DSL 9788 Remote CSU/DSU with SLM	8 8 64
9783-A1-223	FrameSaver DSL 9783 Central Site CSU/DSU with SLM	64
9783-A1-224 9788-A1-224	FrameSaver DSL 9783 Router with SLM FrameSaver DSL 9788 Router with SLM	8

- **ATM VPI/VCI and DLCI Correlation.** For networks with both ATM and frame relay-access endpoints, allows the FrameSaver unit to report the originating Virtual Path and Channel Identifier (VPI/VCI) in the far-end ATM-access endpoint where the local DLCI is mapped.
- **Frame Relay Traffic Policing.** Ensures proper alignment and correlation of CIR values between the FrameSaver unit and the frame relay interworking function on the network switch. Using the same method as the switch, frames that exceed CIR are tagged as Discard Eligible, and frames that exceed excess burst size are discarded.
- **RMON User History Performance Statistics via SNMP Polling.** Provides access to physical interface and basic frame relay performance statistics via SNMP (Simple Network Management Protocol) polling. These statistics are available real-time via the Enterprise MIB (Management Information Base) and historically as an RMON2 (Remote Monitoring, Version 2) User History object.
- **Extensive Testing Capability.** Provides a variety of tests to identify and diagnose device and network problems, including nondisruptive PVC loopbacks and end-to-end connectivity.

  Tests can be commanded from the device's menu-driven user interface or the OpenLane system.These tests include ATM segment and end-to-end loopbacks.

- **Trap Event Log.** Shows the SNMP (Simple Network Management Protocol) trap event log for the FrameSaver unit, with the most recent events first, keeping a running total for all trap events stored, the amount of time since the event was logged, plus a description of the trap.
- **LMI Packet Capture.** Provides a way of uploading LMI data that has been captured on the user data port in a trace file so the data can be uploaded and transferred to a Network Associates Sniffer for analysis, or viewed via the menu-driven user interface. When viewed from the menu-driven user interface, the 12 most recent LMI messages are displayed.
- **Enhanced Ping Operation.** FrameSaver devices can check connectivity and roundtrip response time to any remote device in either direction, via the FrameSaver internal management network or the data path.
- **Payload Management.** Any standard, non-management DLCI can be designated as payload managed, providing management directly from a user data PVC, and support for Telnet, ping, SNMP, and FTP.
- **Endpoint identification.** FrameSaver units can identify all destination units via a specified Circuit (DLCI or VPI/ VCI). Third party destinations (non-FrameSaver units) may be manually configured as endpoints.
- **Class of Service.** Up to 7 Class of Service (COS) types are supported.

Advanced SLM Feature Set

The following additional features are provided with the Advanced SLM Feature set:

- **TruePut™ Technology.** Using FDR/DDR (Frame Delivery Ratio/Data Delivery Ratio), throughput (within and above CIR, between CIR and EIR, and above EIR) can be precisely measured, eliminating averaging inaccuracies.
- **Intelligent Service Level Verification (SLV).** Provides accurate throughput, latency, and availability measurements to determine network performance and whether SLAs (Service Level Agreements) are being met, along with SLA reporting.
- **RMON Alarms and Configurable Alarm Thresholds.** Using the OpenLane system, provides the ability to change the SLA parameters and the RMON alarm thresholds to correct problems in real-time before the SLA is violated.
- **RMON-Based User History Statistics Gathering.** Provides everything needed to monitor network service levels, plus throughput with accurate data delivery, network latency, and LMI and PVC availability. Continuous roundtrip latency testing and reporting, as well as CIR relationship to transmitted and received data performance statistics, are included. In addition, port bursting statistics are kept for all frame relay links for accurate calculation of utilization.
- **FTP User History Poller.** The OpenLane system provides a user history bulk collector that generates a database for graphical and historical reporting.

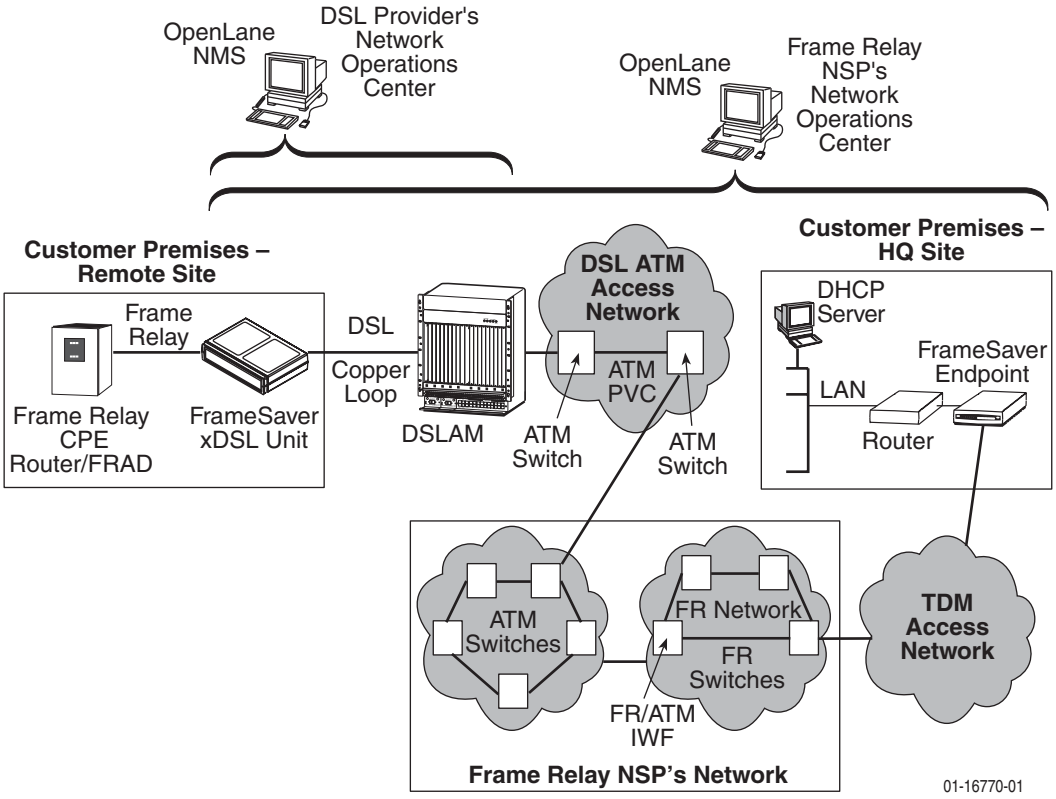
- **Network User History Synchronization.** Allows correlation of RMON2 User History statistics among all SLV devices in a network. Using a central clock, called the network reference time, all SLV device user history statistics are synchronized across the network, further enhancing the accuracy of OpenLane SLV reports.

If upgrading to this feature set, the OpenLane SLM system is required to activate the Advanced SLM Feature Set. FRF.13 compliance is possible with service level performance reporting.

Refer to the *FrameSaver SLV Activation Instructions* for upgrade information and activation procedures. See *Product-Related Documents* in *About This Guide* for the document number.

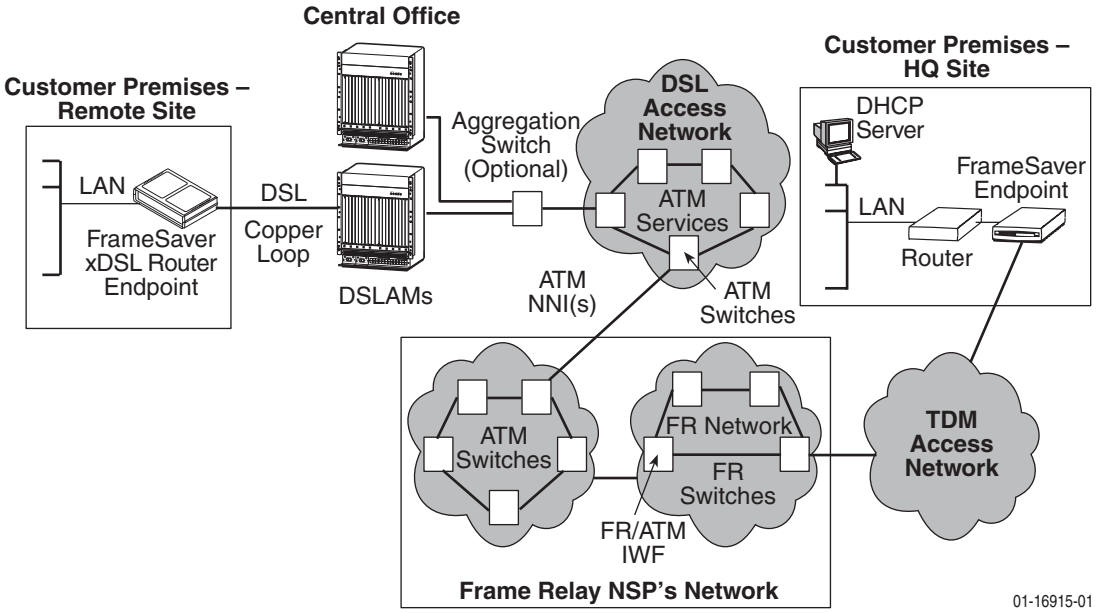
Network Configuration Examples

FrameSaver DSL devices can function in a variety of network configurations. The following illustration shows a typical frame relay network configuration that includes a FrameSaver DSL CSU/DSU.



.

The illustration below shows a typical network configuration that includes a FrameSaver DSL Router.



ATM – Asynchronous Transfer Mode
DHCP – Dynamic Host Configuration Protocol
DSL – Digital Subscriber Line
FR – Frame Relay
HQ – Headquarters
IWF – Interworking Function
LAN – Local Area Network
NSP – Network Service Provider
TDM – Time Division Multiplexer

OpenLane SLM System

Paradyne's OpenLane® Service Level Management (SLM) solution is an open, standards-based, highly distributable system offering robust scalability and flexibility. A Web browser-enabled user interface provides accessibility anytime, anywhere.

Paradyne's network management solution features support for diagnostics, real-time performance monitoring, historical reporting, and detailed health and status indicators for Paradyne's SNMP-managed network access device families.

OpenLane Features

Some of the OpenLane system's features include:

- Easy-to-use Web browser-based user interface
- Optional integration with HP OpenView
- Device configuration through the Web interface
- Real-time device health and status, diagnostics, and performance monitoring
- Extensive Web-based diagnostics, including non-disruptive PVC loopback and end-to-end connectivity testing
- Real-time performance graphs and historical SLV graphs
- Service level management historical reports, including:
  - Frame Delivery Ratio Detail
  - Frame Transfer Delay Detail
  - Availability Detail
  - Network Capacity and Throughput Detail
  - PVC Tx Activity (by % CIR) Detail
  - Protocol Distribution Detail
  - Top 6 IP Communicator Distribution
  - PVC Congestion Detail
  - DTE Port Errors
  - Network Port Errors
  - Port Trend Analysis
  - PVC Trend Analysis
  - SLV Detail
- Diagnostic troubleshooting tests, including end-to-end, connectivity, and nondisruptive PVC, ATM, and frame relay loopbacks
- Automatic SLV device and PVC discovery
- Ability to reset FrameSaver DSL devices from the OpenLane system
- Firmware download to a single device or an entire network
- On-demand polling of FrameSaver devices

User and Command Line Interfaces, and Basic Operation

2

This chapter explains how to access, use, and navigate the menu-driven user interface and the router's Command Line Interface (CLI).

It includes the following:

What appears on interface screens depends on:

- **Current configuration** – How your network is currently configured.
- **Security access level** – The security level set by the system administrator for each user.
- **Data selection criteria** – What you entered in previous screens.

Logging On

Start a session using one of the following methods:

- Telnet session via:
  - An in-band management channel through the frame relay network (frame relay network service provider).
  - An in-band management channel through the ATM network (DSL provider).
  - A local in-band management channel configured on the DTE port between the FrameSaver DSL CSU/DSU and a router (V.35 units only).
  - An Ethernet LAN port.
- Dial-in connection using an external modem.
- Direct terminal connection over the COM port.

If no security was set up or security was disabled, the Main Menu screen appears (see the example in *Main Menu* on page 2-4). You can begin your session.

If security was set up and is enabled, you are prompted for a login. Enter your login ID and password.

If your login was . . .	Then the . . .
Valid	Main Menu appears. Begin your session. **NOTE:** If your login is valid, but access is denied, there are two currently active sessions.
Invalid	Message, **`Invalid Password`**, appears on line 24, and the Login screen is redisplayed. After three unsuccessful attempts: ■ A Telnet session is closed. ■ The User Interface Idle screen appears for a directly connected terminal or modem. ■ An external modem is disconnected. ■ An SNMP trap is generated. Access is denied. See your system administrator to verify your login (Login ID/Password combination).

When the user interface has been idle, the device times out and the session is automatically ended; the screen goes blank. Press Enter to reactivate the interface.

▶ Procedure

To log in when security is being enforced:

1. Type your assigned Login ID and press Enter.
2. Type your Password and press Enter.
   - — Valid characters – All printable ASCII characters
   - — Number of characters – Up to 10 characters can be entered in the Login ID and Password fields
   - — Case-sensitive – Yes

   An asterisk (*) appears in the password field for each character entered.

FrameSaver devices support two sessions simultaneously. If two sessions are currently active, wait and try again.

- If two sessions are currently active and you are attempting to access the unit through Telnet, the local Telnet server process returns a **`Connection refused:`** message at the bottom of the screen.
- If two sessions are currently active and you are attempting to access the unit over the COM port (using a terminal or external modem, not via Telnet), the User Interface Already In Use screen is displayed. In addition, the type of connection (Telnet Connection or Direct COM Port Connection) for each current user is identified, along with the user's login ID.

Ending a Session

When the user interface has been idle, the unit times out and the session is automatically ended; the screen goes blank. Press Enter to reactivate the interface. See Chapter 6, *Security and Logins*, to set up and administer logins.

▶ Procedure

To end the session:

1. Press Ctrl-a to switch to the function keys area of the screen.
2. Type **e** (Exit) and press Enter.
   - — For a terminal-connected to the COM port, the session is ended.
   - — For a modem connected to the COM port, the session is ended and the modem is disconnected.
   - — For a Telnet connection, the session is closed and, if no other Telnet or FTP session is occurring over the connection, the modem is disconnected.

If ending a session from a Configuration menu, see *Saving Configuration Options* in Chapter 3, *Configuration Procedures*.

Main Menu

Entry to all FrameSaver device tasks begins at the Main Menu, which provides access to several menus. The **Access Level** appears at the top of the screen when security has been set up.

```
main                          Access Level: 1                    9783-RtrSLV
Device Name: Node A                                          2/26/2001 02:01

                                  MAIN MENU

                                Status
                                Test
                                Configuration
                                Control
                                Easy Install

--------------------------------------------------------------------------------
Ctrl-a to access these functions, Shift-r to access the Router's CLI      Exit
```

Shift-r to access the Router's CLI appears only for the FrameSaver DSL Router. See *Navigating the Router's CLI* on page 2-9 for additional information.

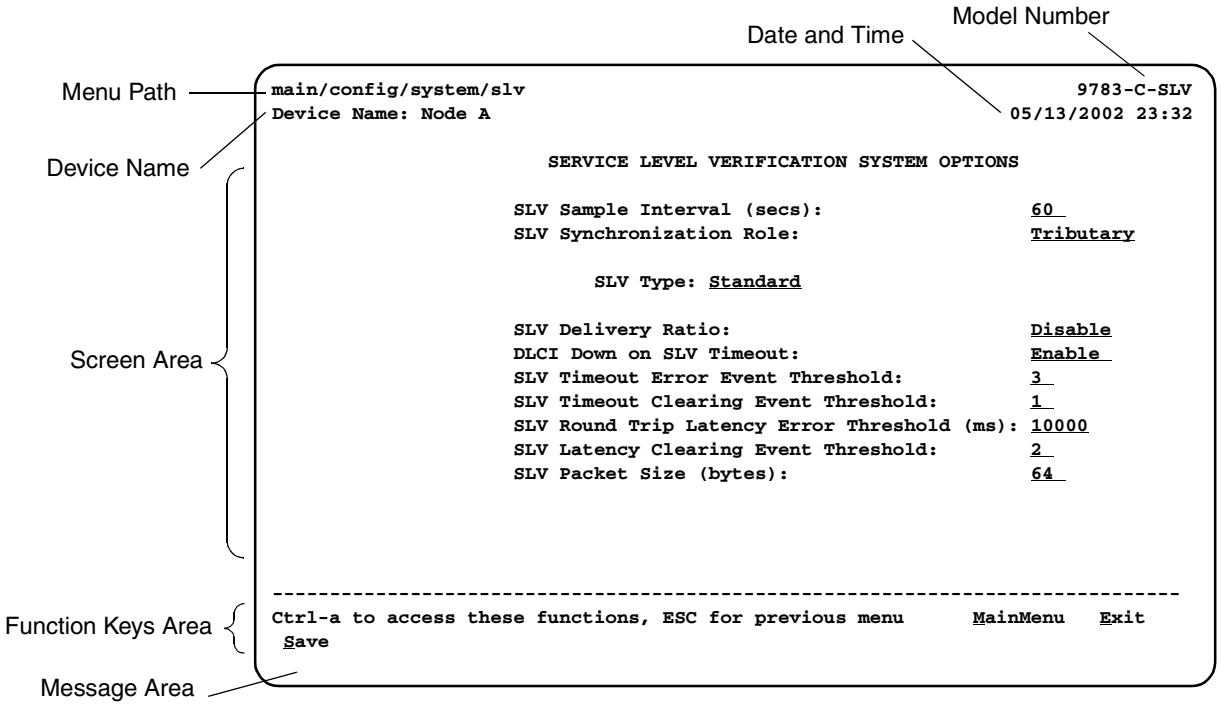
Select . . .	To . . .
Status	View diagnostic tests, interfaces, PVC connections, statistics, LEDs, and FrameSaver unit identity information (except the router's CLI).
Test	Select, start, and stop tests for the FrameSaver unit's interfaces (except the router's CLI).
Configuration	Display and edit the configuration option settings (except the router's CLI).
Control	Control the menu-driven user interface device naming, login administration (except the router's CLI), clock setting, and software releases selection. You can also initiate a power-on reset of the FrameSaver unit.
Easy Install	Perform a quick installation.

See Appendix A, *Menu Hierarchy*, for a pictorial view of FrameSaver device menu structures.

Screen Work Areas

There are two user work areas:

- **Screen area** – Where you input information or information is displayed.
- **Function keys area** – Where you perform specific screen functions.



Screen Format	Description
Menu Path	Menu selections made to reach the current screen.
Device Name	Customer-assigned name for the FrameSaver device.
Model Number: Feature Set 1	■ **9783-C** – Central site CSU/DSU that supports 64 PVCs. ■ **9720, 9783, 9788** – Remote site CSU/DSU that supports 8 PVCs. ■ **9783-Rtr, 9788-Rtr** – Router that supports 8 PVCs.
Model Number: Advanced SLM Feature Set	■ **9783-C-SLV** – Central site CSU/DSU that supports 64 PVCs and has the Advanced SLM Feature Set installed. ■ **9720-SLV, 9783-SLV, 9788-SLV** – Remote site CSU/DSU that supports 8 PVCs and has the Advanced SLM Feature Set installed. ■ **9783-RtrSLV, 9788-RtrSLV** – Router that supports 8 PVCs and has the Advanced SLM Feature Set installed.
Screen Area	Fields for configuring and monitoring the FrameSaver device.
Function Keys Area	Specific functions that can be performed by pressing a specified key, then pressing Enter.
Message Area	■ System-related information and valid settings for input fields in the lower left corner. ■ System and Test Status messages in the lower right corner.

Navigating Menu-Driven User Interface Screens

You can navigate the menu-driven user interface screens by using:

- Keyboard keys.
- Function keys to switch between the two screen work areas.

For CLI navigation, see *Navigating the Router's CLI* on page 2-9.

Keyboard Keys

Use the following keyboard keys to navigate within the screen area.

Press . . .	To . . .
Esc	Return to the previous screen.
Backspace	Move cursor one position to the left or to the last character of the previous field.
Spacebar	Select the next valid value for the field.
Delete (Del)	Delete character that the cursor is on.
Ctrl-a	Move cursor between the screen area and the screen function keys area.
Shift-r	Access the router's Command Line Interface (CLI).
Ctrl-l	Redraw the screen display, clearing information typed in but not yet entered.
Up Arrow or Ctrl-u	Move cursor up one field within a column on the same screen.
Down Arrow or Ctrl-d	Move cursor down one field within a column on the same screen.
Right Arrow or Ctrl-f	Move cursor one character to the right if in edit mode.
Right Arrow (on same screen row), or Tab (on any screen row)	Move cursor to the next field.
Left Arrow or Ctrl-b	Move cursor one character to the left if in edit mode.
Left Arrow (on same screen row), or Ctrl-k	Move cursor to the previous field.
Enter (Return)	■ Accept default or displayed entry, or after entering data. ■ Display valid options on the last row of the screen.

Function Keys

All function keys located in the lower part of the screen (see the example in *Screen Work Areas* on page 2-5) operate the same way throughout the screens. They are not case-sensitive, so upper- or lowercase letters can be used interchangeably.

Select . . .	For the screen function . . .	And press Enter to . . .
M or m	MainMenu	Return to the Main Menu screen.
E or e	Exit	Terminate the menu-driven user interface session.
N or n	New	Enter new data.
O or o	Modify	Change existing data.
L or l	Delete	Delete data.
S or s	Save	Save information.
R or r	Refresh	Update screen with current information.
C or c	ClrStats	Clear network performance statistics and refresh the screen. Select the following functions: ■ ClrSLV&DLCIStats for clearing SLV and DLCI statistics. ■ ClrLinkStats for clearing frame relay link statistics. ■ ClrStats for clearing Ethernet interface statistics.
U or u	PgUp	Display the previous page.
D or d	PgDn	Display the next page.

Selecting from a Menu

▶ Procedure

To select from a menu:

1. Tab or press the down (↓) arrow key to position the cursor on a menu selection, or press the up (↑) arrow key to move the cursor to the bottom of the menu list.

   Each menu selection is highlighted as you press the key to move the cursor from position to position.

2. Press Enter. The selected menu or screen appears.

To return to a previous screen, press the Esc (Escape) key until you reach the desired screen.

Switching Between Screen Areas

Use Ctrl-a to switch between screen areas (see the example in *Screen Work Areas* on page 2-5).

▶ Procedure

To switch to the function keys area from the screen area:

1. Press Ctrl-a.
2. Select either the function's underlined character or Tab to the desired function key.
3. Press Enter. The function is performed as shown in *Function Keys* on page 2-7.

To return to the screen area, press Ctrl-a again.

Selecting a Field for Input

Press the Tab or right arrow key to move the cursor from one field to another. The current setting or value appears to the right of the field.

You can enter information in up to four ways. Select the field, then:

- If a field is blank and the Message area displays valid selections, press the spacebar; the first valid setting for the field appears. Continue pressing the spacebar to scroll through other possible settings.
- Manually type in the field value or command. For example, the Device Name field on the System Information screen is initially blank. Type a name into the input area next to Device Name:

  Device Name: **MyDeviceName**

- Manually type in the first letter(s) of a field value or command, using the unit's character-matching feature. Type as many characters as are required to have the software distinguish one option from another. For example, when configuring the Network ATM option FRF.8 Encapsulation Mode, the default option Transparent is at first displayed; typing **transl** causes the option Translational to be displayed.
- Switch to the function keys area and select or enter a designated function key. For example, Save is one of the available commands in the function keys area of configuration screens. To save a configuration option change, press Ctrl-A and **s** (or **S**). The **s** key is the designated function key for Save.

Navigating the Router's CLI

Access the FrameSaver DSL Router's Command Line Interface by pressing the Shift-r function key from the Main Menu. There is no need to press Ctrl-a first to access the function keys area of the screen.

Once the CLI is accessed, you can use keyboard keys to navigate within the interface. Using the router's CLI, you can display and edit router configuration settings, view router status, and access router tests.

For details of all CLI commands and the conventions used when entering commands, see Appendix C, *Router CLI Commands, Codes, and Designations*. For a summary of abbreviated (minimal) command entries and their default settings, see Appendix D, *Router Command Line Summaries and Shortcuts*.

CLI Keyboard Keys

Use the following keyboard keys to navigate within the router's CLI. Most terminal emulation programs use these same keys.

Press . . .	**To . . .**
Enter (Return)	Accept the current command line input.
Ctrl-c	■ Clear the current command line entry. ■ Abort a command line prompt without answering. ■ Exit a command in progress.
Ctrl-z	Exit Configuration mode and returns to Standard mode. A prompt appears to save any unsaved changes.
Backspace	Erase the character to the left of the cursor.
Delete	Erase the character the cursor is on.
Down Arrow	Recall command line history buffer with the most recent command displaying first. Buffer contains ten lines of history.
Up Arrow	Scroll to the last valid command for editing.
Right Arrow	Move the cursor one position to the right.
Left Arrow	Move the cursor one position to the left.
q (or any key but Spacebar or Enter/Return)	Abort a Move display and return to the command line prompt.

Configuration Procedures

3

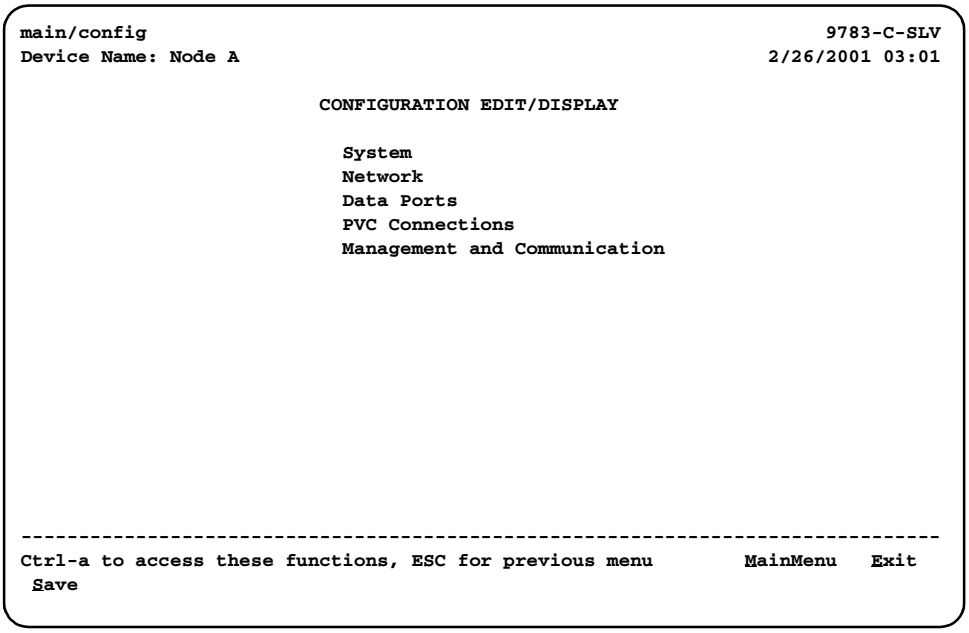
While it is easiest to configure FrameSaver devices using the OpenLane SLM system, you can configure the FrameSaver DSL CSU/DSUs and routers using the menu-driven user interface.

This chapter includes the following:

Basic Configuration From the User Interface

Configuration option settings determine how the FrameSaver DSL device operates. Use the unit's Configuration Edit/Display menu to display or change configuration option settings.

Configuration Edit/Display Menu



Configuration Option Areas

The FrameSaver device arrives with configured factory default settings, which are located in the Factory Default Configuration option area. You can find the default settings for configuration options in the:

- *Configuration Option Tables* in Chapter 4, *Configuration Options*
- *FrameSaver DSL CSU/DSU, Models 9783 and 9788, Quick Reference*, or *FrameSaver DSL Router, Models 9783 and 9788, Quick Reference*

If the factory default settings do not support your network's configuration, you can customize the configuration options to better suit your application.

Four configuration option storage areas are available.

Configuration Option Area	Description
Current Configuration	The currently active set of configuration options.
Customer Configuration 1	An alternate set of configuration options that the customer can set up and store for future use.
Scratchpad Configuration	An alternate configuration area for temporary use. The Scratchpad configuration is reset to the factory default settings when the unit is powered off and on.
Default Factory Configuration	A read-only configuration area containing the factory default set of configuration options. You can load and edit default factory configuration settings, but you can save changes only to the Current, Customer, or Scratchpad configuration option areas. The Current, Customer, and Scratchpad configuration option areas are initially identical with the Default Factory Configuration.

Accessing and Displaying Configuration Options

To access and display configuration options, load a configuration option set into the edit area.

▶ Procedure

To load a set of configuration options for editing:

1. From the Main Menu, press the down arrow key until the cursor is on Configuration.
2. Press Enter to display the Configuration menu. The **Load Configuration From:** menu appears.

   NOTE:

   Loading a configuration with many DLCIs from a unit's Customer or Scratchpad configuration option area may take time. Allow a minute or more for the file to be loaded.

3. Select the configuration option area from which you want to load configuration options (Current Configuration, Customer Configuration, Scratchpad Configuration, or Default Factory Configuration) and press Enter.

   The selected set of configuration options is loaded into the configuration edit area and the **Configuration Edit/Display** menu appears.

This sequence of steps is shown in this guide as the menu selection sequence:

Main Menu→ Configuration

Changing Configuration Options

When security has been set up, only Security Access Level 1 users can change configuration options. See Chapter 6, *Security and Logins,* for additional information.

▶ Procedure

To change configuration option settings:

1. From the Configuration Edit/Display menu, select a set of configuration options and press Enter.

   For example:
   Configuration→PVC Connections

2. Make appropriate changes to the configuration option setting(s). For additional information regarding the user interface, see Chapter 2, *User and Command Line Interfaces, and Basic Operation.*

   When creating new PVC connections or management PVCs, some configuration options will be blank. For a valid setting to appear, Tab to the configuration option and press the spacebar.

3. Repeat Steps 1 and 2 until all changes are complete.

4. Save your changes.

Saving Configuration Options

When changing configuration option settings, you must Save the changes before they will take effect.

▶ Procedure

To save configuration option changes:

1. Press Ctrl-a to switch to the function key area at the bottom of the screen.

2. Type **s** or **S** to select the Save function and press Enter.

   The **Save Configuration To:** screen appears.

   NOTE:

   If you try to exit the Configuration menu without saving changes, a Save Configuration screen appears requiring a Yes or No response.

   — If you select No, the Main Menu screen reappears and the changes are not saved.

   — If you select Yes, the **Save Configuration To:** screen appears.

3. Select the configuration option area to which you want to save your changes (normally the Current Configuration) and press Enter.

   When the Save is complete, **`Command Complete`** appears in the message area at the bottom of the screen.

For the router, saving also updates the router's configuration database, adding newly configured DLCIs or subnets that do not yet exist in the router database.

NOTE:

There are other methods of changing configurations, like SNMP and Auto-Configuration. Since multiple sessions can be active at the same time, the last change made overwrites any previous or current changes being made. For instance:

— Saving your configuration changes would cause configuration changes made via another method to be lost.

— If you are making changes and someone else makes changes and saves them, your changes would be lost.

Configuration Options

4

This chapter describes all the configuration options available on the FrameSaver DSL devices. They can be modifed using the user interface or OpenLane SLM:

- *Configuring Telnet and/or FTP Sessions*
- *Configuring SNMP NMS Security*
- *Configuring SNMP Traps*
- *Configuring Ethernet Management*
- *Configuring the Communication Port*
- *Configuring the COM Port to Support an External Modem*

Default settings for some parameters may be different than shown here for models with customer-specific factory settings.

See Chapter 5, *Configuring the FrameSaver DSL Router*, for additional configuration information when setting up the router.

Using the Easy Install Feature

An Easy Install screen is provided for custom configurations, but is not required for normal installation.

The FrameSaver Easy Install feature provides minimal configuration. Once the installation and configuration are complete, the NOC can complete unit configuration and verify the setup.

Main Menu→ Easy Install

Easy Install Screen

```
main/easy_install                                                    978x-xxxxx
Device Name: Node A                                                09/06/2002 04:02

                                EASY INSTALL

     (9783:) DSLAM Type:                          Paradyne

             Node IP Address:                     000.000.000.000   Clear
             Node Subnet Mask:                    000.000.000.000   Clear
             TS Access: VPI,VCI                          0 ,  35

             Create a Dedicated Network Management Link
             Ethernet Management Options Screen

     (9720:) Network 1 Operating Rate (Kbps)      AutoRate
 (9783/9788:) Network 1 DSL Line Rate (Kbps)      AutoRate
 (9788 DSU:) Port-1 Port Type:                    V.35
 (9783/9788:) Network 1 FRF.8 Encapsulation Mode  Transparent



--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu        MainMenu   Exit
 Save
```

To access the device:

- **For non-managed networks:** Use the TS Access DLCI to ping the unit five times within five seconds.
- **For managed networks:** Use the Dedicated Network Management Link that is created.

Table 4-1, Easy Install Configuration Options, describes the entries on the Easy Install screen.

Table 4-1. Easy Install Configuration Options (1 of 4)

DSLAM Type (9783)
Possible Settings: **Paradyne, Alcatel (NewBridge), PairGain, Nokia** Default Setting: **Paradyne**
Ensures interoperability with non-Paradyne DSLAMs, not just the Hotwire GranDSLAM. This option is only available from the Easy Install screen. NOTES: – The default is set before the unit is shipped, based upon the CLEC customer ordering the unit. If you change the default, you must Save the change for it to take effect, which will reset the unit. – When the default is changed, the default settings for other configuration options change. See *Network 1 DSL Line Rate (9783)* on page 4-6, *DSL Line Rate (Kbps)* on page 4-21, and *Cell Payload Scrambling* on page 4-27 for more information. **Paradyne** – The FrameSaver device is used with a Hotwire GranDSLAM. **Alcatel (NewBridge)** – The FrameSaver device is used with Alcatel's NewBridge DSLAM. **PairGain** – The FrameSaver device is used with PairGain's DSLAM. **Nokia** – The FrameSaver device is used with Nokia's DSLAM.
Node IP Address
Possible Settings: **001.000.000.000–126.255.255.255, 128.000.000.000–223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the node. Since an IP address is not bound to a particular port, it can be used for remote access via a management PVC. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the node, which can be viewed or edited. The first octet of the address cannot be decimal 0 or 127, or greater than 223. **Clear** – Fills the node IP address with zeros.
Node Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the IP address subnet mask that is needed to access the node. Since the subnet mask is not bound to a particular port, it can be used with the Node IP address for remote access via a management PVC. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the node, which can be viewed or edited. **Clear** – Fills the node subnet mask with zeros. When the node's subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the IP address class (Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000).

Table 4-1. Easy Install Configuration Options (2 of 4)

TS Access
Possible Settings: **None, DLCI, VPI,VCI, DLCI_on_VPI,VCI** Default Setting: [Depends on model]
Specifies the type of Virtual Circuit (VC) by which special troubleshooting (TS) access is provided to service providers. **None** – No special troubleshooting link is defined. **DLCI** – Allows the user to select a frame relay DLCI to be designated for special troubleshooting access. **VPI,VCI** – Specifies an ATM VC on a specific ATM VPI,VCI for TS access. It specifies the VPI and VCI on the network interface for service provider troubleshooting. ATM data is presumed to be encapsulated according to RFC 1483 (see *Network 1 FRF.8 Encapsulation Mode (9783 and 9788)* on page 4-7). VPI 0,VCI 35 is the default management path between the FrameSaver device and the DSLAM. The VPI and VCI are entered separately. – VPI range is 0–15. – VCI range is 32–255. **DLCI_on_VPI,VCI** – Specifies a frame relay DLCI VC on a specific ATM VPI,VCI for TS access. DLCI range is 16–1007. ATM data is presumed to be encapsulated according to RFC 1490 (see *Network 1 FRF.8 Encapsulation Mode (9783 and 9788)* on page 4-7).
Create a Dedicated Network Management Link
Possible Settings: **16 – 1007** Default Setting: Initially blank
Enter a DLCI number and VPI,VCI for a dedicated network management PVC. NOTE: With the cursor on the Create a Dedicated Network Management Link field, press Enter. The **`Which DLCI would you like to Create a Dedicated Frame Relay Management PVC on?`** prompt appears. If the DLCI entered is over an ATM link, or Port-1 for the CSU/DSU. Prompts for VPI and VCI also appear. **16 – 1007** – Specifies the DLCI number be used.
Ethernet Management Options Screen
Provides a link to the Ethernet Management Options Screen. Press Enter and the screen appears (see *Configuring Ethernet Management* on page 4-57.) After configuring Ethernet options, press the Esc key to return to the Easy Install screen.
Network 1 DSL Line Rate Mode
Possible Settings: **Hunt** (9783)**, AutoRate, Fixed** Default Setting: **AutoRate**
Specifies the mode to be used for rate selection. **Hunt** – (9783 only.) The unit attempts to train at rate specified by Network 1 DSL Line Rate. If that fails, the unit attempts to train at the next higher rate, and, if unsuccessful, cycles through all the rates until training is successful or the unit is reset. **AutoRate** – The unit automatically detects the line rate from the network interface. **Fixed** – The unit uses the line rate specified by Network 1 DSL Line Rate.

Table 4-1. Easy Install Configuration Options (3 of 4)

Network 1 DSL Line Rate (9783)
Possible Settings: – *If DSLAM Type is set to Paradyne, or if DSLAM Type is set to Nokia and Network 1 DSL Line Rate Mode is set to Fixed:* **144, 192, 208, 256, 272, 384, 400, 512, 528, 768, 784, 1024, 1152, 1168, 1536, 1552, 2320** – *If DSLAM Type is set to Alcatel (NewBridge):* **208, 400, 784, 1168, 1552, 2320** – *If DSLAM Type is set to Nokia and Network 1 DSL Line Rate Mode is set to Hunt:* **192, 384, 768, 1152, 1536** – *If DSLAM Type is set to PairGain:* **144, 192, 208, 256, 272, 384, 400, 512, 528, 768, 784, 1024, 1152, 1168, 1536, 1552, 2320** Default Setting: – *If DSLAM Type is set to Alcatel (NewBridge) and Network 1 DSL Line Rate Mode is set to Hunt:* **208** – *If DSLAM Type is set to Nokia and Network 1 DSL Line Rate Mode is set to Hunt:* **384** – *If DSLAM Type is set to PairGain and Network 1 DSL Line Rate Mode set to Fixed:* **784** – *(If DSLAM Type is set to Paradyne, Network 1 DSL Line Rate Mode is set to AutoRate and Network 1 DSL Line Rate does not appear)*
Determines whether the rate on the DSL interface is set to a specific value or automatically detected using the Conexant AutoBaud algorithm. **144 – 2320** – Sets the DSL line rate in kbps.
Network 1 DSL Line Rate (9788)
Possible Settings: – *If PSD Mask is Symmetric:* **200, 264, 328, 392, 456, 520, 584, 648, 712, 776, 784, 840, 904, 968, 1032, 1096, 1160, 1224, 1288, 1352, 1416, 1480, 1544, 1552, 1608, 1672, 1736, 1800, 1864, 1928, 1992, 2056, 2120, 2184, 2248, 2312** – *If PSD Mask is Asymmetric and Region Setting is Annex A:* **776, 784, 1544, 1552** – *If PSD Mask is Asymmetric and Region Setting is Annex B:* **2056, 2312** Default Setting: [None]
Determines the rate on the DSL network interface. Valid rates, and the rates presented on the screen, depend on the values of Region Setting and PSD Mask on the Network Physical Interface Options screen. If a change to another configuration option renders the selected DSL Line Rate invalid, the line rate is set to AutoRate. *Display Conditions* – Network 1 DSL Line Rate does not appear if Network 1 DSL Line Rate Mode is set to AutoRate. **200 – 2312** – The DSL line rate is set to the specified rate in kbps.
Network 1 Operating Rate (9720)
Possible Settings: **AutoRate, 64, 128, 144** Default Setting: **AutoRate**
Determines the rate on the IDSL network interface. **AutoRate** – The unit automatically detects the line rate from the network interface. **64, 128, 144** – The IDSL line rate is set to the specified rate in kbps.

Table 4-1. Easy Install Configuration Options (4 of 4)

Network 1 Channel (9720)
Possible Settings: **B1, B2** Default Setting: **B1**
Specifies the B channel used for data transfer when the line rate is 64 kbps. *Display Conditions* – Network 1 Channel appears only when Network 1 Operating Rate is set to 64. **B1** – The B1 channel is used for data transfer. **B2** – The B2 channel is used for data transfer.
Port-1 Port Type (9788 CSU/DSU)
Possible Settings: **E530, V.35, X.21** Default Setting: **V.35**
Specifies the port type of the data port. **E530** – The port is configured as an EIA-530-A-compatible DCE. An EIA-530-A-compatible DTE may be directly connected to the DB25 connector for the port. **V.35** – The port is configured as a V.35-compatible DCE. A V.35-compatible DTE may be connected to the port using a DB25-to-MS34 adapter. **X.21** – The port is configured as an X.21-compatible DCE. An X.21-compatible DTE may be connected to the port using a DB25-to-DB15 adapter.
Network 1 FRF.8 Encapsulation Mode (9783 and 9788)
Possible Settings: **Translational, Transparent** Default Setting: **Transparent**
Specifies the type of FRF.8 upper-layer protocol encapsulation used on the link for each pair of interoperable Frame Relay and ATM PVCs. **Translational** – Encapsulated data is translated (RFC 1490 to RFC 1483). FrameSaver multiplexing and SLV communications are not supported in this mode. **Transparent** – Encapsulated data is forwarded without being translated.

Entering System Information and Setting the System Clock

Select System Information to set up or display the general SNMP name for the unit, the location, a contact for the unit, and set the system clock.

Main Menu→ Control→ System Information

The following information is available. Save any entries or changes.

If the selection is . . .	Enter the . . .
Device Name	Unique name to identify the device (up to 20 characters).
System Name	SNMP system name (up to 255 characters).
System Location	System's physical location (up to 255 characters).
System Contact	System person name and how to contact (up to 255 characters).
ATM Location ID	Identification of the ATM location for the system. The ID must be entered as 16 one-byte values, each conveyed as two hexadecimal characters, delimited by colons. When Clear is selected, all octets are filled with 6A (for example, 6A:6A:6A:6A...), which is the factory default and an invalid value. The values are restricted. ■ The first byte must be 01, 02, 03, FF, or 6A. ■ If the first octet is FF, the octets 2–16 must also be FF. ■ If the first octet is 6A, the octets 2–16 must also be 6A.
Date	Current date in the month/day/year format (mm/dd/yyyy).
Time	Current time in the hours:minutes:seconds format (hh:mm:ss).

NOTE:

To clear existing information, place the cursor in the Clear field (Tab to the Clear field) and press Enter.

Changing the Operating Mode

The FrameSaver unit can be connected to another FrameSaver unit without a frame relay switch between them. This is called back-to-back mode and can be used for demonstrations or for a point-to-point configuration over a leased line.

To change the operating mode, select Change Operating Mode from the Control menu:

Main Menu→ Control→ Change Operating Mode

On the ensuing screen, select Back-to-Back Operation or Standard Operation. Standard Operation is the default mode.

Configuration Option Tables

Configuration option descriptions contained in this chapter are in menu order, even though this may not be the order in which they are accessed when configuring the unit.

The following configuration option tables are included:

Configuring the Overall System

The System menu options are described in the following sections:

- *Configuring Frame Relay and LMI for the CSU/DSU*
- *Configuring Class of Service Definitions*
- *Code Point Definitions*
- *Service Level Verification Options* (Advanced SLM Feature Set)
- *Configuring General System Options*

Configuring Frame Relay and LMI for the CSU/DSU

Select Frame Relay and LMI from the System menu to display or change the Frame Relay and LMI (Local Management Interface) options for the entire system (see Table 4-2, CSU/DSU Frame Relay and LMI Options). The Frame Relay and LMI options do not apply to the router.

Main Menu→Configuration→System→Frame Relay and LMI

Table 4-2. CSU/DSU Frame Relay and LMI Options (1 of 3)

LMI Behavior (9720)
Possible Settings: **Independent, Net1-FR1_Follows_Port-1, Port-1_Follows_Net1-FR1, Port-1_Codependent_with_Net1-FR1** Default Setting: **Port-1_Codependent_with_Net1-FR1**
Allows the state of the LMI to be passed from one interface to another. **Independent** – The LMI state for each interface is handled separately, and is not affected by the LMI state of the other interface. **Net1-FR1_Follows_Port-1** – The LMI state for the Net1-FR1 interface follows the state of the LMI of the Port 1 interface. If the LMI is down on the Port 1 interface, the system brings down the LMI on the Net1-FR1 interface, and when the LMI is up on Port 1, the system brings up the LMI on the Net1-FR1 Interface. This setting is useful at a central site when the remote site router on the other end of the PVC connection can initiate recovery via a redundant central site when there is a catastrophic central site LAN or router failure. Not recommended for NSPs. **Port-1_Follows_Net1-FR1** – Brings down LMI on Port-1 when there is a physical failure on the network interface. When the alarm on the network interface is cleared, Port-1 is re-enabled and its control leads are reasserted. This setting is useful if the router connected to Port-1 is used to initiate recovery when network failures are detected. **Port-1_Codependent_with_Net1-FR1** – The LMI state for Port 1 and the Net1-FR1 interface are dependent on each other. If the LMI is down on either interface, the system will bring the LMI down on the other interface. When the LMI is up on either interface, the system will bring the LMI up on the other interface.

Table 4-2. CSU/DSU Frame Relay and LMI Options (2 of 3)

LMI Behavior (9783 and 9788)
Possible Settings: **Independent, Net1-FR1_Follows_Port-1, Port-1_Follows_Net1-FR1, Port-1_Codependent_with_Net1-FR1** Default Setting: **Port-1_Codependent_with_Net1-FR1**
Configures the state of LMI on Port-1 and the state of the ATM link on the network interface to be passed from one interface to another. **Independent** – Handles the state of each interface separately so that the LMI state of Port-1 has no effect on the state of the ATM link on the network interface, and vice versa. **Net1-FR1_Follows_Port-1** – Brings down VCs cross-connected to Port-1 on the network interface when LMI on Port-1 goes down, and sends F5 OAM cells on all network VCs cross-connected to Port-1 DLCIs to alert the network and far-end device that frame relay data can not be delivered through the device. When LMI on Port-1 comes back up, the network VCs are also re-enabled. This setting is useful at a central site when the remote site router on the other end of the PVC connection can initiate recovery via a redundant central site when there is a catastrophic central site LAN or router failure. Not recommended for NSPs. **Port-1_Follows_Net1-FR1** – Brings down LMI on Port-1 when there is a physical failure or ATM failure on the network interface. When the alarm on the network interface is cleared, Port-1 is re-enabled and its control leads are reasserted. This setting is useful if the router connected to Port-1 is used to initiate recovery when network failures are detected. **Port-1_Codependent_with_Net1-FR1** – The LMI state for Port 1 and the Net1-FR1 interface are dependent on each other. If the LMI is down on either interface, the system will bring the LMI down on the other interface. When the LMI is up on either interface, the system will bring the LMI up on the other interface. When Port-1 LMI goes down, in addition to bringing down the internal network frame relay link, the unit also sends F5 OAM cells on all network VCs cross-connected to Port-1 DLCIs to alert the network and far-end device that frame relay data can not be delivered through the device. Use this setting when backup is through the router instead of the unit. Note that when the router is disconnected, the NSP cannot access the unit using multiplexed VCs.
LMI Error Event (N2)
Possible Settings: **1 – 10** Default Setting: **3**
Configures the LMI-defined N2 parameter, which sets the number of errors that can occur on the LMI link before an error is reported. Applies to both the user and network sides of a UNI. **1 – 10** – Specifies the maximum number of errors before reported.
LMI Clearing Event (N3)
Possible Settings: **1 – 10** Default Setting: **1**
Configures the LMI-defined N3 parameter with the number of error-free messages that must be received before clearing an error event. Applies to both the user and network sides of a UNI. **1 – 10** – Specifies how many error-free messages it will take to clear the error event.

Table 4-2. CSU/DSU Frame Relay and LMI Options (3 of 3)

LMI Status Enquiry (N1)
Possible Settings: **1 – 255** Default Setting: **6**
Configures the LMI-defined N1 parameter, which sets the number of status enquiry polling cycles that the user side of the LMI initiates before a full status enquiry is initiated. Applies to the user side of a UNI only. **1 – 255** – Specifies the number of status enquiry polling cycles that can be initiated before a full status enquiry is initiated.
LMI Heartbeat (T1)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **10**
Configures the LMI-defined T1 parameter with the number of seconds between the initiation of status inquiry messages on the user side of the LMI. Applies to the user side of a UNI only. **5 – 30** – Specifies the number of seconds between the initiation of status inquiry messages in increments of 5 seconds.
LMI Inbound Heartbeat (T2)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **15**
Configures the LMI-defined T2 parameter with the number of seconds between the receipt of status enquiry messages on the network side of the LMI. Applies to the network side of a UNI only. **5 – 30** – Specifies the number of seconds between the receipt of status enquiry messages in increments of 5 seconds.
LMI N4 Measurement Period (T3)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **20**
Configures the LMI-defined T3 parameter with the time interval in seconds that the LMI network side uses to measure the maximum number of status enquiry messages that have been received (N4) from the user side. Applies to the network side of a UNI only. **5 – 30** – Specifies the interval of time in increments of 5 seconds.

Configuring Class of Service Definitions

Select Class of Service Definitions from the System menu to display or change the Class of Service definitions to be used with latency, availability, and throughput measurements of IP traffic on IP Enabled circuits.

Main Menu→ Configuration→ System →Class of Service Definitions

The Class of Service Definitions screen appears.

▶ Procedure

To create a new Class of Service definition:

1. To manually assign definition names and code points, proceed to Step 4
2. To automatically create Class of Service names and associate them with code points according to RFCs 2474, 2497, and 2498, select RfcCodePoints. The following settings are established:

Field	Setting After RfcCodePoints Selected
Class of Service Name	1 – NewCtrl 2 – Expd Fwd 3 – AFClass4 4 – AFClass3 5 – AFClass2 6 – AFClass1 7 – Default
Measure Latency & Availability	1 – N 2 – Y 3 – Y 4 – Y 5 – Y 6 – Y 7 – Y
Code Points	1 (NetwCtrl) – 110000, 111000 2 (Expd Fwd) – 101110 3 (AFClass4) – 100010, 100100, 100110 4 (AFClass3) – 011010, 011100, 011110 5 (AFClass2) – 010010, 010100, 010110 6 (AFClass1) – 001010, 001100, 001110 7 (Default) – 000000

3. If these settings are satisfactory, proceed to Step 10.
4. Type a name of up to 8 characters into one of the Name fields next to IDs 1–6.
5. To unassign all code points by inserting blank names, select ClrAllCodePoints. To assign all Code Points to a Class of Service name of Default, select DefaultCodePoints.
6. Select PgDn or PgUp. The Code Point Assignment screen appears.
7. For any Code Point you want to assign to the name, type the name you selected in Step 4 into the Name field to the right of the Code Point.

8. Select Save, then select PgDn or PgUp. The Class of Service Definitions page reappears. In the Code Points Assigned column next to your selected name there is now a Y for Yes.
9. If latency and availability should be measured for the selected name, change the N in the Measure Latency & Availability column to Y.
10. Select Save.

To configure these options, Service Type on the Easy Install screen must be set to Frame Relay.

Table 4-3. Class of Service Definitions

Class of Svc Name
Possible Settings: ***ASCII Text Entry*** Default Setting: – *For IDs 2–7:* **blank** – *For ID 1:* **Default**
Specifies a name to identify a Class of Service definition. ***ASCII Text Entry*** – Enter a unique name for the definition (maximum length 8 characters).
Measure Latency & Availability
Possible Settings: **N, Y** Default Setting: – *For IDs 2–7:* **N** – *For ID 1:* **Y**
Determines whether latency and availability are measured for this Class of Service ID. *Display Conditions* – This option is set to N and is read-only until the class of service is defined and code points are assigned to it. **N** – Latency and availability are not measured for this Class of Service ID. **Y** – Latency and availability are measured for this Class of Service ID.
Code Points Assigned
Possible Settings: **Y, N** Default Setting: – *For IDs 2–7:* **N** – *For ID 1:* **Y**
This read-only field shows whether a Code Point has been assigned to this Class of Service ID on the Code Point Definitions screen. **N** – No Code Point is assigned to this ID. **Y** – At least one Code Point is assigned to this ID.

Code Point Definitions

Select Class of Service Definitions from the System menu, then PgDn or PgUp, to display or change the Code Point definitions for a Class of Service ID. See *Configuring Class of Service Definitions* on page 4-13 for instructions.

Table 4-4. Code Point Definitions

Code Pnt
Possible Settings: **000000–111111** Default Setting: None.
This read-only field shows the possible Code Points. Code Points are described in RFC 2474.
ID
Possible Settings: **1–7** Default Setting: **1**
This read-only field shows the ID associated with the Name field. If you change a name in a Name field on this screen and select Save, the ID changes to match the name.
Name
Possible Settings: ***ASCII Text*** Default Setting: **Default**
The Name field specifies the Class of Service to which you want to assign the Code Point. ***ASCII Text*** – Specifies one of the Class of Service Names entered on the Class of Service Definitions screen.

Configuring Service Level Verification Options

SLV options are selected from the System menu.These options only appear when SLV is activated in the unit (see *Advanced SLM Feature Set* in Chapter 1, *About FrameSaver DSL Devices*, for information about this feature).

Main Menu→ Configuration→ System→ Service Level Verification

NOTE:

Options in Table 4-5, Service Level Verification Options, are not valid when FRF.8 Encapsulation mode is set to Translational (see Table 4-12, Network ATM Options, for details).

Table 4-5. Service Level Verification Options (1 of 3)

SLV Sample Interval (secs)
Possible Settings: **10 – 3600** Default Setting: **60**
Sets the inband communications interval between FrameSaver SLV devices. Inband communications are used to pass frames that calculate latency, as well as transmission success and other SLV information. **10 – 3600** – Sets the SLV Sample Interval (secs) in seconds.
SLV Synchronization Role
Available Settings: **Tributary, Controller, None** Default Setting: **Tributary**
Determines the role the unit plays in maintaining synchronization of user history data collection and storage between SLV devices. **Tributary** – Uses network timing received from incoming SLV communications and provides network-based synchronization information to other devices in the network. **Controller** – Uses its own internal time-of-day clock and provides synchronization information to other devices in the network based upon its own clock. NOTE: Only one device in the network should be configured as the SLV synchronization controller. **None** – Incoming timing information is ignored and no timing information is sent out. This setting should only be used when network synchronization is not desirable, or when a single unit connects multiple networks or network segments.

Table 4-5. Service Level Verification Options (2 of 3)

SLV Type
Available Settings: **Standard, COS 1–COS 7** Default Setting: – *If SLV Feature is enabled:* **Standard** – *If SLV Feature is disabled:* **COS 1**
Determines the type of SLV measurements to which these other SLV options apply: ■ SLV Timeout Error Event Threshold ■ SLV Timeout Clearing Event Threshold ■ SLV Round Trip Latency Error Threshold ■ SLV Latency Clearing Event Threshold ■ SLV Packet Size **Standard** – The options selected apply to standard FrameSaver SLV measurements, utlizing an EDLCI for FrameSaver-to-FrameSaver communication. This option is not available if the SLV Feature is disabed. **COS 1–COS 7** – The options selected apply to this Class of Service. Different settings may be saved for each Class of Service.
SLV Delivery Ratio
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether communication of Frame and Data Delivery Ratios (FDR/DDR) between FrameSaver SLV devices is enabled. This capability requires FrameSaver SLV units at both ends of the PVC, running software version 1.2 or higher. *Display Conditions* – This option appears only if SLV Type is Standard. **Enable** – An extra byte for FDR/DDR statistics collection is included with each frame, which is used at the receiving end to determine the amount of data dropped by the network. **Disable** – Extra byte is not included.
DLCI Down on SLV Timeout
Available Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether a DLCI is declared Inactive after the configured threshold for SLV Timeout has been exceeded. *Display Conditions* – This option appears only if SLV Type is Standard. NOTE: This option does not apply to multiplexed DLCIs connected to a far-end unit with hardware bypass capability. **Enable** – After the configured threshold for missed SLV packets has been exceeded, the DLCI's status is changed to Inactive. **Disable** – An SLV Timeout Error Event does not affect DLCI status.

Table 4-5. Service Level Verification Options (3 of 3)

SLV Timeout Error Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **3**
Specifies the number of consecutive missed SLV packets that must be detected before an SLV Timeout Error Event is declared. **1–20** – Sets the limit for these error events.
SLV Timeout Clearing Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **1**
Specifies the number of consecutive SLV messages that must be received before the DLCI Inactive status is cleared. **1 – 20** – Sets the limit for the clearing event.
SLV Round Trip Latency Error Threshold
Available Settings: **50 – 10000** Default Setting: **10000**
Specifies, in milliseconds, the 15-sample average round trip latency which must be exceeded before an SLV Latency Threshold alarm event is declared. If SLV Type is Standard, the latency applies to a multiplexed DLCI. If SLV Type is a Class of Service (COS 1 – COS 7), the latency applies to the COS on an IP Enabled path. **50 – 10000** – Sets the limit for the clearing event.
SLV Latency Clearing Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **1**
Specifies the number of consecutive SLV latency measurements below the error threshold that must be received before the error status is cleared. **1 – 20** – Sets the limit for the clearing event.
SLV Packet Size (bytes)
Available Settings: **64 – 2048** Default Setting: **64**
Sets the size of packets, in bytes, that will be used for SLV communications. SLV packets are used to track latency and other SLV-related variables. When the packet size is changed, a new round trip and average latency calculation must be performed, so these measurements will not appear on the SLV Performance Statistics screen until a new sampling interval has occurred. **64 – 2048** – Sets the packet size for SLV communications.

Configuring General System Options

Select General from the System menu to configure the general system configuration options (see Table 4-6, General Options).

Main Menu→ Configuration→ System→ General

Table 4-6. General Options

Test Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines if loopback and pattern tests terminate automatically. This setting does not effect DTE-commanded tests or the LMI Packet Capture Utility feature. **Enable** – All Loopback and Pattern tests have an automatic timeout. This setting is recommended when the FrameSaver unit is managed remotely via an inband data stream. If the FrameSaver unit is accidently commanded to execute a disruptive test on the interface providing management access, control can be regained after the timeout expires, causing the test to terminate. **Disable** – Loopback and pattern tests must be manually terminated.
Test Duration (min)
Possible Settings: **1 – 120** Default Setting: **10**
Specifies the maximum duration of user-initiated tests. *Display Conditions* – This option appears only when Test Timeout is set to Enable. **1 – 120** – Sets the Test Timeout period in minutes.

Configuring Network Interfaces

Configuration of network interface is described in the following sections:

- *Configuring the Network Physical Interface*
- *Configuring Frame Relay for the Network Interface*
- *Configuring DLCI Records for the Network Interface (9720)*
- *Configuring Circuit Records for the Network Interface (9783, 9788)*
- *Configuring ATM for the Network Interface (9783, 9788)*

Configuring the Network Physical Interface

When configuring network interface physical characteristics, select Physical from the Network menu. See Table 4-7, Network Physical Interface Options (9720), Table 4-7, Network Physical Interface Options (9720), or Table 4-9, Network Physical Interface Options (9788).

Main Menu→Configuration→Network→Physical

Table 4-7. Network Physical Interface Options (9720)

Operating Rate
Possible Settings: **AutoRate, 64, 128, 144** Default Setting: **AutoRate**
Specifies the IDSL line rate. **AutoRate** – The line rate is automatically detected when the frame relay LMI is brought up on one or both channels. **64** – The line rate is 64 kbps. One B channel is used for the data transfer, and automatic rate detection is disabled. **128** – The line rate is 128 kbps. Both B channels are used for the data transfer, and automatic rate detection is disabled. **144** – The line rate is 144 kbps. Both B channels are used for the data transfer, and automatic rate detection is disabled.
Channel
Possible Settings: **B1, B2** Default Setting: **B1**
Specifies the B channel used for data transfer when the line rate is 64 kbps. *Display Conditions* – Channel appears only when Operating Rate is set to 64. **B1** – The B1 channel is used for data transfer. **B2** – The B2 channel is used for data transfer.

Table 4-8. Network Physical Interface Options (9783)

Line Rate Mode
Possible Settings: **Hunt, AutoRate, Fixed** Default Setting: **AutoRate**
Specifies the mode to be used for rate selection. **Hunt** – The unit attempts to train at rate specified by DSL Line Rate. If that fails, the unit attempts to train at the next higher rate, and, if unsuccessful, cycles through all the rates until training is successful or the unit is reset. **AutoRate** – The unit automatically detects the line rate from the network interface. **Fixed** – The unit uses the line rate specified by DSL Line Rate.
DSL Line Rate (Kbps)
Possible Settings: – *If DSLAM Type is set to Paradyne, or if DSLAM Type is set to Nokia and Line Rate Mode is set to Fixed:* **144, 192, 208, 256, 272, 384, 400, 512, 528, 768, 784, 1024, 1152, 1168, 1536, 1552, 2320** – *If DSLAM Type is set to Alcatel (NewBridge):* **208, 400, 784, 1168, 1552, 2320** – *If DSLAM Type is set to Nokia and Line Rate Mode is set to Hunt:* **192, 384, 768, 1152, 1536** – *If DSLAM Type is set to PairGain:* **144, 192, 208, 256, 272, 384, 400, 512, 528, 768, 784, 1024, 1152, 1168, 1536, 1552, 2320** Default Setting: – *If DSLAM Type is set to Alcatel (NewBridge) and Line Rate Mode is set to Hunt:* **208** – *If DSLAM Type is set to Nokia and Line Rate Mode is set to Hunt:* **384** – *If DSLAM Type is set to PairGain and Line Rate Mode is set to Fixed:* **784** – *(If DSLAM Type is set to Paradyne, Line Rate Mode is set to AutoRate and DSL Line Rate does not appear)*
Determines the rate on the DSL network interface (if Line Rate Mode is Fixed), or the rate the device will first use to attempt to train (if Line Rate Mode is Hunt). *Display Conditions* – DSL Line Rate does not appear if DSL Line Rate Mode is set to AutoRate. **144 – 2320** – The DSL line rate is set to the specified rate in Kbps.
SNR Margin Alarm Threshold (dB)
Possible Settings: **–5, –4, –3, –2, –1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **3**
Specifies the level in decibels at which a Signal to Noise Ratio (SNR) margin alarm condition is declared. **–5 – 10** – Specifies the threshold level in dB.

Table 4-9. Network Physical Interface Options (9788)

Line Rate Mode
Possible Settings: **AutoRate, Fixed** Default Setting: **AutoRate**
Specifies the mode to be used for rate selection. **AutoRate** – The unit automatically detects the line rate from the network interface. **Fixed** – The unit uses the line rate specified by DSL Line Rate.
DSL Line Rate (Kbps)
Possible Settings: – *If PSD Mask is Symmetric:* **200, 264, 328, 392, 456, 520, 584, 648, 712, 776, 784, 840, 904, 968, 1032, 1096, 1160, 1224, 1288, 1352, 1416, 1480, 1544, 1552, 1608, 1672, 1736, 1800, 1864, 1928, 1992, 2056, 2120, 2184, 2248, 2312** – *If PSD Mask is Asymmetric (available in future release) and Region is Annex A:* **776, 784, 1544, 1552** – *If PSD Mask is Asymmetric (available in future release) and Region is Annex B:* **2056, 2312** Default Setting: [Depends on settings of Line Rate Mode, PSD Mask, and Region]
Determines the rate on the DSL network interface. Valid rates, and the rates presented on the screen, depend on the values of Region and PSD Mask. If a change to another configuration option renders the selected DSL Line Rate invalid, the Line Rate Mode is set to AutoRate. *Display Conditions* – DSL Line Rate does not appear if DSL Line Rate Mode is set to AutoRate. **200 – 2312** – The DSL line rate is set to the specified rate in Kbps.
Region
Possible Settings: **Annex A, Annex B** Default Setting: [Depends on model]
Determines the annex of the G.991.2 recommendation that the unit will conform to. The value of Region in part determines what DSL Line Rates are available. If a change in the Region renders the current DSL Line Rate invalid, the Line Rate Mode is set to AutoRate. **Annex A** – The unit conforms to Annex A (for North America). **Annex B** – The unit conforms to Annex B (for Europe).
PSD Mask
Possible Settings: **Symmetric** Default Setting: **Symmetric**
Read-only. Specifies the Power Spectral Density (PSD) mask the unit will use. The value of PSD Mask in part determines what DSL Line Rates are available. If a change in the PSD Mask setting (available in a future release) renders the current DSL Line Rate invalid, the Line Rate Mode is set to AutoRate. **Asymmetric** – (Future use.) The unit uses the asymmetric PSD mask. **Symmetric** – The unit uses the symmetric PSD mask.

Configuring Frame Relay for the Network Interface

Select Frame Relay from the Network menu to display or change the network Frame Relay options (see Table 4-10, Network Frame Relay Options).

Main Menu→Configuration→Network →Frame Relay

Table 4-10. Network Frame Relay Options

Traffic Policing
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines if CIR (Committed Information Rate) and EIR (Excess Information Rate) are enforced by the unit on frames sent to the network interface. **Enable** – CIR and EIR are enforced: – Frames that exceed CIR are marked Discard Eligible (DE). – Frames in excess of EIR are discarded. – For the CSU/DSU only, DE frames received from the external router are credited as frames transmitted above CIR. They are credited as frames transmitted between CIR and EIR until that count reaches its limit, at which point they are counted as frames transmitted above EIR. **Disable** – CIR and EIR are not enforced.

Configuring DLCI Records for the Network Interface (9720)

DLCI records can be created and modified using the Network DLCI Records screen.

Main Menu →Configuration →Network →DLCI Records

DLCI Records options are similar for the network, data ports, and virtual router ports. See *Configuring DLCI Records* on page 4-32.

Configuring Circuit Records for the Network Interface (9783, 9788)

Circuit records can be created or modified and PVCs can be created based on existing DLCIs using the Network Circuit Records screen.

Main Menu → *Configuration* → *Network* → *Circuit Records*

If any DLCI records exist, you may enter a DLCI number at the bottom of the screen to display, copy from, or modify a DLCI record.

Select CreatePVC to create a new PVC based on an existing DLCI record.

Table 4-11. Circuit Records Options (1 of 3)

DLCI Number
Possible Settings: **16 – 1007** Default Setting: Initially blank
Specifies the number for the DLCI in the DLCI record. The parameter determines which DLCI record is used for transferring data on a particular frame relay interface. DLCI numbers range from 0–1023 with numbers 0–15 and 1008–1023 reserved. Entry of an invalid number results in the error message **`Value Out of Range (16-1007)`**. If the DLCI number is part of a connection, this field is read-only. NOTES: – If a DLCI number is not entered, the DLCI record is not created. – The DLCI number entered must be unique for the interface. – Changing this setting causes the FrameSaver unit to abort any active frame relay tests. **16 – 1007** – Specifies the DLCI number.
VPI,VCI Number
Possible Settings: – *For the VPI:* **0 – 15** – *For the VCI:* **32 – 255** Default Setting: Initially blank
Specifies the VPI and VCI. Entry of an invalid number results in the error message **`Value Out of Range (0 – 15)`** for the VPI, and **`Value Out of Range (32 – 255)`** for the VCI. The VPI/VCI must be unique on the ATM link. **0 – 15** – Specifies the VPI. **32 – 255** – Specifies the VCI.

Table 4-11. Circuit Records Options (2 of 3)

DLCI Type
Possible Settings: **Standard, Multiplexed, IP Enabled** Default Setting: **Multiplexed**
Specifies whether the DLCI is standard, multiplexed, or IP Enabled. This field is read-only when the selected DLCI is used in a PVC or Management link connection and the DLCI Type is Standard. *Display Conditions* – This option cannot be changed if the DLCI is specified as the TS Access Management Link. It is not applicable when FRF.8 Encapsulation Mode is set to Translational (see Table 4-12, Network ATM Options). **Standard** – Supports standard DLCIs as specified by the Frame Relay Standards. Use this setting when a non-FrameSaver unit is at the other end. **Multiplexed** – Enables multiplexing of multiple connections into a single DLCI. Allows a single PVC through the frame relay network to carry multiple DLCIs as long as these connections are between the same two endpoints (proprietary). Do not select Multiplexed unless there are FrameSaver units at both ends of the connection. **IP Enabled** – Enables connection to one or more endpoints through a Layer 3 network. A Payload Management PVC is created as well as the IP Enabled DLCI.
CIR (bps)
Possible Settings: – *9783:* **0 – 2320000** – *9788:* **0 – 2312000** Default Setting: **0**
Determines the data rate in bits per second for the DLCI that the network commits to accept and carry without discarding frames. Entry of an invalid rate causes the error message **`Value Out of Range (0 – x)`**, where ***x*** is the maximum line rate available on the port. **0 – *maximum*** – Specifies the network-committed data rate.
Tc
Possible Settings: **1 – 65535** Default Setting: Read-Only
Displays the DLCI's calculated value of its committed rate measurement interval (Tc) in milliseconds based on the CIR (bps) and Committed Burst Size Bc (Bits) settings.
Committed Burst Size Bc (Bits)
Possible Settings: **CIR, Other** Default Setting: **CIR**
Specifies whether the DLCI's committed burst size uses the CIR setting or is entered independently. This value is the maximum amount of data that the service provider has agreed to accept during the committed rate measurement interval (Tc). **CIR** – Uses the value in the CIR (bps) option as the committed burst size (Bc). The Bc and excess burst size (Be) options are updated when a CIR update is received from the network switch. **Other** – Allows you to specify the committed burst size for the DLCI. When Other is selected, the Bc and Be values must be manually entered and maintained.

Table 4-11. Circuit Records Options (3 of 3)

Bc
Possible Settings: – *9783:* **0 – 2320000** – *9788:* **0 – 2312000** Default Setting: **0**
Allows you to display or change the DLCI's committed burst size. *Display Conditions* – This option appears only when Committed Burst Size is set to Other. **0 – *maximum*** – Specifies the DLCI's committed burst size.
Excess Burst Size Be (Bits)
Possible Settings: – *9783:* **0 – 2320000** – *9788:* **0 – 2312000** Default Setting: – *9783:* **2320000** – *9788:* **2312000**
Specifies the maximum amount of data in bits that the network may accept beyond the CIR without discarding frames. *Display Conditions* – This option appears only when Committed Burst Size is set to Other. **0 – *maximum*** – Specifies the DLCI's committed burst size.
Outbound Management Priority
Possible Settings: **Low, Medium, High** Default Setting: **Medium**
Specifies the relative priority for management traffic sent on management PVCs on this DLCI to the network. **Low** – Management data configured for the DLCI has low priority. **Medium** – Management data configured for the DLCI has medium priority. **High** – Management data configured for the DLCI has high priority.

Configuring ATM for the Network Interface (9783, 9788)

Select ATM from the Network menu to display or change ATM option settings (see Table 4-12, Network ATM Options).

Main Menu→ Configuration→ Network → ATM

Table 4-12. Network ATM Options

Cell Payload Scrambling
Possible Settings: **Enable, Disable** Default Setting: – *9783 – If DSLAM Type is set to Paradyne:* **Enable** – *9783 – If DSLAM Type is set to a non-Paradyne DSLAM:* **Disable** – *9788:* **Enable**
Specifies whether the 48-byte information field of ATM cells is scrambled/descrambled per ANSI T1.646 on this ATM link. NOTE: For the 9783 CSU/DSU, the default setting is changed based upon the DSLAM Type setting. See *DSLAM Type (9783)* on page 4-4 for more information. **Enable** – Activates scrambling/descrambling of transmitted or received ATM cells. **Disable** – No scrambling/descrambling is performed.
Cell Delineation Error Event Threshold
Possible Settings: **1 – 1000** Default Setting: **10**
Specifies the number of OCD (Out of Cell Delineation) events that must occur in a one-minute interval for an LCD (Loss of Cell Delineation) alarm to be declared. **1 – 1000** – Specifies the LCD alarm threshold.
FRF.8 Encapsulation Mode
Possible Settings: **Translational, Transparent** Default Setting: **Transparent**
Specifies the type of FRF.8 upper-layer protocol encapsulation used on the link for each pair of interoperable Frame Relay and ATM PVCs. **Translational** – Encapsulated data is translated (RFC 1490 to RFC 1483). FrameSaver multiplexing and SLV communications are not supported in this mode. **Transparent** – Encapsulated data is forwarded without being translated.
ILMI
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies the state of the Integrated Local Management Interface (ILMI). ILMI can be used in support of hybrid management, allowing access to the endpoint from a DSL provider's Network Operation Center using the same management PVC that is used to manage the DSLAM. **Enable** – The ILMI channel is enabled. SNMP traffic, embedded in the ATM cells, is supported. **Disable** – The ILMI channel is disabled.

Configuring the User Data or Virtual Router Port

The following user data port and virtual router port interface characteristics are described in the following sections:

- *Configuring the CSU/DSU's Data Port Physical Interface*
- *Configuring Frame Relay on the CSU/DSU's Data Port*
- *Configuring DLCI Records*

Configuring the CSU/DSU's Data Port Physical Interface

Select Physical from the Data Ports menu to configure the user data port physical characteristics (see Table 4-13, CSU/DSU Data Port Physical Interface Options).

Main Menu→Configuration→Data Ports→Physical

Data Port Physical Interface Options do not apply to the router.

Table 4-13. CSU/DSU Data Port Physical Interface Options (1 of 2)

Port Type (9788)
Possible Settings: **E530, V.35, X.21** Default Setting: **V.35**
Determines the configuration of the data port. **E530** – The port is configured as an EIA-530-A-compatible DCE. An EIA-530-A-compatible DTE may be directly connected to the DB25 connector for the port. **V.35** – The port is configured as a V.35-compatible DCE. A V.35-compatible DTE may be connected to the port using a DB25-to-MS34 adapter. **X.21** – The port is configured as an X.21-compatible DCE. An X.21-compatible DTE may be connected to the port using a DB25-to-DB15 adapter.
Invert Transmit Clock
Possible Settings: **Auto, Enable, Disable** Default Setting: **Auto**
Determines if the FrameSaver unit clock on interchange circuit DB (ITU 114) – Transmit Signal Element Timing (DCE Source) TXC is phase inverted with respect to the clock used to time the incoming Transmitted Data (TD). **Auto** – The port will check the clock supplied by the DCE on TXC on this port. If necessary, the port will automatically phase invert the clock with respect to the transmitted data. **Enable** – Phase inverts the TXC clock. Use this setting when long cable lengths between the FrameSaver unit and the DTE are causing data errors. **Disable** – Does not phase invert the TXC clock.

Table 4-13. CSU/DSU Data Port Physical Interface Options (2 of 2)

Transmit Clock Source
Possible Settings: **Internal, External** Default Setting: **Internal**
Determines whether the DTE's transmitted data is clocked into the FrameSaver unit by internal transmit clock or external clock provided by the DTE. NOTE: Changing this setting causes the FrameSaver unit to abort any physical port tests, including any DTE-initiated loopback tests. **Internal** – The FrameSaver unit uses its own internal clock, the interchange circuit DB (ITU 114) – Transmit Signal Element Timing (TXC) (DCE source), for timing the incoming data. **External** – The DTE provides the clock for the transmitted data, and the FrameSaver unit uses the interchange circuit DA (ITU 113) – Transmit Signal Element Timing (XTXC) (DTE source) for timing the incoming data.
Monitor RTS (Control)
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies if the state of the Request To Send (RTS) circuits on the user data port are used to determine when valid data communication with the DTE is possible. When the RTS off condition is detected, CTS is deasserted, LMI is declared down, and no further transfer of frame relay data can occur on this interface. **Enable** – Interchange circuit CA (ITU 105) – RTS is monitored to determine when valid DTE data communication is possible. **Disable** – RTS is not monitored. RTS is assumed to be asserted and data is being transmitted, regardless of the state of the lead.
Monitor DTR
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the DTE Ready (DTR) circuit on the user data port used to determine when valid data communication is possible with the DTE. When the DTR off condition is detected, an alarm is generated, LMI is declared down, and no further transfer of frame relay data can occur on this interface. **Enable** – Interchange circuit CD (ITU 108/1/2) – DTR is monitored to determine when valid data is sent from the DTE. **Disable** – DTR is not monitored. DTR is assumed to be asserted and data is being transmitted, regardless of the state of the lead.
Port (DTE) Initiated Loopbacks
Possible Settings: **Local**, **Disable** Default Setting: **Disable**
Allows a local external DTE Loopback to be started or stopped via the port's attached DTE interchange lead LL (ITU 141). **Local** – The DTE attached to the port controls the local external DTE Loopback. **Disable** – The DTE attached to the port cannot control the local external DTE Loopback.

Configuring Frame Relay on the CSU/DSU's Data Port

Select Frame Relay from the Data Ports menu to configure the user data port frame relay characteristics (see Table 4-14, CSU/DSU Frame Relay Options).

Main Menu → *Configuration* → *Data Ports* → *Frame Relay*

Frame Relay Options do not apply to the router.

Table 4-14. CSU/DSU Frame Relay Options (1 of 2)

LMI Protocol
Possible Settings: **Initialize_From_Interface, Auto_On_LMI_Fail, Standard, Annex-A, Annex-D** Default Setting: **Initialize_From_Interface**
Specifies either the LMI protocol supported on the frame relay interface or the discovery source for the LMI protocol. **Initialize_From_Interface** – The LMI type supported on this frame relay link will be configured to match the LMI protocol discovered from the attached DTE device. Once a protocol has become active, the protocol will be set to the protocol discovered (Standard, Annex-A, or Annex-D) on the frame relay link. The frame relay link discovers the LMI protocol from an attached device via LMI status polls. The protocol will *not* be updated after the initial discovery. **Auto_On_LMI_Fail** – The LMI type supported on this frame relay link will be configured to match the LMI protocol discovered from the attached Network line or the DTE device when an LMI Link Down failure occurs. This option is available for frame relay links on the Port and network interfaces. The frame relay link discovers the LMI protocol from LMI status polls by the attached DTE device. **Standard** – Supports Standard LMI and the StrataCom enhancements to the Standard LMI. **Annex-A** – Supports LMI as specified by Q.933, Annex A. **Annex-D** – Supports LMI as specified by ANSI T1.617, Annex D.
LMI Parameters
Possible Settings: **System**, **Custom** Default Setting: **System**
Allows you to use the system LMI options or to set specific LMI options for this interface. **System** – Use system LMI options (refer to Table 4-2, CSU/DSU Frame Relay and LMI Options). **Custom** – Use the following options in this table to configure LMI parameters.
LMI Error Event (N2)
Possible Settings: **1 – 10** Default Setting: **3**
Configures the LMI-defined N2 parameter, which sets the number of errors that can occur on the LMI link before an error is reported. Applies to both the user and network sides of an UNI. *Display Conditions* – This option appears only when LMI Parameters is set to Custom. **1 – 10** – Specifies the maximum number of errors.

Table 4-14. CSU/DSU Frame Relay Options (2 of 2)

LMI Clearing Event (N3)
Possible Settings: **1 – 10** Default Setting: **1**
Configures the LMI-defined N3 parameter, which sets the number of error-free messages that must be received before clearing an error event. Applies to UNI user and network sides. *Display Conditions* – This option appears only when LMI Parameters is set to Custom. **1 – 10** – Specifies how many error-free messages it will take to clear the error event.
LMI Inbound Heartbeat (T2)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **15**
Configures the LMI-defined T2 parameter, which sets the number of seconds between the receipt of status enquiry messages on the network side of the LMI. Applies to the network side of a UNI only. *Display Conditions* – This option appears only when LMI Parameters is set to Custom. **5 – 30** – Specifies the number of seconds between the receipt of status enquiry messages in increments of 5 seconds.
LMI N4 Measurement Period (T3)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **20**
Configures the LMI-defined T3 parameter, which is the time interval (in seconds) that the network side of the LMI uses to measure the maximum number of status enquiry messages that have been received (N4) from the user side. *Display Conditions* – This option appears only when LMI Protocol is set to Standard and LMI Parameters is set to Custom. **5 – 30** – Specifies the interval of time in increments of 5 seconds.

Configuring DLCI Records

Depending on the model, DLCI records can be created and modified, and PVCs created based on existing DLCIs, using the Network, Data Ports, or Virtual Router Ports DLCI Records screen.

Main Menu → Configuration → Network → DLCI Records

Main Menu → Configuration → Data Ports → DLCI Records

Main Menu → Configuration → Virtual Router Ports → DLCI Records

Table 4-15. DLCI Records (1 of 3)

DLCI Number
Possible Settings: **16 – 1007** Default Setting: Initially blank
Specifies the number for the DLCI in the DLCI record. The parameter determines which DLCI record is used for transferring data on a particular frame relay interface. DLCI numbers range from 0–1023 with numbers 0–15 and 1008–1023 reserved. Entry of an invalid number results in the error message **`Value Out of Range (16-1007)`**. If the DLCI number is part of a connection, this field is read-only. NOTES: – If a DLCI number is not entered, the DLCI record is not created. – The DLCI number entered must be unique for the interface. – Changing this setting causes the FrameSaver unit to abort any active frame relay tests. **16 – 1007** – Specifies the DLCI number.
DLCI Type
Possible Settings: **Standard, Multiplexed, IP Enabled** Default Setting: **Multiplexed**
Specifies whether the DLCI is standard or multiplexed. This field is read-only when the selected DLCI is used in a PVC or Management link connection and the DLCI Type is Standard. This option cannot be changed if the DLCI is specified as the TS Access Management Link. **Standard** – Supports standard DLCIs as specified by the Frame Relay Standards. Use this setting when a non-FrameSaver unit is at the other end. **Multiplexed** – Enables multiplexing of multiple connections into a single DLCI. Allows a single PVC through the frame relay network to carry multiple DLCIs as long as these connections are between the same two endpoints (proprietary). Do not select Multiplexed unless there are FrameSaver units at both ends of the connection. **IP Enabled** – Enables connection to one or more endpoints through a Layer 3 network. A Payload Management PVC is created as well as the IP Enabled DLCI.

Table 4-15. DLCI Records (2 of 3)

CIR (bps)
Possible Settings: – *9720:* **0 – 144000** – *9783:* **0 – 2320000** – *9788:* **0 – 2312000** Default Setting: **0**
Determines the data rate for the DLCI that the network commits to accept and carry without discarding frames; the CIR in bits per second. Entry of an invalid rate causes the error message **`Value Out of Range (0 – x)`**, where ***x*** is the maximum line rate available on the port. **0 – *maximum*** – Specifies the network-committed data rate.
Committed Burst Size Bc (Bits)
Possible Settings: **CIR, Other** Default Setting: **CIR**
Specifies whether the DLCI's committed burst size will follow the CIR, or whether it will be entered independently. This value is the maximum amount of data that the service provider has agreed to accept during the committed rate measurement interval (Tc). **CIR** – Uses the value in the CIR (bps) option as the committed burst size (Bc). The Bc and excess burst size (Be) options are updated when a CIR update is received from the network switch. **Other** – Allows you to specify the committed burst size for the DLCI. When Other is selected, the Bc and Be values must be manually entered and maintained, as well.
Bc
Possible Settings: – *9720:* **0 – 144000** – *9783:* **0 – 2320000** – *9788:* **0 – 2312000** Default Setting: **0**
Allows you to display or change the DLCI's committed burst size. *Display Conditions* – This option appears only when Committed Burst Size is set to Other. **0 – *maximum*** – Specifies the DLCI's committed burst size.

Table 4-15. DLCI Records (3 of 3)

Excess Burst Size Be (Bits)
Possible Settings: – *9720:* **0 – 144000** – *9783:* **0 – 2320000** – *9788:* **0 – 2312000** Default Setting: – *9720:* **144000** – *9783:* **2320000** – *9788:* **2312000**
Specifies the maximum line rate on the port; the amount of data in bits that the network may accept beyond the CIR without discarding frames. **0 – *maximum*** – Specifies the DLCI's excess burst size.
DLCI Priority
Possible Settings: **Low, Medium, High** Default Setting: **High**
Specifies the relative priority for data received on the DLCI from an attached device (also known as QoS). All data on Port 1 is cut-through, as long as there is no higher-priority data queued from another user port. The DLCI priority set for an interface applies to data coming into that interface. For example, the priority set for DLCIs on Port 1 applies to data coming into Port 1 from the attached equipment (such as a router). *Display Conditions* – This option is not available for the network interface. **Low** – Data configured for the DLCI has low priority. **Medium** – Data configured for the DLCI has medium priority. **High** – Data configured for the DLCI has high priority.
Outbound Management Priority
Possible Settings: **Low, Medium, High** Default Setting: **Medium**
Specifies the relative priority for management traffic sent on this DLCI to the network. *Display Conditions* – This option is not available for data ports. **Low** – Management data configured for the DLCI has low priority. **Medium** – Management data configured for the DLCI has medium priority. **High** – Management data configured for the DLCI has high priority.

Configuring PVC Connections

TS Management is initially enabled and configured on VPI,VCI 0,35 by default. Any valid DLCI, VPI,VCI can be used.

Main Menu→ Configuration→ PVC Connections

From this screen, create the PVC connections and go directly to the Management PVC screen by selecting the MgmtPVCs function key. See *Configuring Management PVCs* on page 4-41 for management PVC configuration options.

You can quickly remove unused DLCIs in an existing PVC connection by selecting the Delete function key and responding Yes to the **`Remove otherwise unused components associated with the deleted PVC?`** prompt.

Table 4-16. PVC Connections (1 of 2)

Source Link
Possible Settings: **Port-1, Net1-FR1** Default Setting: Initially blank
Specifies the frame relay interface that starts a PVC connection; the **from** end of a from-to link. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined that are not part of a PVC connection or management link. For example, if Port-1 has no DLCIs defined, Port-1 would not appear as a valid setting. **Port-1** – For the FrameSaver CSU/DSU, specifies the user data port as the source link. **Net1-FR1** – Specifies the Network interface or network data port as the source link. **Clear All** – Clears all Link and DLCI settings, and suppresses EDLCIs.
Source DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank
Specifies the source DLCI for a frame relay interface. The DLCI must be defined and cannot be part of a PVC connection or management link. For multiplexed DLCIs, at least one EDLCI must be unconnected for the DLCI to be a valid selection. NOTE: Source DLCI has no value if Source Link contains no value. **16 – 1007** – Specifies the DLCI number.
Source EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank
Specifies the source Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection. *Display Conditions* – This option appears only when Source DLCI contains a multiplexed DLCI record number, and is not applicable when FRF.8 Encapsulation Mode is set to Translational (see Table 4-12, Network ATM Options). **0 – 62** – Specifies the EDLCI number.

Table 4-16. PVC Connections (2 of 2)

Destination Link
Possible Settings: **Net1-FR1** Default Setting: Initially blank
Specifies the frame relay interface used as the destination link; the **to** end of a from-to link. The only valid setting for this option is a frame relay interface that has at least one DLCI or EDLCI defined which is not part of a PVC connection or management link; i.e., if the network interface has no DLCIs defined, Net1-FR1 does not appear as an option. **Net1-FR1** – Specifies the Network interface as the destination link.
Destination DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank
Specifies the destination DLCI for a frame relay interface. The DLCI must be defined and cannot be part of a PVC connection or management link. For multiplexed DLCIs, at least one EDLCI must be unconnected for the DLCI to be a valid selection. NOTES: – Primary Destination DLCI has no value if Primary Destination Link contains no value. – For the Diagnostic Feature Set, only one EDLCI per multiplexed DLCI may be used in the PVC connection. **16 – 1007** – Specifies the DLCI number.
Destination EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank
Specifies the destination Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection. *Display Conditions* – This option appears only when the Primary Destination DLCI contains a multiplexed DLCI and is not applicable when FRF.8 Encapsulation Mode is set to Translational (see Table 4-12, Network ATM Options). **0 – 62** – Specifies the EDLCI number.

Configuring the IP Path List

Select IP Path List (Static) from the Configuration Edit/Display menu to display or change the list of static path IP addresses explicitly defined in the unit.

Main Menu→ Configuration→ IP Path List (Static)

The IP Path List (Static) screen appears, showing any existing static paths. Paths discovered as SLV packets are received from other FrameSaver units are not shown. To view the entire current IP Path List, use the IP Path Connection Status screen. See *IP Path Connection Status* in Chapter 7, *Operation and Maintenance*.

▶ Procedure

To add a static path:

1. Select New. The following prompt appears:

   ```
   Enter IP Address (press ESC to abort): ___.___.___.___ FWD: No_
   ```

2. Enter the IP address of a static path and select a forwarding option of No or Yes using the spacebar.
3. Press enter. Select Save.

Table 4-17. IP Path List

IP Address
Possible Settings: **000.000.000.001 – 126.255.255.255, 128.000.000.000 – 223.255.255.255** Default Setting: Initially blank; no default.
Specifies the address of a FrameSaver or other device at the other end of a path. **000.000.000.001 – 126.255.255.255, 128.000.000.000 – 223.255.255.255** – Specifies the address of a device.
FWD
Possible Settings: **No, Yes** Default Setting: **No**
Determines whether this path list item is sent to all other addresses in the list that represent FrameSaver devices. **No** – The IP address associated with this path list item is not distributed. **Yes** – The IP address associated with this path list entry is distributed to devices in the list.

Setting Up Management and Communication

Options available from the Management and Communication menu are described in the following sections:

Configuring Node IP Information

Select Node IP to display, add, or change the information necessary to support general IP communications for the node (see Table 4-18, Node IP Options). When deploying units to remote sites, minimally configure the Node IP Address and Subnet Mask.

The Node IP set of configuration options includes a troubleshooting (TS) management link feature that service providers can use to isolate network device problems and allows unit link access via Telnet or FTP. Link troubleshooting is essentially transparent to customer operations because no alarms or SNMP traps are generated.

The TS Management Link option is initially enabled. The unit ships from the factory with a TS Management PVC already configured (e.g., 0,35). Any valid network Management PVC created on a standard DLCI can be used. An assigned security level can control access and is recommended.

When a DLCI has been defined as the troubleshooting management link, the link is identified in the status field at the bottom of the Management PVC Entry screen with the message:

`Note: This PVC has been designated as the TS Access Management Link.`

Select Node IP from the Management and Communication menu.

Main Menu→Configuration→Management and Communication→Node IP

Table 4-18. Node IP Options (1 of 2)

Node IP Address
Possible Settings: **001.000.000.000–126.255.255.255, 128.000.000.000–223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the node. Since an IP address is not bound to a particular port, it can be used for remote access via a management PVC. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the node, which can be viewed or edited. The first octet of the address cannot be decimal 0 or 127, or greater than 223. **Clear** – Fills the node IP address with zeros.
Node Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the IP address subnet mask that is needed to access the node. Since the subnet mask is not bound to a particular port, it can be used with the Node IP address for remote access via a management PVC. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the node, which can be viewed or edited. **Clear** – Fills the node subnet mask with zeros. When the node's subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the IP address class (Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000).
Default IP Destination
Possible Settings: **None, COM, Ethernet, *PVCname*** Default Setting: **None**
Specifies an IP destination to route data that does not have a specifically defined route. NOTE: If the link to the IP destination selected as the default route becomes disabled or down, the data which cannot be routed will be discarded. Make sure that the link selected is operational, and if that link goes down, the default destination is changed. CAUTION: Use care when configuring a default route to an interface that has a subnet route configured at a remote end where the NMS, router, LAN adapter, terminal server, etc. is connected. Communicating with an unknown IP address on the subnet will cause temporary routing loops, which will last 16 iterations multiplied by the retry count. **None** – No default IP network destination is specified. Unrouteable data is discarded. This is the recommended setting. **COM** – Specifies that the default IP destination is the COM port. Appears only when Port Use is set to Net Link (see Table 4-25, Communication Port Options). **Ethernet** – Specifies that the default IP destination is the Ethernet interface. Appears only when the Ethernet interface's Status is enabled. When selected, the Default Gateway Address must also be configured (see Table 4-24, Ethernet Management Options). ***PVCname*** – Specifies a name for the management PVC. Appears only when a management PVC name is defined for the node. For example, when the network is connected to a remote device located in the London office, London can be specified as the *PVCname*, which is the link between the local FrameSaver unit and the one located in London. London would appear as one of the available selections (as defined by the Name configuration option, Table 4-19, Management PVC Options).

Table 4-18. Node IP Options (2 of 2)

Management MTU Size
Possible Settings: **90–1500** Default Setting: **1500**
(Release 2.1.) Specifies the Maximum Transmission Unit (MTU) size, in bytes, to be used for management traffic. This can be used to minimize jitter introduced to the data stream. MTU is not enforced for traffic on the COM port or Ethernet port. **90–1500** – Specifies the MTU size.
TS Access Management Link
Possible Settings: **None, *PVCname*** Default Setting: [Depends on model]
Specifies a troubleshooting management link for the network service provider's use. If the setting is changed from the management PVC name to None, the **`Delete the Management PVC PVCname and the associated DLCI|Circuit Record?`** prompt appears. If you select: ■ No – The link designation is removed and the option is set to None. ■ Yes – The link designation is removed, the option is set to None, and the link and its DLCI and/or VPI,VCI are deleted. **None** – Disables or does not specify a TS Access Management Link. ***PVCname*** – Specifies the name of the TS Management Link PVC. Upon receiving five Ping packets with the same destination address within five seconds, this management link assumes the IP address of the destination address. This selection appears only when a dedicated management PVC has been defined on the network frame relay or ATM link.
TS Management Link Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the highest access level allowed when accessing the unit via a Telnet or FTP session using the TS Access Management Link. *Display Conditions* – This option does not appear if TS Access Management Link is set to None. NOTES: – Telnet and FTP sessions on this link **are not** affected by the access level set by the Session Access Level, Login Required, or FTP Login Required option settings (see Table 4-21, Telnet and FTP Session Options). – Telnet and FTP sessions on this link **are** affected by the Telnet Session, Inactivity Timeout, Disconnect Time and FTP Session option settings. **Level-1** – Allows Telnet or FTP access by network service providers with the capability to view unit information, add, change, and display configuration options, and perform device testing. This is the highest access level allowed. Use this setting when downloading files. **Level-2** – Allows Telnet or FTP access by network service providers with the capability to monitor and perform tests and display status and configuration option information; they cannot change configuration options. **Level-3** – Allows Telnet access by network service providers with the capability to monitor and display status and configuration screens only; they cannot change configuration options or run tests.

Configuring Management PVCs

To define inband management links, select Management PVCs (see Table 4-19, Management PVC Options). First, configure the DLCI interface records at the Management PVC location. See *Configuring Circuit Records for the Network Interface (9783, 9788)* on page 4-24 or *Configuring DLCI Records* on page 4-32 for additional information.

Select New or Modify to add or change Management PVCs.

- When you select New, the configuration option field is blank.
- When you select Modify, the values displayed for all fields are based on the PVC ID number that you specified.

These options do not apply when the Management PVC is designated as a TS Management Link (see *Configuring Node IP Information* on page 4-38 for additional information).

For easy movement between screens, from the Management PVCs screen, select the PVCConn function key to go directly to the PVC connection screen.

For quick removal of unused DLCIs, select the Delete function key, a Management PVC ID, and respond Yes to the prompt: **`Remove otherwise unused components associated with the deleted PVC?`**

If the Management PVC selected is defined as a TS Access Management Link, a Default IP Destination, or a trap for Initial Route Destination, a prompt appears to warn you: **`Are You Sure?`**

To view the Management PVCs screen, select Management PVCs from the Management and Communication menu.

Main Menu→ Configuration→ Management and Communication→ Management PVCs

A payload management circuit is identified by **`PM`** in the EDLCI field of the Management PVCs Options screen. If a payload management management circuit is deleted, the associated PVC remains standard, even if was a multiplexed PVC (automatically converted to standard) when the management circuit was created.

If an existing PVC with an associated payload managed management circuit is deleted, then the payload management circuit is also deleted

Table 4-19. Management PVC Options (1 of 4)

Name
Possible Settings: ***ASCII Text Entry*** Default Setting: Initially blank
For the management PVC, specify a unique name to display on screens (e.g., Tampa). ***ASCII Text Entry*** – Enter a unique name for the management PVC (maximum length 8 characters).
Payload Managed
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether the PVC is payload managed. **Enable** – The network PVC created will be monitored for the presence of IP frames containing the IP address specified in the Intf IP Address field. When such a frame is identified, it is extracted from the data stream and sent to the management stack. **Disable** – A normal management PVC is created using the specified DLCI or EDLCI.
Intf IP Address
Possible Settings: **Node-IP-Address, Special** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-IP-Address**
Specifies the Interface IP address needed to access the unit via this management PVC to provide connectivity to an external IP network through the frame relay network. **Node-IP-Address** – Defaults to the IP address contained in the Node IP Address (see Table 4-18, Node IP Options). **Special** (001.000.000.000–223.255.255.255) – Allows you to display/edit an IP address for the unit's management PVC when the IP address for this interface is different from the node's IP address.
Intf Subnet Mask
Possible Settings: **Node-Subnet-Mask, Calculate, Special** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-Subnet-Mask**
Specifies the Subnet Mask needed to access the unit via this management PVC to provide connectivity to an external IP network through the frame relay network. **Node-Subnet-Mask** – Uses the Subnet mask contained in the Node-Subnet Mask configuration option (see Table 4-18, Node IP Options). **Calculate** – Calculates the subnet mask created by the IP protocol based on the class of the IP address (Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000). Cannot be displayed or edited. **Special** (000.000.000.000–255.255.255.255) – Allows you to edit/display the subnet mask for the management PVC when the subnet mask is different for this interface.

Table 4-19. Management PVC Options (2 of 4)

Set DE
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether frames (packets) sent on a management PVC have the Discard Eligible (DE) bit set. During network congestion, this bit prioritizes which frames to discard first, giving management traffic a lower priority than customer data. *Display Conditions* – This option does not appear if Primary Link is set to Net1-ATM. **Enable** – Sets the DE bit to one on all frames sent on the management PVC. **Disable** – Sets the DE bit to zero on all frames sent on the management PVC. This is the recommended setting, particularly for NSPs providing a managed network service.
Primary Link
Possible Settings: **Net1-FR1, Port-1, Rtr-S0, Net1-ATM, Clear** Default Setting: Initially blank
Specifies the frame relay interface to use for this management PVC. The interface selected must have at least one DLCI (or DLCI with EDLCI) defined, which is not part of a PVC connection or already assigned as a management PVC. *Display Conditions* – The Port-1 setting does not appear if the PVC is Payload Managed or IP Enabled. **Net1-FR1** – Specifies that the network frame relay link interface be used in the connection. **Port-1** – For the FrameSaver CSU/DSU, specifies that the user data port frame relay link be used in the connection. **Rtr-S0** – For the FrameSaver router, specifies that the router's virtual Serial port 0 interface (S0) be used in the connection. **Net1-ATM** – Specifies that the network ATM link be used in the connection. **Clear** – Clears the link field and suppresses the EDLCI field for a multiplexed DLCI.
Primary DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank
Specifies the DLCI number used for the management PVC after the frame relay interface is selected. The DLCI must be defined for the link (i.e., have a DLCI record) and must not be part of a PVC connection or already assigned as a management PVC. For multiplexed DLCIs, at least one EDLCI must be unconfigured for the DLCI. NOTES: – DLCI cannot be entered if the Link field is blank. – Clearing the Link also clears the DLCI. **16 – 1007** – Specifies the DLCI number.

Table 4-19. Management PVC Options (3 of 4)

Primary EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank
Specifies the EDLCI number used by a management PVC when a multiplexed DLCI is selected. EDLCIs identify unique individual connections within multiplexed DLCIs. Use 0 to identify the primary EDLCI. Use 1 – 62 to identify secondary EDLCIs. Use the primary EDLCI for customer data, which has a higher utilization rate than management data, with slightly less line overhead. *Display Conditions* – This option does not appear if the DLCI field does not reference a multiplexed DLCI, if Network 1 FRF.8 Encapsulation Mode is set to Translational (see Table 4-12, Network ATM Options), or if Payload Managed is enabled. NOTE: Clearing the DLCI or changing to a standard DLCI suppresses the EDLCI field. **0 – 62** – Specifies the EDLCI number.
Primary VPI,VCI Number
Possible Settings: – VPI: **0 – 15** – VCI: **32 – 255** Default Setting: – *If Payload Managed is disabled:* Blank. – *If Payload Managed is enabled:* Lowest VPI, VCI number of a non-management circuit found in the network.
This option represents the VPI,VCI of the primary link. If Payload Managed is enabled, this option specifies the VPI,VCI for the payload managed PVC. *Display Conditions* – This option appears for an ATM link. **0 – 15** – Specifies the VPI. **32 – 255** – Specifies the VCI.

Table 4-19. Management PVC Options (4 of 4)

Primary Link RIP
Possible Settings: **None, Proprietary, Proprietary In, Standard_out** Default Setting: – *For multiplexed DLCIs:* **Proprietary** – *For nonmultiplexed DLCIs:* **Standard_out**
Specifies which Routing Information Protocol (RIP) is used to enable routing of management between FrameSaver units and attached equipment. *Display Conditions* – This option does not appear if Payload Managed is enabled. **None** – Does not use a routing protocol. **Proprietary** – Uses a proprietary variant of RIP Version1 to communicate routing information between FrameSaver units. A FrameSaver unit must be on the other end of the link. This is the factory default for management PVCs configured on multiplexed DLCIs (see Table 4-11, Circuit Records Options). **Proprietary In** – (Release 2.1.) The device distributes only the following local routes to the far end: – Trap manager routes – Default route – Routes to this device – MIB-injected routes – RIP split horizon with poison reversed routes **Standard_out** – The device sends standard RIP messages to communicate routing information only about FrameSaver units in the network. This is the factory default for management PVCs configured on standard DLCIs. NOTE: The router must be configured to receive RIP on the FrameSaver management interface port.
Encapsulation
Possible Settings: **Routed** Default Setting: **Routed**
This read-only field specifies that the IP encapsulation used is RFC 1490/RFC 2427 routed Network Level Protocol IDentifier (NLPID) encapsulation, and not SubNetwork Access Protocol (SNAP) encapsulation. *Display Conditions* – This option appears only if the PVC is Payload Managed or IP Enabled. **Routed** – IP encapsulation is routed NLPID.

Configuring General SNMP Management

Using SNMP protocols, the FrameSaver unit can be managed as an NMS SNMP agent. You must have Level-1 access to display or configure these options.

Select General SNMP Management to add, change, or delete configuration information (see Table 4-20, General SNMP Management Options).

Main Menu→ Configuration→ Management and Communication→ General SNMP Management

Table 4-20. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the FrameSaver unit can be managed as an SNMP agent by an SNMP-compatible NMS. **Enable** – Can be managed as an SNMP agent. **Disable** – Cannot be managed as an SNMP agent. The FrameSaver unit will not respond to SNMP messages or send SNMP traps.
Community Name 1
Possible Settings: ***ASCII text entry*, Clear** Default Setting: **Public**
Specifies the first of two names that are allowed to access the objects in the FrameSaver unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access a MIB object. ***ASCII text entry*** – Add or change Community Name 1 (maximum 255 characters). **Clear** – Clears Community Name 1 field.
Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read/Write**
Specifies the type of MIB access allowed. With this access type, SNMP managers can externally access MIB objects, using Community Name 1. **Read** – Allows read-only access (SNMP **Get** command). This includes all MIB RFCs objects specified as either read-only or read/write. **Read/Write** – Allows read and write access (SNMP **Get** and **Set** commands).

Table 4-20. General SNMP Management Options (2 of 2)

Community Name 2
Possible Settings: ***ASCII text entry*****, Clear** Default Setting: **Clear**
Specifies the second of two names that are allowed to access the objects in the FrameSaver unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access a MIB object. ***ASCII text entry*** – Add or change Community Name 2 (maximum 255 characters). **Clear** – Clears Community Name 2 field.
Name 2 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Specifies the type of MIB object access allowed for external SNMP managers accessing MIB objects using Community Name 2. **Read** – Allows read-only access (SNMP **Get** command). This includes all MIB RFCs specified as either read-only or read/write. **Read/Write** – Allows read and write access (SNMP **Get** and **Set** commands).

Configuring Telnet and/or FTP Sessions

Telnet and FTP options control interconnected IP network and security access applicable to the session. Two Telnet sessions can be active simultaneously on the user interface and one Telnet session can be active on the router interface (see Table 4-21, Telnet and FTP Session Options).

Main Menu→ Configuration→ Management and Communication→ Telnet and FTP Sessions

When a TS Management Link has been configured and activated, the following options have no effect upon the PVC:

- Telnet Login Required
- Session Access Level
- FTP Login Required

Table 4-21. Telnet and FTP Session Options (1 of 3)

Telnet Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the FrameSaver unit will respond to a session request from an interconnected IP network Telnet client. This option affects the TS Access Management Link. **Enable** – Allows Telnet sessions between the FrameSaver unit and Telnet client. **Disable** – Does not allow any Telnet session.
Telnet Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether a user ID and password are required to access the menu-driven user interface via a Telnet session. If required, use the same login used for a menu-driven user interface session. This option does not affect the TS Access Management Link. **Enable** – Requires a login to access a Telnet session. **Disable** – Does not require a login.

Table 4-21. Telnet and FTP Session Options (2 of 3)

Session Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the highest security level allowed when accessing the menu-driven user interface via a Telnet session. If a login is required for the session, the effective access level is also determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. This option does not affect the TS Access Management Link. NOTE: The effective access level is always the lowest level assigned to either the session or the user. For example, if the assigned Session Access Level is Level-2, but the User Access Level is Level-3, then only Level-3 access is allowed for the session. **Level-1** – Allows Telnet access to view system information, change configuration options, and run tests. This is the highest access level allowed. CAUTION: Before changing the session access level to Level-2 or 3, make sure that the COM port's Port Access Level is set to Level-1 and that at least one Login ID is set to Level-1. If levels are not set properly, access will be lost until the unit is reset to factory defaults. A reset is required if the Communication Port's Port Use option is set to Net Link (see Table 4-25, Communication Port Options). **Level-2** – Allows Telnet access to view system information and run tests only; cannot change configuration options. **Level-3** – Allows Telnet access to view system information only; cannot change configuration options or run tests.
Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a Telnet session is disconnected after a specified period of keyboard inactivity. **Enable** – Terminates the session after the Disconnect Time expires. **Disable** – Does not terminate Telnet session during inactivity.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Sets the amount of keyboard inactive time allowed before a user session is disconnected. *Display Conditions* – This option does not appear when Inactivity Timeout is disabled. **1 – 60** – Up to an hour can be set in minutes as the disconnect time.
FTP Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the system responds as a server when an FTP client on an interconnected IP network requests an FTP session. This option must be enabled when downloading files. This option affects the TS Access Management Link. **Enable** – Allows an FTP session between the system and an FTP client. **Disable** – Does not allow FTP sessions.

Table 4-21. Telnet and FTP Session Options (3 of 3)

FTP Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies if a login ID and password are required for an FTP session. If required, the login used is the same login used for a menu-driven user interface session. This option does not affect the TS Access Management Link. **Enable** – User is prompted for a login ID and password. **Disable** – No login is required for an FTP session.
FTP Max Transfer Rate (Kbps)
Possible Settings: – *9720:* **1 – 144** – *9783:* **1 – 2320** – *9788:* **1 – 2312** Default Setting: – *9720:* **144** – *9783:* **2320** – *9788:* **2312**
Sets the maximum transmit and receive rate of a file transfer via management PVCs. This option allows new firmware and configuration files to be downloaded in the background using selected bandwidth without interfering with normal operation. Files can be downloaded quickly using the default settings or downloaded at a slower rate over an extended period of time by selecting a slower speed. Based on TCP flow control, the system FTP server throttles bandwidth to match this setting. **1 – *maximum*** – Sets the line speed from 1 Kbps to the maximum management speed.

Configuring SNMP NMS Security

Select SNMP NMS Security from the Management and Communication menu to configure trap managers (see Table 4-22, SNMP NMS Security Options).

Main Menu→ Configuration→ Management and Communication→ SNMP NMS Security

A table displays with the network management systems (with their respective IP addresses) allowed access to the SNMP FrameSaver unit.

Table 4-22. SNMP NMS Security Options (1 of 2)

NMS IP Validation
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether security checks are performed on the IP address of SNMP management systems attempting to access the node. Only allows access when the sending manager's IP address is listed on the SNMP NMS Security Options screen. **Enable** – Performs security checks. **Disable** – Does not perform security checks.
Number of Managers
Possible Settings: **1 – 10** Default Setting: **1**
Specifies the number of SNMP management systems that are authorized to send SNMP messages to the FrameSaver unit. An IP address must be configured for each management system allowed to send messages. Configure IP addresses in the NMS *n* IP Address configuration option. **1 – 10** – Specifies the number of authorized SNMP managers.
NMS *n* IP Address
Possible Settings: **001.000.000.000–126.255.255.255, 128.000.000.000–223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Provides the IP address of an SNMP manager that is authorized to send SNMP messages to the unit. If an SNMP message is received from an unauthorized NMS and its IP address cannot be matched here, access is denied and an authenticationFailure trap is generated. If a match is found, the type of access (read-only or read/write) is determined by the corresponding Access Type. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **001.000.000.000 – 223.255.255.255** – Adds or changes the NMS IP address. The first octet of the address cannot be decimal 0 or 127, or greater than 223. **Clear** – Fills the NMS IP address with zeros.

Table 4-22. SNMP NMS Security Options (2 of 2)

Access Type
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Specifies the type of access allowed for an authorized NMS when IP address validation is performed. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **Read** – Allows read-only MIB objects access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows MIB objects read and write access (SNMP Get and Set commands). However, access for all read-only objects is specified as read-only.

Configuring SNMP Traps

Select SNMP Traps from the Management and Communication menu to configure SNMP traps when a trap is generated (see Table 4-23, SNMP Traps Options).

Main Menu→ Configuration→ Management and Communication→ SNMP Traps

See Appendix B, *SNMP MIBs, Traps, and RMON Alarm Defaults*, for trap format standards and special trap features, including RMON-specific traps, and the default settings that will generate RMON-specific SNMP traps.

Table 4-23. SNMP Traps Options (1 of 4)

SNMP Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the FrameSaver unit sends trap messages to the currently configured SNMP trap manager(s). **Enable** – Sends trap messages. **Disable** – Does not send trap messages.
Number of Trap Managers
Possible Settings: **1 – 6** Default Setting: **1**
Specifies the number of SNMP management systems that will receive SNMP trap messages from the FrameSaver unit. For each trap manager to receive trap messages, an NMS IP Address must be configured in the NMS *n* IP Address configuration option (next option). **1 – 6** – Specifies the number of trap managers.
NMS *n* IP Address
Possible Settings: **001.000.000.000–126.255.255.255, 128.000.000.000–223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address that identifies the SNMP manager(s) to receive SNMP traps. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **001.000.000.000 – 223.255.255.255** – Adds to or changes the IP address for the trap manager. The first octet of the address cannot be decimal 0 or 127, or greater than 223. **Clear** – Fills the NMS IP address with zeros.

Table 4-23. SNMP Traps Options (2 of 4)

Initial Route Destination
Possible Settings: **AutoRoute, Ethernet, COM, *PVCname*** Default Setting: **AutoRoute**
Specifies the initial route used to reach the specified Trap Manager. When proprietary RIP is active, only one unit in the network needs to specify an interface or management link as the initial destination. All other units can use the default setting. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **AutoRoute** – Uses proprietary RIP from other FrameSaver devices to learn the route for sending traps to the specified Trap Manager, or the Default IP Destination when no route is available in the routing table (see Table 4-18, Node IP Options). **Ethernet** – Uses the Ethernet interface. Appears only when Interface Status for the interface is enabled (see Table 4-24, Ethernet Management Options). **COM** – Uses the COM port. Only available when Port Use is set to Net Link (see Table 4-25, Communication Port Options). ***PVCname*** – Uses the defined management *linkname* (the name given the Management PVC). Appears only when at least one Management PVC is defined for the node.
General Traps
Possible Settings: **Disable, Warm, AuthFail, Both** Default Setting: **Both**
Determines whether SNMP trap messages for warmStart and/or authenticationFailure events are sent to the currently configured trap manager(s). **Disable** – Does not send trap messages for these events. **Warm** – Sends trap messages for warmStart events only. **AuthFail** – Sends trap messages for authenticationFailure events only. **Both** – Sends trap messages for both warmStart and authenticationFailure events.
Enterprise Specific Traps
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether trap messages for enterpriseSpecific events are sent to the currently configured trap manager(s). **Enable** – Sends trap messages for enterpriseSpecific events. **Disable** – Does not send trap messages for enterpriseSpecific events.

Table 4-23. SNMP Traps Options (3 of 4)

Link Traps
Possible Settings: **Disable, Up, Down, Both** Default Setting: **Both**
Determines whether SNMP linkDown or linkUp traps are sent to the currently configured trap manager(s). A linkDown trap indicates that the unit recognizes a failure in one of the interfaces. A linkUp trap indicates that the unit recognizes that one of its interfaces is active. Use the Link Traps Interface and the DLCI Traps on Interface configuration options to specify which interface will monitor linkUp and linkDown traps messages. **Disable** – Does not send linkDown or linkUp trap messages. **Up** – Sends trap messages for linkUp events only. **Down** – Sends trap messages for linkDown events only. **Both** – Sends trap messages for linkUp and linkDown events.
Link Traps Interfaces
Possible Settings: **Network, Ports, All** Default Setting: **All**
Specifies which interfaces will generate linkUp, linkDown, and enterpriseSpecific trap messages. These traps are not supported on the COM port. **Network** – Generates trap messages on the network interface only. **Ports** – Generates trap messages for linkUp, linkDown, and enterpriseSpecific events on the user data port only. **All** – Generates trap messages for linkUp and enterpriseSpecific events on all interfaces, except for the COM port, that are applicable to the FrameSaver model.
DLCI Traps on Interfaces – Interface Selection Field
Possible Settings: **Network, Ports, All, None** Default Setting: **All**
Specifies which interfaces will generate linkUp and linkDown trap messages for individual DLCIs. These traps are only supported on the frame relay interfaces. **Network** – Generates trap messages on DLCIs for the network interface only. **Ports** – Generates trap messages for DLCIs on a user data port only. **All** – Generates trap messages on all frame relay interfaces. **None** – No DLCI trap messages are generated.
DLCI Traps on Interfaces – Filter Selection Field
Possible Settings: **Normal, Filter** Default Setting: **Normal**
Controls whether the traps on the interfaces specified in the DLCI Traps on Interfaces configuration option are sent regardless of their cause. **Normal** – Generates trap messages specified by DLCI Traps on Interfaces regardless of cause. **Filter** – Prevents traps from being generated for the interfaces specified by DLCI Traps on Interfaces if their cause is the loss of the interface connection or LMI. This includes Latency and IP SLV Availability traps.

Table 4-23. SNMP Traps Options (4 of 4)

RMON Traps
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether remote monitoring traps are sent to the currently configured trap manager(s). RMON traps are typically sent when a selected variable in the RMON1 Alarms and Events Groups determines that the configured threshold is exceeded. *Display Conditions* – This option appears only for units with the SLV Feature Set 2. **Enable** – Sends RMON trap messages when set thresholds are exceeded. **Disable** – Does not send RMON trap messages.
Latency Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether a Latency Threshold Alarm causes the generation of a Latency Threshold Exceeded Trap. **Enable** – Sends trap messages for Latency Threshold Alarm events. **Disable** – Does not send trap messages for Latency Threshold Alarm events.
IP SLV Availability Traps
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a Path Unavailability condition causes the generation of an IP SLV Availability Trap. **Enable** – Sends trap messages for Path Unavailability events. **Disable** – Does not send trap messages for Path Unavailability events.

Configuring Ethernet Management

Select Ethernet Management from the Management and Communication menu to configure management traffic options for the Ethernet interface (see Table 4-24, Ethernet Management Options).

Main Menu→ Configuration→ Management and Communication→ Ethernet Management

– or –

Main Menu→ Easy Install→ Ethernet Management Options Screen

NOTE:

If accessing Ethernet Management options from the Easy Install screen, Save your changes. Press the Esc key to return to the Easy Install screen.

Table 4-24. Ethernet Management Options (1 of 2)

Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the Ethernet interface is being used for management traffic. ■ If Status is changed from Disable to Enable, the prompt **`Would you like to set the Node's Default IP Destination to Ethernet?`** appears. – If Yes is selected, the Ethernet interface is enabled and the node's Default IP Destination is set to Ethernet. – If No, Esc, or Ctrl-a are selected, the Ethernet interface is enabled, but the node's Default IP Destination is not changed. ■ If Status is changed from Enable to Disable, the prompt **`Would you like to clear the Ethernet Management Options?`** appears. – If Yes is selected, the Ethernet management link is disabled and all Ethernet Management options are reset to their default values. – If No, Esc, or Ctrl-a are selected, the Ethernet management link is disabled. **Enable** – The Ethernet interface is active for management traffic and can only receive Version 2 or IEEE 802.3 MAC frames and transmit Version 2 MAC frames. **Disable** – The Ethernet interface is not available for management traffic and: ■ No alarms or traps associated with the Ethernet management interface are generated. ■ All port uses that refer to the Ethernet interface, like Default IP Destination and Initial Route Destinations, are reset to their default settings (see Table 4-18, Node IP Options, and Table 4-23, SNMP Traps Options).

Table 4-24. Ethernet Management Options (2 of 2)

IP Address
Possible Settings: **001.000.000.000–126.255.255.255, 128.000.000.000–223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed for the Ethernet management link. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the Ethernet management link so it can be viewed or edited. The first octet of the address cannot be decimal 0 or 127, or greater than 223. **Clear** – Fills the IP address with zeros.
Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the IP address's Subnet Mask for the Ethernet management link. **000.000.000.000 – 255.255.255.255** – Sets the Ethernet management link's subnet mask. The range for each byte is 000 to 255. When set to 000.000.000.000, the IP protocol creates a default Subnet Mask based on the IP address's class (Class A; 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000). **Clear** – Fills Subnet Mask with zeros.
Default Gateway Address
Possible Settings: **001.000.000.000–126.255.255.255, 128.000.000.000–223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the IP address for the Ethernet management link's default gateway, used for packets sent out the Ethernet management link that do not have a route. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the Ethernet management link so the address can be edited. The first octet of the address cannot be decimal 0 or 127, or greater than 223. **Clear** – Fills the default gateway's IP address with zeros. All packets without a route are discarded.
Proxy ARP
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the Ethernet interface can be used to supply the FrameSaver MAC address at the opposite end of a PVC by using ARP. This technique is used for communication between devices on the same network, but on the different subnets. Using this technique, the Default Gateway Address is provided when there is an ARP request. When data is sent to the gateway, the gateway forwards the data to the appropriate device. The gateway acts as an agent destination device. **Enable** – Proxy ARP is enabled on the Ethernet interface. **Disable** – The Ethernet interface cannot be used to acquire the FrameSaver IP address at the opposite end of the PVC.

Configuring the Communication Port

Select Communication Port from the Management and Communication menu to display or change the communication port configuration options (see Table 4-25, Communication Port Options).

Main Menu→ Configuration→ Management and Communication→ Communication Port

Table 4-25. Communication Port Options (1 of 4)

Port Use
Possible Settings: **Terminal, Net Link** Default Setting: **Terminal**
Assigns a specific use to the COM port. It can be configured as a communications link that provides connectivity to an IP network (to support SNMP managers and Telnet sessions), or it can be configured as a an asynchronous terminal interface. NOTE: If Default IP Destination is set to COM (see Table 4-18, Node IP Options) and Port Use is changed to Terminal, the Default IP Destination option is forced to None and Initial Route Destination (see Table 4-23, SNMP Traps Options) is set to AutoRoute. **Terminal** – The COM port is used for an asynchronous terminal connection. **Net Link** – The COM port is used as the network communications link to an IP network or IP device.
Data Rate (Kbps)
Possible Settings: **9.6, 14.4, 19.2, 28.8, 38.4, 57.6, 115.2** Default Setting: **19.2**
Specifies COM port rate in kilobits per second. **9.6 – 115.2** – Sets the COM port speed in Kbps.
Character Length
Possible Settings: **7, 8** Default Setting: **8**
Specifies the number of bits needed to represent one character. **7** – Sets the character length to seven bits. Not available if Port Use is set to Net Link. **8** – Sets the character length to eight bits. Use this setting if the COM port is used as the network communication link (Port Use set to Net Link).
Parity
Possible Settings: **None, Even, Odd** Default Setting: **None**
Provides a method of checking the accuracy of binary numbers for the COM port. A parity bit is added to the data to make the “1” bits of each character add up to either an odd or even number. Each transmitted data character is approved as error-free if the “1” bits add up to an odd or even number as specified by this option. **None** – Provides no parity. **Even** – Makes the sum of all 1 bits and the corresponding parity bit even. **Odd** – Makes the sum of all 1 bits and the corresponding parity bit odd.

Table 4-25. Communication Port Options (2 of 4)

Stop Bits
Possible Settings: **1, 2** Default Setting: **1**
Determines the number of COM port stop bits. **1** – Provides one stop bit. **2** – Provides two stop bits.
Ignore Control Leads
Possible Settings: **Disable, DTR** Default Setting: **Disable**
Specifies whether DTR is used. *Display Conditions* – This option does not apply to the router. **Disable** – Treats control leads as standard operation. **DTR** – Ignores DTR. This may be necessary when connecting to some PAD devices.
Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether a user ID and password login are required to log on to the async terminal connected to the COM port. *Display Conditions* – This option appears only when Port Use is set to Terminal. **Enable** – Requires a login to access the menu-driven user interface. **Disable** – Does not requires a login.
Port Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies level of user access privilege for an async terminal connected to the COM port. If a login is required for the COM port, the effective access level is determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. *Display Conditions* – This option appears only when Port Use is set to Terminal. NOTE: The effective access level is always the lowest one assigned to either the port or the user. For example, if the Port Access Level assigned is Level-2, but the User Access Level is Level-3, then only Level-3 access is permitted for the port. **Level-1** – Allows full access and control of the device, including monitoring, diagnostics, and configuration. The user can add, change, and display configuration options and perform device testing. CAUTION: Before changing the communication port's access level to Level-2 or Level-3, make sure that the Telnet Session Access Level is set to Level-1 and at least one Login ID is set to Level-1. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. **Level-2** – User limited to display status, run tests, and view configuration option settings. **Level-3** – User limited to display status and view configuration screens only.

Table 4-25. Communication Port Options (3 of 4)

Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a user session is disconnected after a specified time of inactivity (no keyboard activity). *Display Conditions* – This option appears only when Port Use is set to Terminal. **Enable** – Disconnects user session after the specified time of inactivity (next option). **Disable** – Does not timeout and disconnect user session.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Sets the number of minutes of inactivity that can elapse before the session is ended. *Display Conditions* – This option appears only when Port Use is set to Terminal. **1 – 60** – Sets the time from 1 to 60 minutes.
IP Address
Possible Settings: **001.000.000.000–126.255.255.255, 128.000.000.000–223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies a unique IP address for accessing the unit via the COM port. This option is only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). *Display Conditions* – This option appears only when Port Use is set to Net Link. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the COM port, which you can view or edit. The first octet of the address cannot be decimal 0 or 127, or greater than 223. **Clear** – Clears the IP address for the COM port and fills the address with zeros. When the IP Address is all zeros, the COM port uses the Node IP Address if one has been configured.
Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the unit. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). *Display Conditions* – This option appears only when Port Use is set to Net Link. **000.000.000.000 – 255.255.255.255** – Shows COM port subnet mask, which you can view or edit. **Clear** – Clears the subnet mask for the COM port and fills the address with zeros. When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the IP address class: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.

Table 4-25. Communication Port Options (4 of 4)

RIP
Possible Settings: **None, Standard_out** Default Setting: **None**
Specifies which Routing Information Protocol (RIP) is used to enable routing of management data between devices. *Display Conditions* – This option appears only when Port Use is set to Net Link. **None** – No routing is used. **Standard_out** – The device will send standard RIP messages to communicate routing information about other FrameSaver units in the network. Standard RIP messages received on this link are ignored. NOTE: The router must be configured to receive RIP on the port connected to the COM port, configured as the management interface. To create this management interface, make sure that Node or COM Port IP information has been set up (refer to *Configuring Node IP Information* on page 4-38).

Configuring the COM Port to Support an External Modem

Select External Modem (Com Port) to display or change the configuration options that control COM port external device call processing (see Table 4-26, External Modem (COM Port) Options).

Main Menu→ Configuration→ Management and Communication→ External Modem (Com Port)

NOTE:

A standard EIA-232 crossover cable is required when connecting an external modem to the FrameSaver unit's COM port. See *DB25-to-DB25 Crossover Cable* or *DB9-to-DB25 Crossover Cable* in Appendix E, *Connectors, Cables, and Pin Assignments*, for cable pin assignments.

Table 4-26. External Modem (COM Port) Options

External Modem Commands
Possible Settings: **Disable, AT** Default Setting: **Disable**
Specifies the type of commands to be sent over the COM port. CAUTION: Do *not* use this setting when an async terminal is connected to the COM port (see Table 4-25, Communication Port Options). **Disable** – Commands will not be sent over the COM port. **AT** – Standard Attention (AT) Commands are sent over the COM port to control the external device. All AT command strings will end with a carriage return (hex 0x0D) and a line feed (hex 0x0A).
Dial-In Access
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Controls whether external devices can dial-in to the FrameSaver unit through the COM port (based on the Port Use option setting). *Display Conditions* – This option does not appear if External Modem Commands is disabled. **Enable** – Answers incoming calls and establishes connection to the remote terminal or IP network. **Disable** – Does not answer incoming calls.

Configuring the FrameSaver DSL Router

5

This chapter includes the following:

FrameSaver DSL Router Overview

The FrameSaver DSL Router supports locally attached hosts or subnets and various customer premises distribution networks that contain IP forwarding devices or routers. The DSL router is shipped as an 802.1d bridge, and it can be configured to simultaneously support IP routing and bridging of all non-IP protocols. The router maintains two routing tables to keep customer data and management data separate.

The router supports Internet Protocol (IP), specified in RFC 791, and Internet Control Message Protocol (ICMP), as specified in RFCs 792 and 950 (with exceptions). It acts as a router or gateway as defined in RFC 791.

The router has two interfaces:

- **DSL Network Interface**

  Frame relay packets converted to ATM are transported over the DSL line using this interface.

- **Ethernet**

  This is a 10/100BaseT interface that automatically negotiates the rate. If all attached Ethernet devices support 100BaseT, the router defaults to 100BaseT. Otherwise, the router operates at 10BaseT. The interface has a unique MAC address.

  — In router mode, the router accepts on the Ethernet interface only those frames with its own MAC address or a broadcast or multicast MAC address.

  — In bridge mode, the router accepts all frames and forwards only ones for which the destination MAC address does not match an entry in the bridge table. This is the default setting.

NOTES:

— The configuration examples included in this chapter cover some common configurations, providing only a few of the possible scenarios.

— IP addresses used in the examples are for illustrative purposes only; they are not intended to be used when configuring your local network.

— Command syntax will vary based on your network setup.

— Configuration commands require an access level of Administrator-Config, and changes need to be saved when being configured to take effect.

For additional information, refer to:

- Appendix B, *SNMP MIBs, Traps, and RMON Alarm Defaults*, for details on the supported MIBs and RFCs.
- Appendix C, *Router CLI Commands, Codes, and Designations,* for specific commands and complete syntax.
- Appendix D, *Router Command Line Summaries and Shortcuts*, for specific command default settings and abbreviated command line syntax.

IP Routing

The router uses destination-based routing. IP routing tables are maintained for both the customer data and management data domains to specify how IP datagrams are forwarded. The router can support up to 32 entries in the data IP routing table, and up to 300 entries for the management IP routing table. When an IP address and subnet mask are assigned to an interface, an entry is automatically created in the IP routing table.

Address Resolution Protocol

The router supports Address Resolution Protocol (ARP), as specified in RFC 826. The router provides for 256 ARP table entries. The timeout for completed and uncompleted ARP table entries is configurable.

The Command Line Interface provides the ability to:

- Create up to 64 static ARP table entries to be retained across power cycles.
- Display the ARP table.
- Delete ARP table entries.
- Display and delete automatically added static ARP table entries by the DHCP server and relay functions. Refer to *Dynamic Host Configuration Protocol Server* on page 5-11.

Proxy ARP

The router supports Proxy ARP. Proxy ARP responses are based on the contents of the IP routing table for management traffic. The IP routing table for management traffic must have an entry for every host that is reachable on the Ethernet interface, including hosts for which the router will not forward packets because of IP filters. For additional information on filtering, refer to *IP Filtering* on page 5-16.

If an ARP request is received on one interface for an IP address that is reachable on the other interface, the router will respond with its own MAC address. Proxy ARP is enabled via the user interface. Refer to *Configuring Ethernet Management* in Chapter 4, *Configuration Options.*

NOTES:

— When Basic NAT is enabled, the DSL interface must have Proxy ARP enabled if the interface address is part of the Basic NAT global IP network address.

— Proxy ARP and NAPT cannot be enabled at the same time.

Interface Configuration

The following examples require that IP addresses have been assigned to the Ethernet and Serial interfaces, and that a passthrough PVC connection exists to Rtr-S0. Optionally you might also disable bridging.

In the following example, the Serial 0 sub-interface is shown as x. The valid range is 0–4,294,967,295.

▶ Procedure

To set up the router's interfaces:

1. If a Net1-FR1 DLCI does not exist:
   - — Create one using the Network Circuit Records screen, then select CreatePVC.
   - — When the **`Create PVC using DLCI Number?`** prompt appears, select a DLCI and press Enter.
   - — When the **`Create Pass-Thru PVC Connection to:?`** prompt appears, enter **Rtr-S0**.
   - — Save the configuration.
2. From the Main Menu screen, press Ctrl-a then Shift-r to access the router's Command Line Interface. Set the IP addresses of the interfaces.

   The following example commands:
   - — Set the Ethernet interface address to 10.1.3.1
   - — Set the Serial 0.*x* interface to 172.20.95.2
   - — Disable bridging for both interfaces
   - — Specify that messages for all IP addresses should be routed to the upstream router at 172.20.95.1

```
en
config t
int e 0
ip address 10.1.3.1 255.255.255.0
no bridge-group 1
int se 0.x
ip address 172.20.95.2 255.255.255.0
no bridge group 1
exit
ip route 0.0.0.0 0.0.0.0 172.20.95.1
save
exit
```

Network Address Translation

Network Address Translation (NAT) is used when a private network's internal IP addresses cannot be used outside the private network. IP addresses may be restricted for privacy reasons, or they may not be valid public IP addresses.

The router provides NAT as described in RFC 1631, The IP Network Address Translator (NAT). NAT allows hosts in a private (local) network to transparently access the external (public or global) network by using a block of public addresses. Static mapping enables access to selected local hosts from the outside using these external IP addresses.

Traditional NAT and Network Address Port Translation (NAPT) are supported. When both NAT and NAPT are enabled, one-to-one NAT mapping is performed by translating a range of assigned public IP addresses to a similar-sized pool of private addresses, followed by many-to-one NAPT bindings. Up to 254 IP addresses can be allocated for NAT usage.

IP Options Processing

The NAT and NAPT functions handle and process the IP datagrams with options set as described below. No command is available to set IP options.

The router does not process (and drops) any IP datagrams with the following IP options:

- Loose source and record route (type 131)
- Strict source and record route (type 133)
- Security (type 130)
- Stream ID (type 136)

The router does process IP datagrams with the following IP options, but does not provide its IP address or timestamp information in the response message:

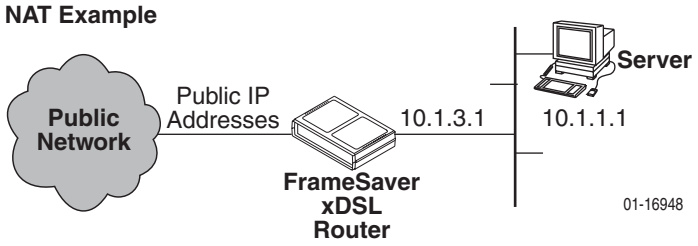
- Record route (type 7)
- Timestamp (type 68)

Applications Supported by NAT

The router supports the following applications and protocols:

- FTP
- HTTP
- Ping
- RealPlayer
- Telnet
- TFTP

NAT Configuration Example



In this NAT example:

- NAT is used for one-to-one mapping of addresses.
- The Ethernet interface is in the private address space and the DSL interface is in public address space. With NAT enabled, a single global PVC is used to access the public network.
- When using NAT, the DSL interface must be numbered because the Ethernet interface is configured within the private address space.
- The next hop router (default gateway) for the clients is the Ethernet IP address of the router, 10.1.3.1.
- There are four private IP addresses configured on the Ethernet side of the router with NAT static mappings to four public IP addresses.

NAT Mapping Public IP Addresses	Private IP Addresses
192.128.22.28	10.1.3.2
192.128.22.29	10.1.3.3
192.128.22.30	10.1.3.4
192.128.22.31	10.1.3.5

▶ Procedure

To set up NAT:

1. From the Main Menu screen, press Ctrl-a then Shift-r to access the router's Command Line Interface. Enter the following commands:

```
en
config t
ip nat inside source static 10.1.3.2 192.128.22.28
ip nat inside source static 10.1.3.3 192.128.22.29
ip nat inside source static 10.1.3.4 192.128.22.30
ip nat inside source static 10.1.3.5 192.128.22.31
```

2. Enable NAT on interfaces with the following commands (where *x* is the number configured for the sub-interface):

```
interface ethernet 0
ip nat inside
interface serial 0.x
ip nat outside
```

3. Save the configuration and exit the CLI:

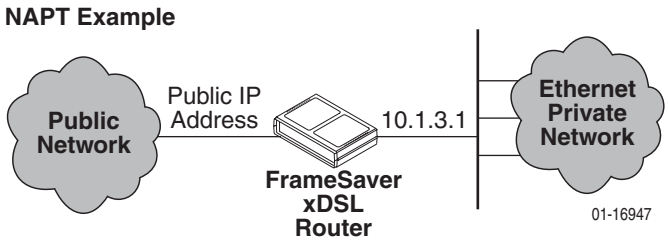
```
save
exit
```

Network Address Port Translation

Network Address Port Translation (NAPT) allows multiple clients in a local network to simultaneously access remote networks using a single IP address. This benefits telecommuters and SOHO (Small Office/Home Office) users that have multiple clients in an office running TCP/UDP applications. NAPT is sometimes referred to as PAT (Port Address Translation).

NAPT provides a many-to-one mapping and uses one public address to interface numerous private users to an external network. All hosts on the global side view all hosts on the local side as one Internet host. The local hosts continue to use their corporate or private addresses. When the hosts are communicating with each other, the translation is based on the IP address and the IP port numbers used by TCP/IP applications. Only TCP/UDP applications can access the public network.

NAPT Configuration Example



In this NAPT example the router is configured for NAPT using:

- A single public IP address. Multiple public addresses can be used.
- A public network. NAPT can also be used between private networks.
- An access list. A pool can also be used, instead or in addition.

NAPT Mapping Public IP Address	Private IP Addresses
172.20.95.2:zzzz	10.1.3.2:zzzz
172.20.95.2:yyyy	10.1.3.3:yyyy
172.20.95.2:xxxx	10.1.3.4:xxxx

▶ Procedure

To set up NAPT:

1. From the Main Menu screen, press Ctrl-a then Shift-r to access the router's Command Line Interface.
2. Set up an access list. The following command specifies a list that includes addresses 10.1.3.1 through 10.1.3.254:

   ```
   access-list 1 permit 10.1.3.0 0.0.0.255
   ```

3. Enable NAPT. The following command specifies that inside address translation is performed on the addresses in Access List 1, and the outside address is the address of the Serial interface 0, sub-interface *x*:

   ```
   ip nat inside source list 1 interface se 0.x overload
   ```

4. Specify which interface uses inside (private) and which uses outside (public) IP addresses:

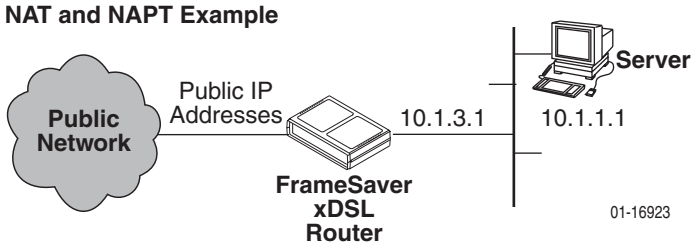
   ```
   int ethernet 0
   ip nat inside
   int serial 0.x
   ip nat outside
   ```

5. Save the configuration and exit the CLI:

   ```
   save
   exit
   ```

NAT and NAPT Configuration Example

The router can be configured for NAT and NAPT simultaneously.



In this NAT and NAPT example:

- Multiple workstations in the private address space can use NAPT, and the server in the private address space can use NAT.
- The server may need NAT to send more than TCP/UDP traffic, or accommodate multiple types of inbound traffic types.

  For example, a Web server that uses FTP for maintenance needs access from the public address side for HTTP and FTP using NAT.

▶ Procedure

To configure the router for both NAPT and NAT:

1. Set up the router for NAPT. See *Network Address Port Translation* on page 5-8.
2. Set up a static address for any host not using NAPT:

   ```
   ip nat inside source static 10.1.1.1 155.22.17.1
   ```

Dynamic Host Configuration Protocol Server

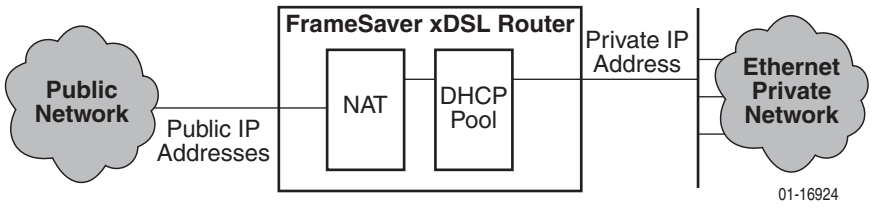
The router provides a Dynamic Host Configuration Protocol (DHCP) Server feature as specified in RFC 2131, Dynamic Host Configuration Protocol, and RFC 2132, DHCP Option and BOOTP Vendor Extensions. DHCP is the protocol used for automatic IP address assignment.

DHCP setup considerations:

- The range of IP addresses to be used by the DHCP server must be configured. The maximum number of clients is 253.
- The DHCP server is not activated until one IP address and subnet mask are assigned to the Ethernet interface.
- DHCP server and DHCP relay functions cannot be enabled at the same time.
- When the DHCP IP address range is changed, all binding entries, automatically added routes, and ARP table entries for the clients configured with the old address range are removed.
- When the DHCP Server is enabled, there can be only one IP address configured for the Ethernet interface.
- The IP address for the next hop router provided to the hosts in the DHCP reply must be configured.
- The minimum and maximum lease time settings can be configured.
- The subnet mask can be configured along with the IP address range (optional).
- The DHCP server domain name can be configured (optional).
- The Domain Name Server (DNS) IP address can be configured (optional).

DHCP Server with NAT Configuration Example

NAT with DHCP Server



In this DHCP Server with NAT example:

- The clients are using dynamic IP address assignment and use the Ethernet interface of the router as the next hop router (default gateway).
- The DHCP server assigns private IP addresses which are converted to public IP addresses by NAT.
- The DSL interface must be numbered.
- The router is configured as the DHCP server giving the private IP addresses to the clients.
- The Ethernet interface is in private address space. NAT is used for one-to-one mapping of addresses.

Public IP Addresses for NAT	Private IP Addresses
192.128.22.1	10.1.3.2
192.128.22.2	10.1.3.3
. . .	. . .
192.128.22.nnn	10.1.3.nnn

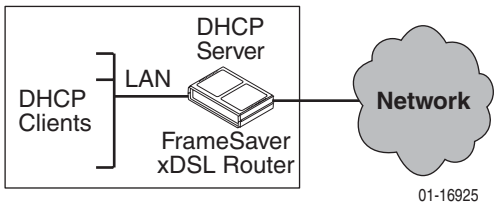
The command line syntax for this example, where *x* is the number configured for the sub-interface, is:

```
ip nat pool public 192.128.22.1 netmask 255.255.255.0
access-list 1 permit 10.1.1.0 0.0.0.255
ip nat inside source list 1 pool public
interface ethernet 0
ip nat inside
interface serial 0.x
ip nat outside
```

DHCP Server at Remote Site Configuration Example

DHCP Server at Remote Site

Customer Premises – Remote Site



In this DHCP Server at the remote site example:

- The DHCP clients send IP address requests to the specified DHCP server.
- The router is the DHCP server and provides IP addresses to DHCP clients on the local Ethernet segment.
- This example creates a pool of 254 reusable IP addresses.

The command line syntax for this example is:

```
ip dhcp pool pool17
network  155.1.3.0  255.255.255.0
default-router 155.1.3.254
```

DHCP Relay Agent

The router provides the capability of serving as a DHCP Relay Agent, as specified in RFC 2131, Dynamic Host Configuration Protocol. The router provides the capability to enable and disable the DHCP Relay Agent and to configure the IP address of the DHCP server to which the DHCP requests are to be sent.

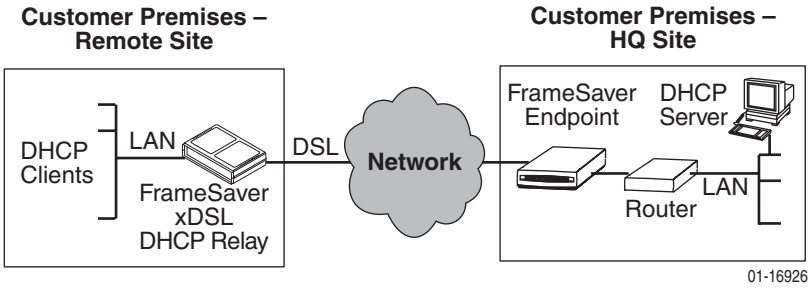
The DHCP server assigns an IP address to the end-user system. When DHCP Relay is enabled, it is possible to limit the number of DHCP clients. The router's IP Routing table and ARP table are automatically updated. The DHCP relay agent in the router should be used when there is a DHCP server at the customer's headquarters or central site.

DHCP relay agent setup considerations include the following:

- DHCP server IP address must be configured.
- DHCP relay must be enabled; i.e., both the server address and the interface closest to the server are configured.
- The number of DHCP clients is limited to 1–253.
- DHCP server and DHCP relay functions cannot be enabled at the same time.
- NAT and DHCP relay cannot be enabled at the same time.
- With DHCP relay enabled, the router sends the DHCP request to the DHCP server.

DHCP Relay Configuration Example

DHCP Relay Example



In this DHCP Relay example:

- The router is configured as a DHCP relay.
- UDP broadcasts received from DHCP clients are converted to routed DHCP requests and sent to the DHCP server.
- The DHCP server is specified.

The command line syntax for this example, where *x* is the number configured for the sub-interface, is:

```
ip dhcp server 155.1.3.254
ip route 155.1.3.254 serial 0.x
```

Router Security

The router offers security via the following:

- Filtering can be enabled or disabled for inbound and/or outbound traffic:
  - Ethertype
  - ICMP Message Type, Code
  - IP Protocol Type: TCP, UDP, or ICMP
  - TCP/UDP Ports
  - IP Source/Destination IP Address
- Always enabled:
  - Land Bug Prevention
  - Smurf Attack Prevention

IP Router Filtering

Router filtering does not apply when the router is in bridge-only mode. By default, filtering is disabled on the router. Filtering provides security advantages on LANs by restricting traffic on the network. A filter consists of a set of rules applied to a specific interface to indicate whether a packet received or sent on that interface is forwarded or discarded.

Filters are configured in general router configuration mode, then applied to the Ethernet or frame relay network interface. Filters are applied to traffic in either the transmit or receive direction on that interface.

There is one filter access list per interface, per direction, with a maximum of 33 rules per list. For IP filters, all rules with a source host IP address are applied first; all rules with a destination host IP address are applied next. The remaining filters are applied in the order in which they were configured.

Bridge Filtering

Bridge filtering does not apply when the router is in router-only mode. When bridging is enabled, separate ethertype filters are applied to the Ethernet and frame relay interfaces. They are applied to traffic in either the transmit or receive direction on that interface, with one filter access list per interface, per direction. There is a maximum of 16 rules per list. Each rule in the access list allows the user to filter a single ethertype or range of ethertypes.

MAC frames can be filtered based on the:

- SNAP Ethernet field in the 802.2 and 802.3 header.
- Protocol type field in the DIX Ethernet header.

For ethertype filters, the rules are applied in the order in which they were configured.

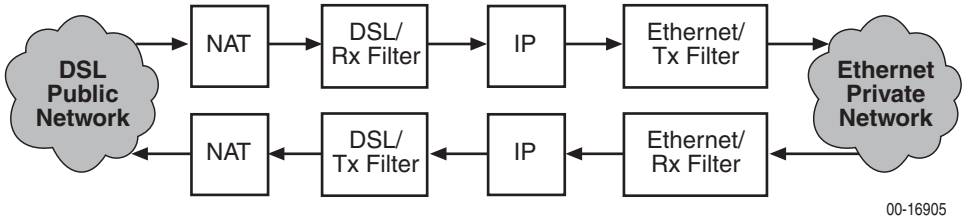
IP Filtering

For more information about IP filtering, see the *Hotwire MVL, ReachDSL, RADSL, IDSL, and SDSL Cards, Models 8310, 8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*.

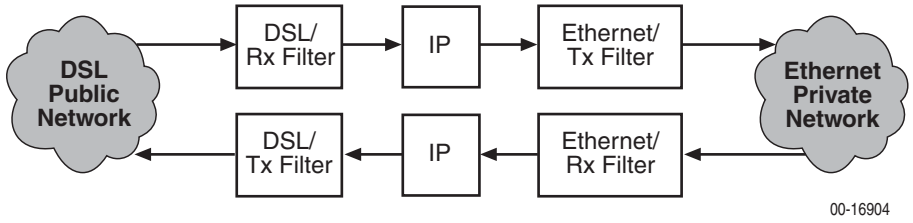
With NAT – When NAT is enabled and the IP filters are active, filtering is done on the Ethernet port – upstream first, then downstream.

- Upstream: From the client to the server
- Downstream: From the server to the client

Filtering with NAT



Filtering without NAT



Land Bug Prevention

The router drops all packets received on a network PVC interface or the Ethernet interface when the Source IP address is the same as the Destination IP address.

Smurf Attack Prevention

The router ignores requests to send an ICMP echo reply to the broadcast address and ICMP echo requests with a destination of the broadcast address.

Verifying the End-to-End Management Path

After installation of a remote router, run an ATM Ping test from the Hotwire GranDSLAM.

▶ Procedure

To ping the router:

1. From the Hotwire ATM Line Card's Main Menu, select the ATM Ping test.

   Diagnostics → *ATM Ping* (**D-C**)

2. Enter a VPI of 0 and a VCI of 35.
3. Select a Direction of Endpoint, then Start.

If both tests are successful, the VC has been tested from end to end.

Provisioning the Router Interface

The FrameSaver DSL Router defaults to bridge mode. Routing without bridging, and simultaneous routing and bridging, are also options.

Use the bridge command from the router's CLI to configure the bridge and routing attributes. Also, enter an Ethernet IP address and a DHCP IP address.

Refer to Appendix C, *Router CLI Commands, Codes, and Designations*, for command line syntax and information about CLI commands. For a list of default settings, see *CLI Command Default Settings* in Appendix D, *Router Command Line Summaries and Shortcuts*.

Configuring the Router Using Terminal Emulation

The CLI is available via a Telnet session or a direct connection over the router's COM port to a VT100-compatible terminal or a PC running a terminal emulation program. You access the CLI through the router's menu-driven user interface. From the Main Menu, press Shift-r to access the CLI.

Verify the required terminal settings:

- Data rate is set to 19.2 Kbps (19200 bps).
- Character length is set to 8.
- Parity is set to None.
- Stop bits is set to 1.
- Flow control is set to Off or None.

Uploading and Downloading the Router Configuration Via the CLI

Use the **show configuration** command to output command strings needed to restore the current running configuration.

Output from the show configuration command can be captured to a text file using most terminal emulation programs. Once the text file is captured, the router can be placed in configuration mode. The text file can then be fed back to configure the router.

Security and Logins

6

This chapter includes the following:

Limiting Access

The FrameSaver DSL device provides access security on the following interfaces:

- Asynchronous (async) terminal
- Telnet
- FTP
- SNMP
- Router's Command Line Interface (CLI)

The number of user interface active sessions available are:

- Two simultaneous Telnet sessions
- One Telnet session and one active COM port terminal session

The router's CLI allows one active session:

- One Telnet session or
- One COM port terminal session

Controlling Asynchronous Terminal Access

Direct asynchronous terminal access to the menu-driven user interface can be limited by:

- Requiring a login to the Communications port.
- Assigning an access level to the port or interface.

See *Configuring the Communication Port* in Chapter 4, *Configuration Options,* for more information about COM port configuration options.

▶ Procedure

To limit asynchronous terminal access to the user interface:

1. Select the Communication Port option.

   Main Menu→Configuration→Management and Communication→Communication Port

2. Set the following configuration options, as appropriate:

To . . .	Set the configuration option . . .
Require a login	Login Required to: Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login for the User Interface* on page 6-13.
Limit the access level to Level-3 or Level-2	Port Access Level to: Level-2 or Level-3. **NOTE:** A user cannot operate at a level higher than the access level set for the port. Keep the access at Level-1 if you are going to allow Level-1 users to configure the unit.

3. Save your changes.

NOTE:

If you are locked out inadvertently, see *Resetting the Unit and Restoring Communication* in Chapter 8, *Troubleshooting*.

Controlling External COM Port Device Access

Dial-in access to the user interface can be controlled when an external device (modem) is connected to the unit's COM port. The External Device Commands option must be set to AT.

▶ Procedure

To control dial-in access:

1. Select the External Modem options.

   Main Menu→ Configuration→ Management and Communication→ External Modem (Com Port)

2. Enable the Dial-In Access configuration option.

   This option appears only when the External Device Commands option is set to AT.

3. Save your changes.

See *Configuring the COM Port to Support an External Modem* in Chapter 4, *Configuration Options,* for more information about external device communication port configuration options.

Controlling Telnet and FTP Access

The FrameSaver unit provides several methods for limiting access to the user interface via a Telnet and/or FTP session. Telnet or FTP access can be via a standard management link or a service provider's TS (Troubleshooting) management link. For details regarding Telnet access to the Command Line Interface, refer to *Controlling Router CLI Access* on page 6-11.

Limiting Telnet Access

Telnet access can be limited by:

- Disabling Telnet access completely.
- Assigning an access level for Telnet sessions.
- Requiring a login for Telnet sessions that are not on the TS Management Link.
- Disabling TS Management Link access.

To limit Telnet access via a service provider's troubleshooting management link, see *Limiting Telnet or FTP Access Over the TS Management Link* on page 6-7.

▶ Procedure

To limit Telnet access when the session is **not on** the TS Management Link:

1. Select the Telnet and FTP Sessions option.

   Main Menu→Configuration→Management and Communication→Telnet and FTP Sessions

2. Set the following configuration options, as appropriate:

To . . .	Set the configuration option . . .
Disable Telnet access	Telnet Session to: Disable.
Require a login	Login Required to: Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login for the User Interface* on page 6-13.
Assign an access level	Session Access Level to: Level-2 or Level-3. **NOTE:** A user cannot operate at a level higher than the access level set for the Telnet session. Keep the access at Level-1 if you are going to allow Level-1 users to configure the unit.

3. Save your changes.

See *Configuring Telnet and/or FTP Sessions* in Chapter 4, *Configuration Options,* for more information about setting Telnet and FTP configuration options.

Limiting FTP Access

FTP access can be limited by:

- Disabling FTP access completely.
- Limiting FTP bandwidth.
- Requiring a user ID and password to login.

▶ Procedure

To limit FTP access when the session is **not on** the TS Management Link:

1. Select the Telnet and FTP Session options.

   Main Menu→ Configuration→ Management and Communication→ Telnet and FTP Sessions

2. Set the following configuration options, as appropriate:

To . . .	Set the configuration option . . .
Disable FTP	FTP Session to: Disable.
Require a login	Login Required to: Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login for the User Interface* on page 6-13. Level-1 access is required to download software to the unit, or to upload or download configuration files. Level-3 is sufficient to access SLV historical information via NMS. If you want to allow users to configure the unit or perform file transfers and downloads, keep the access at Level-1.
Limit bandwidth for FTP	FTP Max Transfer Rate to: a rate less than the network line speed, typically less than or equal to the CIR. This method is not recommended if SLV reports are desired since FTP is required to generate the reports.

3. Save your changes.

See *Configuring Telnet and/or FTP Sessions* in Chapter 4, *Configuration Options,* for more information about setting FTP configuration options.

Limiting Telnet or FTP Access Over the TS Management Link

▶ Procedure

To limit Telnet or FTP access for a session on the TS Management Link:

1. Select the Telnet and FTP Sessions options.

   Main Menu→ Configuration→ Management and Communication→ Telnet and FTP Sessions

2. Disable Telnet Session and/or FTP Session, as appropriate.
3. Return to the Management and Communication menu, and select Node IP.

   Main Menu→ Configuration→ Management and Communication→ Node IP

4. Set the following configuration options, as appropriate:

To . . .	Set the configuration option . . .
Disable access via a TS Management Link	TS Management Link to: None.
Assign an access level to the TS Management Link	TS Management Link Access Level to: Level-2 or Level-3. **NOTE:** A user cannot operate at a level higher than the access level specified for the session. To allow users to configure the unit, keep the access at Level-1.

5. Save your changes.

See *Configuring Telnet and/or FTP Sessions* or *Configuring Node IP Information* in Chapter 4, *Configuration Options,* for more information about these configuration options.

Controlling SNMP Access

The FrameSaver unit supports SNMP Version 1, which provides limited security through the use of community names. There are three methods for limiting SNMP access:

- Disabling SNMP access.
- Assigning SNMP community names and the access type.
- Assigning the IP address of each NMS that can access the unit.

Disabling SNMP Access

When the SNMP access is disabled, the FrameSaver unit will not respond to SNMP messages.

▶ Procedure

To disable SNMP access:

1. Select the General SNMP Management options.

   Main Menu→ Configuration→ Management and Communication→ General SNMP Management

2. Disable the SNMP Management option.
3. Save your changes.

See *Configuring General SNMP Management* in Chapter 4, *Configuration Options,* for more information about General SNMP Management configuration options.

Assigning SNMP Community Names and Access Levels

The FrameSaver unit supports the SNMP protocol and can be managed by an SNMP manager. SNMP manager access can be limited by:

- Assigning the SNMP community names that are allowed to access the FrameSaver unit's MIB.
- Specifying the type of access allowed for each SNMP community name.

Whenever an SNMP manager attempts to access a MIB object, the community name must be supplied.

▶ Procedure

To assign SNMP community names and access types:

1. *Select the General SNMP Management options.*

   Main Menu→Configuration→Management and Communication→ General SNMP Management

2. Set the following configuration options, as appropriate:

To . . .	Set the configuration option . . .
Assign SNMP Community Name 1 and/or 2	Community Name text: Up to 255 characters.
Assign the type of access allowed for each SNMP community name	Name 1 Access and Name 2 Access to: Read or Read/Write.

3. Save your changes.

See *Configuring General SNMP Management* in Chapter 4, *Configuration Options,* for more information about General SNMP Management configuration options.

Limiting SNMP Access Through IP Addresses

An additional level of security is provided by:

- Limiting the NMS IP addresses that can access the FrameSaver unit.
- SNMP Management System IP address validation.
- Specifying the access level allowed at the time IP address validation is performed.

Make sure that SNMP Management is set to Enable. Menu selection sequence:

Main Menu → Configuration → Management and Communication → General SNMP Management

See *Configuring General SNMP Management* in Chapter 4, *Configuration Options,* for more information about SNMP management configuration options.

The SNMP NMS Security Options screen provides the configuration options that determine whether security checking is performed on an IP address when unit communications attempts are being made.

▶ Procedure

To limit SNMP access through IP addresses:

1. Select the SNMP NMS Security option:

   Main Menu→ Configuration→ Management and Communication→ SNMP NMS Security

2. Set the following configuration options, as appropriate:

To . . .	Set the configuration option . . .
Enable IP address checking	NMS IP Validation to: Enable.
Specify the number (1–10) of SNMP management systems that are authorized to send SNMP messages to the FrameSaver unit	Number of Managers to: the desired number.
Specify the IP address(es) that identifies the SNMP manager(s) authorized to send SNMP messages to the unit	NMS *n* IP Address to: the appropriate NMS IP address.
Specify the access allowed for an authorized NMS when IP address validation is performed	Access Level to: Read or Read/Write.

3. Save your changes.

See *Configuring SNMP NMS Security* in Chapter 4, *Configuration Options,* for more information about SNMP NMS Security configuration options.

Controlling Router CLI Access

The FrameSaver DSL Router can be managed from an NMS using SNMP, or from the router's command line interface (CLI). There are two methods to access the command line interface:

- Local access at the DSL router through the COM port, or
- Access via a Telnet session.

  Telnet access defaults to Administrator level. If the current login is at the Operator level, only Operator level access is available for the session. Telnet access is always enabled.

The router accepts one CLI login session at a time and is configured at the factory without a default login ID and password. To provide login security to the DSL system, configure a login ID and password.

When a local console connection is first established, a login prompt appears. If the Device Name field has been configured via the Control menu *(Control Menu→System Information)*, the login prompt displays the device name. For example, a device name of Largo is shown as:

```
Largo>
```

See *Creating a Login for the User Interface* on page 6-13 for security information for each Login ID.

Access Levels (Command Modes)

There is one login ID and several levels of privileges for the router's CLI. Your user account can be configured with one user name and different passwords for:

- **Operator**. The Operator has read-only access to display device information with no modification permission and limited access to diagnostic functions. With a device name of Largo, the prompt appears as Largo>.
- **Administrator**. The Administrator has several levels of access to the DSL router's CLI. The # sign in the following prompts indicates Administrator access level.

Display Prompt with Device Name of Largo	Administrator Access Levels
Largo #>	Standard (same as Operator)
Largo(config) #	Configuration
Largo(config-if) #	Configuration Interface
Largo(config-subif) #	Configuration Sub-Interface
Largo(config-dhcp) #	Configuration DHCP Pool

Refer to Appendix C, *Router CLI Commands, Codes, and Designations*, for access level details for each command line entry.

Changing Access Levels

The Operator and Administrator have the same Login ID with different passwords for their access level. To determine the level of access for a session, refer to *Access Levels (Command Modes)* on page 6-11.

After accessing the router's CLI:

- You can access the Administrator access level by entering:

  `enable`

- The router's defaults to no password required. To require a password to access the Administrator access level, enter:

  `enable password` *password*

  Once saved, the router responds with a prompt to enter a password for Administrator access. This command is in effect until **`no enable password`** [*password*] is entered and saved.

- You can end the current Administrator access level by entering:

  `exit`

  This command results in ending the current Administrator access level session. Exit may need to be entered several times to reach Operator level and/or end the session.

- You can end the Administrator access level by entering:

  `end`

  This command results in ending the Administrator access level session and returning immediately to Operator level.

For further details, refer to *Chapter 5, Configuring the FrameSaver DSL Router,* and Appendix C, *Router CLI Commands, Codes, and Designations*.

Creating a Login for the User Interface

A login is required to access the user interface if security is enabled. Security is enabled by configuration options for:

- Communication Port Login Required
- FTP Login Required
- Telnet Login Required

Logins must be unique and are case sensitive. Up to six login ID/password combinations can be created and each login ID has a specified access level.

▶ Procedure

To create a login record:

1. Select Administer Logins.

   Main Menu→Control→Administer Logins

2. Select New, and set the following configuration options, as appropriate:

In the field . . .	Enter . . .
Login ID	1 to 10 ASCII characters.
Password	1 to 10 ASCII characters.
Re-enter Password	Password verification.
Access Level	■ **Level-1** – Top level. User can add, change, and display configuration options, save changes, and run device tests. All functions from the Main Menu are available. ■ **Level-2** – User can monitor and perform diagnostics and display status and configuration option information. Main menu displays Status, Test, and Configuration. ■ **Level-3** – User can only monitor and display status and configuration screens. Main menu displays Status and Configuration only. **CAUTION:** Make sure at least one login is set up for Level-1 access so you are not inadvertently locked out.

NOTE:

If you are locked out, see *Resetting the Unit and Restoring Communication* in Chapter 8, *Troubleshooting*.

3. Save your changes. You must save on this screen for updates to be valid.

   When Save is complete, the cursor is repositioned at the Login ID field, ready for another entry.

For information about SNMP security options, see *Configuring SNMP NMS Security* in Chapter 4, *Configuration Options*.

Modifying a Login

Logins are modified by deleting the existing login and creating a new one.

Deleting a Login

▶ Procedure

To delete a login record:

1. Select Administer Logins:

   Main Menu→ Control→ Administer Logins

2. Page through login pages/records using the PgUp or PgDn function keys until the login to be deleted is displayed.

3. Select Delete.

4. Save your deletion.

   When the deletion is complete, the number of login pages/records reflects one less record.

   Example:
   Page 2 of 4 is changed to Page 2 of 3.

Operation and Maintenance

7

This chapter includes the following information:

Displaying Identity System Information

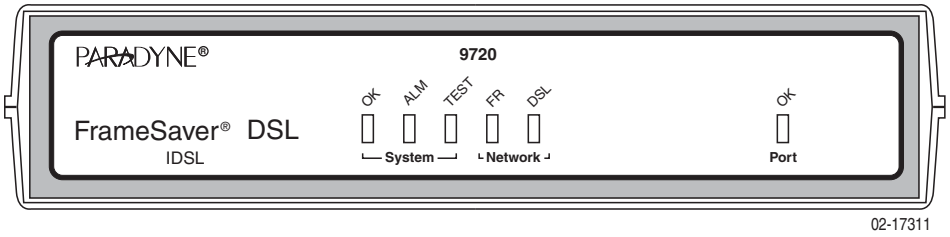
Use the Identity screen to view FrameSaver unit identification information. This information is useful if you are purchasing additional or replacement units and/or making firmware upgrades.

Main Menu→Status→Identity

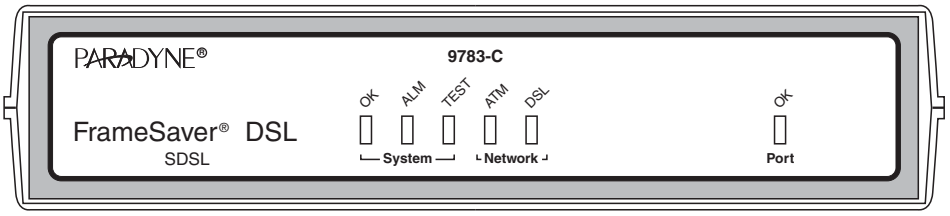
View this field . . .	To find the . . .
System Name	Domain name for this SNMP-managed node (if entered).
System Contact	Contact person for this SNMP-managed node.
System Location	Physical location for this SNMP-managed node.
NAM IDENTITY	
NAM Type	Type of Network Access Module installed: DSL FR-ATM NAM. This card type is supported by the SNMP SysDescr Object.
Hardware Revision	Unit's hardware version. Format *nnnn-nnx* consists of a 4-digit number, followed by two digits and one alphabetic character.
Current Software Revision	Software version currently being used by the unit. Format *nn.nn.nn* consists of a 6-digit number that represents the major and minor revision levels.
Alternate Software Revision	Software version that has been downloaded into the unit, but has not yet been implemented. Format *nn.nn.nn* consists of a 6-digit number that represents the major and minor revision levels. ■ **`In Progress`** indicates that the flash memory is currently being downloaded. ■ **`Invalid`** indicates that no download has occurred or the download was not successful.
Serial Number	Unit's 7-character serial number.
Ethernet MAC Address	MAC (Media Access Control) address assigned to the Ethernet port during manufacturing.

Viewing LEDs and Control Leads

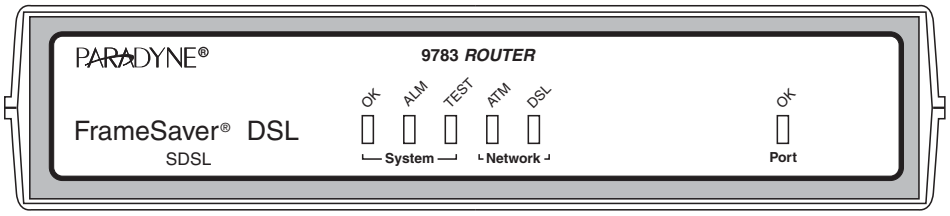
The FrameSaver DSL unit's faceplate includes LEDs (light-emitting diodes) that provide status on the unit and its interfaces.



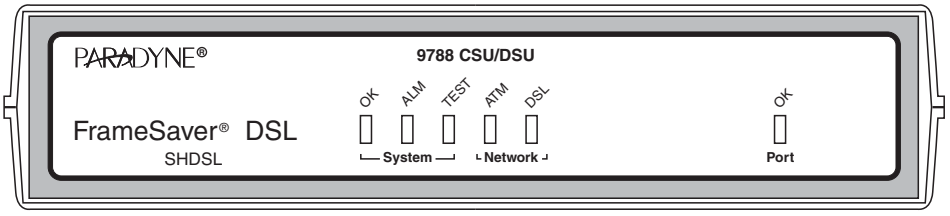
02-17311



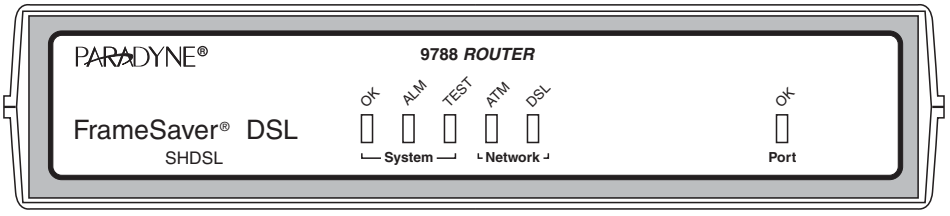
01-16946



01-16945



01-16990



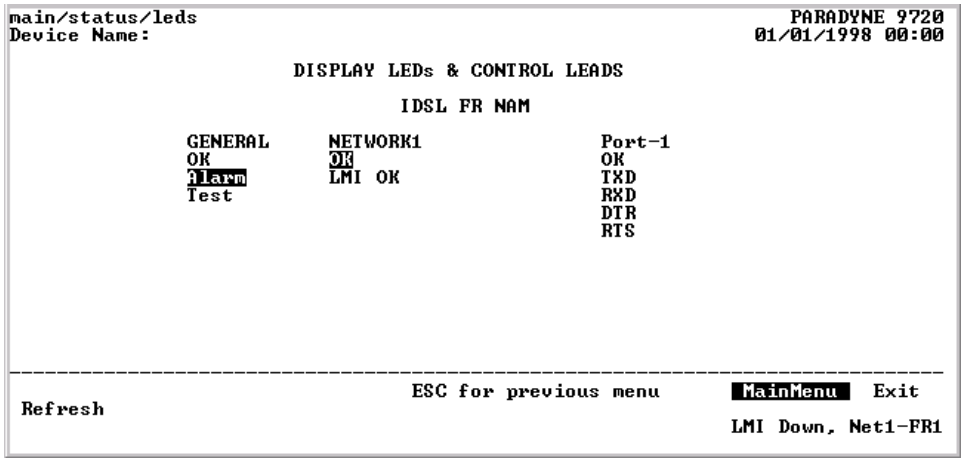
01-16991

In addition to LEDs, control leads can be monitored via the menu-driven user interface.

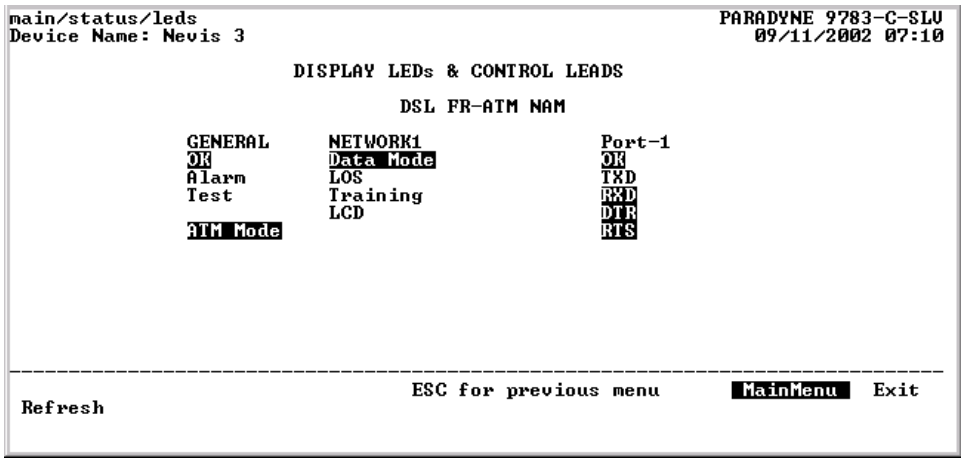
Main Menu → Status → Display LEDs and Control Leads

The Display LEDs and Control Leads screen allows you to monitor a remote unit and is useful when troubleshooting control lead problems. The appropriate interfaces are shown on this screen with the active status highlighted.

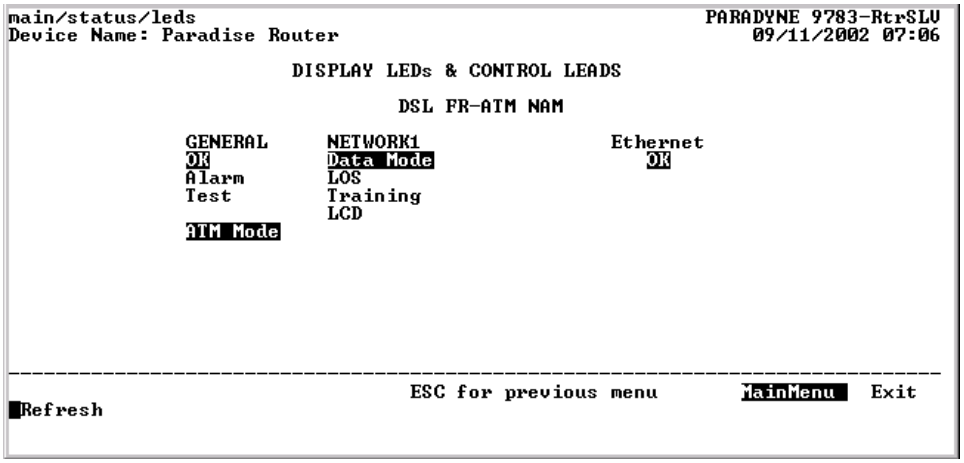
Display LEDs & Control Leads Screen for a 9720 CSU/DSU



Display LEDs & Control Leads Screen for a 9783 CSU/DSU



Display LEDs & Control Leads Screen for a 9783 Router



Refresh the screen to view control lead transitions.

LED Descriptions

Table 7-1, LED Descriptions, identifies the front panel LEDs.

Table 7-1. LED Descriptions (1 of 2)

Label	Indication	Color	What It Means
System LEDs			
OK	Power and Operational Status	Green	ON – The unit has power. OFF – The unit is in a power-on self-test, or there is a failure.
ALM	Operational Alarm (Fail)	Red	ON – The unit has been reset, or an error has been detected. OFF – No failures have been detected. See *Health and Status Messages* on page 7-20 for additional information about alarms.
TEST	Test Mode	Yellow	ON – A loopback or test pattern is in progress, initiated locally, remotely, or via the network. OFF – No tests are active.

Table 7-1. LED Descriptions (2 of 2)

Label	Indication	Color	What It Means
Network LEDs			
ATM (9783)	ATM Link Status	Green or Yellow	Green – The ATM link is active with cell delineation in sync. Yellow – The ATM link is active with loss of cell delineation. OFF – The ATM link is not active.
ATM (9788)	ATM Link Status	Green	Green – The ATM link is active with cell delineation in sync. OFF – The ATM link is active with loss of cell delineation, or the ATM link is not active.
FR (9720)	Frame Relay Link Status	Green	ON – LMI is up. OFF – LMI is down.
DSL	DSL Link Status	Green	ON – The DSL link is ready to transmit and receive data. OFF – The DSL link has not been established. Blinking – The DSL link is training.
Port LED — CSU/DSU			
OK	Port Status	Green	ON – The user data port is up and ready for operation. OFF – No device is detected on the user data port.
Port LED — Router			
OK	Interface Status	Green	ON – The Ethernet port is up and ready for operation. OFF – No device is detected on the Ethernet port.

Control Lead Descriptions

In addition to these LEDs, additional control leads can be monitored through the Display LEDs & Control Leads screen. They are described in Table 7-2, Control Leads. Port-1 leads do not apply to a router.

Table 7-2. Control Leads

Label	Indication	What It Means
General		
OK	Operational	The device's hardware and firmware are operational.
Alarm	Alarm Present	The device has detected a fault that may interfere with operation.
Test	Test in Progress	The unit is in a maintenance mode, such as a loopback test.
ATM Mode (9783, 9788)	ATM Mode is Active	The unit is configured for ATM operation. The front panel ATM LED is on.
Network Interface (9783, 9788)		
Data Mode	Data Mode Active	The unit has trained up and is operating in normal data mode. The front panel DSL LED is on.
LOS	Loss Of Signal	An LOS condition has been detected on the network. The front panel ALM LED is on.
Training	Training in Progress	The unit is training and the DSL LED is flashing.
LCD	Loss of Cell Delineation	An LCD alarm condition has been detected. On the 9783, the front panel ATM LED is yellow.
Network Interface (9720)		
OK	DSL Line OK	The unit has trained up and is operating in normal data mode. The front panel DSL LED is on.
LMI OK	LMI Operating	The LMI is operating successfully on the first frame relay link on the network interface.
Port-1 — CSU/DSUs only		
OK	Port-1 is Active	The user data port is transmitting and receiving data.
TXD	Transmit Data	Data is being sent to the far-end device.
RXD	Receive Data	Data is being received from the far-end device.
DTR	Data Terminal Ready	The DTE is not ready to operate.
RTS	Request to Send	The DTE has indicated that it is ready to transmit data.
Ethernet		
OK	Ethernet is Active	The Ethernet connection is transmitting and receiving data.

Device Messages

Messages in Table 7-3, Device Messages, appear in the messages area at the bottom of the user interface screens. All device messages are listed in alphabetical order.

Table 7-3. Device Messages (1 of 5)

Message	What It Indicates	What To Do
Access level is *n*, Read-only.	User's access level is 2 or 3; user is not authorized to change configurations.	No action is needed.
Already Active	Test selected is already running.	■ Allow test to continue. ■ Select another test. ■ Stop the test.
Blank Entries Removed	New had been selected from the Administer Logins screen, no entry was made, then Save was selected.	■ No action is needed. ■ Reenter the Login ID, Password, and Access Level.
Cannot delete Trap Manager	Delete was selected from Management PVCs Options, but the PVC had been defined as a trap destination.	No action needed, or configure another path for traps and try again.
Cannot Save – no Level 1 Login IDs	Security was being set up, but all the logins were assigned either Level-2 or Level-3.	Set up at least one login with Access Level-1 so the unit can be configured.
Command Complete	Configuration saved or all tests have been aborted.	No action is needed.
Connection Refused *(Seen at an FTP terminal.)*	Two menu-driven user interface sessions are already in use when a Telnet session was attempted.	Wait and try again.
Destination Not Unique	Destination entered is already being used.	Enter another destination indicator.
DLCI in connection. Delete connection first	User tried to delete a DLCI that was part of a connection.	■ No action needed, or ■ Delete the connection, then delete the DLCI.
DLCI Number Already Exists	The DLCI number entered on the DLCI Record Entry screen is not unique.	Enter another DLCI number.
DLCI Number Reserved	User tried to designate a special troubleshooting DLCI.	No action is needed.

Table 7-3. Device Messages (2 of 5)

Message	What It Indicates	What To Do
Duplicate DLCI Number	DLCI entered is not unique for the frame relay link.	No action is needed; previous contents of the DLCI number field are restored.
File Transfer Complete *(Seen at an FTP terminal.)*	A file transfer was performed successfully.	Switch to the newly downloaded software. See *Activating Software* on page 7-47.
File Transfer Failed – Invalid file *(Seen at an FTP terminal.)*	A file transfer was attempted, but it was not successful.	■ Try again, making sure you type the filename correctly. ■ Exit the FTP session, or download another file. See *Activating Software* on page 7-47.
Invalid Character (*x*)	A non-valid printable ASCII character has been entered.	Reenter information using valid characters.
Invalid date: must be mm/dd/yyyy	An invalid date was entered on the System Information screen.	Reenter the date in the month/day/4-digit year format.
Invalid date and/or time	An invalid date or time was entered on the System Information screen.	Reenter the date in the month/day/4-digit year format and/or time in the hour:minutes:seconds format.
Invalid time: must be hh:mm:ss	An invalid system time was entered on the System Information screen.	Reenter the time in the hour:minutes:seconds format.
Invalid – Already Active	A selected test was already in progress.	No action is needed.
Invalid Password	Login is required and an incorrect password was entered; access is denied.	■ Try again. ■ Contact your system administrator to verify your password.
Invalid Test Combination	When Start was selected, a conflicting loopback or pattern test was in progress, or was active on the same or another interface.	■ Wait until other test ends and message clears. ■ Cancel all tests from the Test screen (Path: *Main*→*Test*). ■ Stop the test from the same screen the test was started from.
Limit of six Login IDs reached	Attempting to enter a new login ID and the limit of six login/password combinations has been reached.	■ Delete another login/password combination. ■ Reenter the new login ID.

Table 7-3. Device Messages (3 of 5)

Message	What It Indicates	What To Do
Limit of Mgmt PVCs reached	New was selected from the PVC Connection Table and the maximum number of management PVCs has already been created.	Do not create the management PVC. Delete another management PVC, and try again.
Limit of PVC Connections reached	The maximum number of PVCs has already been created and New was selected from the PVC Connection Table.	Do not create the PVC connection. Delete another PVC connection, and try again.
Name Must be Unique	Name entered for a management PVC has been used.	Enter another 4-character name for the logical/management link.
No Circuits available for Mgmt PVC	New was selected from the Management PVCs screen, but no unconnected frame relay Link/DLCI/EDLCI or ATM Link/VPI/VCI has been defined that can be used in a management PVC.	Define a new frame relay Link/DLCI/EDLCI or ATM Link/VPI/VCI for the management PVC.
No Destination Link DLCIs Available	New was selected from the PVC Connection Table, but no DLCIs are available on the network link.	Even though DLCIs are available to form a connection, configure additional DLCIs for the network link and try again.
No DLCIs available for connection	All configured DLCIs have been connected but New was selected from the PVC Connection Table.	No action needed, or configure additional DLCIs and try again.
	All Link/DLCI pairs have been connected but New was selected from the Management PVCs screen.	Configure additional network and/or Port-1 Links/DLCIs pairs and try again.
No DLCIs Available for Mgmt PVC	All configured DLCIs have been connected but New was selected from the Management PVCs screen.	Configure additional network and/or Port-1 DLCIs and try again.
No DLCIs Defined	DLCI Records was selected from an interface's Configuration Edit menu, and no DLCI Records have been created for this interface.	Select New and create a DLCI record.
No more DLCIs allowed	New or CopyFrom was selected from an interface's DLCI Records screen, and the maximum number of DLCI Records had already been reached.	Delete a DLCI, then create the new DLCI Record.

Table 7-3. Device Messages (4 of 5)

Message	What It Indicates	What To Do
No Primary Destination Link DLCIs Available	New or Modify was selected from the PVC Connection Table, but even though DLCIs are available to form a connection, no DLCIs are available on the network link, which is a suitable Primary PVC Destination.	Configure additional DLCIs for the network link and try again. If a network DLCI has been entered as a Source DLCI: 1. Change the Source DLCI to a user data port DLCI. 2. Enter the network DLCI as the PVC's Primary Destination.
No Security Records to Delete	Delete was selected from the Administer Logins screen, and no login exists.	■ No action is needed. ■ Enter a security record.
Password Matching Error – Re-enter Password	Password entered in the Re-enter Password field of the Administer Logins screen does not match what was entered in the Password field.	■ Try again. ■ Contact your system administrator to verify your password.
Permission Denied *(Seen at an FTP terminal.)*	A file transfer was attempted, but the: ■ User did not have Level-1 security. ■ Wrong file was specified when the **put** command was entered. ■ User attempted to upload a program file from the unit.	■ See your system administrator to get your security level changed. ■ Try again, entering the correct file with the **put** command. ■ Enter the **put** command instead of a **get** command; you can only transfer files to the unit, not from it. See *Upgrading System Software* on page 7-46.
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Port Inactive	The port is disabled.	No action is needed.
Requested action aborted: *Reason* *(Seen at an FTP terminal.)*	A file transfer was aborted for the *Reason* shown: ■ Invalid file or model number ■ Invalid file checksum ■ Insufficient memory ■ File database version does not match device database version ■ File slot config does not match device slot config	■ Download the correct configuration file. ■ Download a different file. ■ Notify your service representative. ■ Download the correct configuration file. ■ Download the correct configuration file.

Table 7-3. Device Messages (5 of 5)

Message	What It Indicates	What To Do
Resetting Device, Please Wait ...	**Yes** was entered for **Reset COM Port usage** field of the System Paused menu.	No action is needed.
Save Cancelled	Changes were made on the Easy Install screen, but the Esc key was pressed or **No** was entered in response to the **Save Changes?** prompt.	No action is needed.
Test Active	No higher priority health and status messages exist, and a test is running.	■ Contact service provider if test initiated by the network. ■ Wait until the test ends and message clears. ■ Cancel all tests from the Test screen. Path: *Main→Test*. ■ Stop the test from the same screen the test was started from.
User Interface Already in Use	Two Telnet sessions are active when an attempt to access the menu-driven user interface through the COM port is made. IP addresses and logins of the users currently accessing the interface are displayed.	■ Wait and try again. ■ Contact one of the IP address users and request that they log off.
User Interface Idle	Previously active session is ended, and access via the COM port is now available.	Log on to the FrameSaver unit.
	Session has been ended due to timeout.	No action is needed.
Value Out of Range	CIR entered for the DLCI is a number greater than the maximum allowed.	Enter a valid CIR (0–1536000).
	Excess Burst Size entered for the DLCI is a number greater than the maximum allowed.	Enter a valid Excess Burst Size (0–1536000).
	DLCI Number entered is less than 16 or greater than 1007.	Enter a valid number (16–1007).

Router CLI Messages

The router's Command Line Interface messages are listed alphabetically in Table 7-4, CLI Messages. Refer to Appendix C, *Router CLI Commands, Codes, and Designations*, for **show** commands and additional information.

Table 7-4. CLI Messages (1 of 5)

Message	What It Indicates
% Access list entry already exists	An attempt was made to add an already existing access list rule.
% Access list does not exist	An attempt was made to delete a non-existent access list.
% Access list is not assigned	An attempt was made to delete a non-existent access list assignment.
% Access list number must be between 1 and 299	The access list number entered is outside the valid range.
% Access list number must be between 200 and 299	The access list number entered to create a bridge filter rule is outside the valid range.
% Administrator level access is required for this command.	An attempt was made to access configuration information without the authorized access level.
% ARP Timeout can only be specified on the Ethernet port	An attempt was made to specify the ARP timeout on an interface other than the Ethernet port.
% ARP Timeout must in the range 0–4294967	An attempt was made to specify an ARP timeout that is outside the valid range.
% Bridge group filter already exists	An attempt was made to create an already existing bridge filter rule.
% Bridge group filter does not exist	The bridge group filter specified for deletion does not exist.
% Bridge group filter list is full	An attempt was made to add a bridge filter rule, but the maximum number of rules have already been created.
% Bridge group not assigned	An attempt was made to remove a non-existent bridge group assignment.
% Destination IP address is already part of an interface route	The route entered for a destination IP address is within the IP address range assigned to the interface.
% DHCP max clients must be 1–*MaximumDHCPClients*	An attempt was made to enter an invalid DHCP client limit.
% DHCP network does not exist	An attempt was made to delete a non-existent DHCP network.
% DHCP Network Prefix range 1–32	An attempt was made to enter an invalid prefix length.
% DHCP pool does not exist	An attempt was made to delete a non-existent DHCP pool.

Table 7-4. CLI Messages (2 of 5)

Message	What It Indicates
% DLCI number must be 16−1007	The DLCI entered is not in the valid range.
% Frame-Relay encapsulation is only supported on Serial ports	An attempt was made to enable frame relay encapsulation on the Ethernet port.
% For Ethernet ports, interface must be 0	An unsupported interface index was entered for the Ethernet port.
% For Serial ports, interface must be 0	An unsupported interface index was entered for the serial port.
% Gateway of last resort is not set	No Gateway of last resort was configured.
% ICMP Message type and code combination not supported	The ICMP message type/code combination entered is not supported by the product.
% ICMP Message type must be 0−255	The ICMP message type entered is not within the valid range.
% ICMP Message code must be 0−255	The ICMP message code entered is not within the valid range.
% Invalid IP address or Mask specified	The prefix length entered is not valid for the *start-ip-address* or *end-ip-address*.
% Invalid sub-interface specified	The sub-interface specified for deletion does not exist.
% IP Address already in use for device management	An attempt was made to reassign the Ethernet port's or node's IP address, but the address is being used.
% IP Address cannot be removed, since a static route relies on it	An attempt was made to delete an interface address assignment that has routing table entries other than an interface route, with Next Hop Router addresses that fall within its address range.
% IP Address does not exist in ARP table	An attempt was made to delete an ARP entry for an IP address, but no ARP entry exists for the specified address.
% Lease must be 0−365 days, 0−24 hours, 0−59 minutes	An invalid lease time was entered.
% Maximum number of access lists exceeded	An attempt was made to add an access list, but the maximum number of access lists have already been created.
% Maximum number of access list assignments to interface exceeded	An attempt was made to add an access list assignment, but the maximum number of access lists have already been assigned to the interface.
% Maximum number of filters exceeded on this access list	An attempt was made to add an access list filter rule, but the maximum number of filter rules have already been created.
% Maximum number of NAT pools reached	An attempt was made to add a NAT pool, but the maximum number of pools have already been reached.

Table 7-4. CLI Messages (3 of 5)

Message	What It Indicates
% Maximum number of dynamic NAT translations rules reached	An attempt was made to add a dynamic NAT translation, but the maximum number of translations have already been reached. Keywords **list** and **pool** were specified, but not **overload**.
% Maximum number of static NAT translations reached	An attempt was made to add a static NAT translation, but the maximum number of translations have already been reached. Keyword **static** was entered, with two IP addresses, but no protocol specified.
% Maximum number of dynamic PAT translations rules reached	An attempt was made to add a dynamic PAT translation, but the maximum number of translations have already been reached. Keywords **list** and either **pool** or **interface**, and **overload** are specified.
% Maximum number of static PAT translations reached	An attempt was made to add a static PAT translation, but the maximum number of translations have already been reached. Keywords **static** and **interface** were entered that specify two IP addresses, protocol, and a local TCP/UDP port number.
% Maximum number of sub-interfaces already exist	An attempt was made to create a new sub-interface, but the maximum number of sub-interfaces have already been created.
% NAT pool does not exist	The NAT pool entered does not exist.
% NAT pools can't have more than 254 IP addresses	The number of IP addresses in a NAT pool cannot exceed 254.
% NAT Prefix range is 24–32	An attempt was made to enter a prefix length that is outside the valid range.
% NAT Translation timeout must be in the range 0–2147483647	An attempt was made to enter a NAT timeout that is outside the valid range.
% Next Hop IP address is assigned to an interface	The route entered with a Next Hop IP address is the IP address assigned to the interface.
% Next Hop IP address must fall within the IP address range assigned to the interface	The route entered with a Next Hop IP address does not fall within the IP address range for the interface.
% Only bridge group 1 is supported at this time	A bridge group was specified that is outside the valid range.
% Ping packets must be between 0–1500 bytes	An attempt was made to initiate a Ping test with a packet length that is outside the valid range.
% Ping timeout must be between 1–30 seconds	An attempt was made to initiate a Ping test with a timeout that is outside the valid range.
% PVC already assigned to sub-interface *sub-interface*	The DLCI is already assigned on an interface other than the current sub-interface.
% PVC is already defined	The DLCI is already defined on the current sub-interface.

Table 7-4. CLI Messages (4 of 5)

Message	What It Indicates
% Sub-interfaces are only supported on the Serial 0 Interface	An attempt was made to enter a sub-interface on the Ethernet port.
% Sub-interface does not exist	An attempt was made to create a route using a non-existent sub-interface.
% Sub-interface in use. Sub-interface uses must be removed first.	An attempt was made to delete a sub-interface that is currently in use. Perform the following configuration changes prior to deleting a sub-interface: ■ Delete all route entries destined for the sub-interface. ■ Delete all route entries destined for the sub-interface's subnet ip address range. ■ Delete the IP address (or IP unnumbered designation) on the sub-interface, if one exists. ■ Delete the frame relay DLCI on the sub-interface, if one exists. ■ Delete bridge group assignments from the sub-interface. ■ Delete IP NAT inside/outside assignments for the sub-interface. ■ Delete the IP helper address on the sub-interface.
% Sub-interface must be specified for Serial interfaces	An attempt was made to specify a serial interface without specifying a sub-interface.
% Sub-interface must be specified for Serial interfaces	A serial interface was specified without the sub-interface also being specified.
% Sub-interface number must be 0−4294967295	The number entered is outside the supported sub-interface range.
% Sub-interfaces are only supported on the Serial 0 Interface	An attempt was made to create a sub-interface on the Ethernet port.
% Subnet must be unique	The subnet mask for the sub-interface entered is not unique.
% The DHCP Server and DHCP Relay cannot both be enabled	An attempt was made to enable the DHCP server and DHCP Relay is already enabled.
% The static ARP table is full	An attempt was made to create a new ARP entry, but the maximum number of static ARP entries have already been created.
%The static route table is full	An attempt was made to assign an IP address, but the maximum number of static routes have already been configured.
% The DHCP Server and DHCP Relay cannot both be enabled	An attempt was made to enable DHCP Relay and the DHCP Server is already enabled.

Table 7-4. CLI Messages (5 of 5)

Message	What It Indicates
% The DHCP Server and NAT cannot both be enabled	An attempt was made to enable the DHCP server and Network Address Translation (NAT), but they are already enabled.
% The Next Hop IP address is assigned to an interface or sub-interface on this device	The route entered had a Next Hop IP address that is in the interface's assigned address range.
% TCP/UDP port must be 0−65535	The port number entered is outside the specified range.
% Traceroute hops must be between 1 and 128 hops	A TraceRoute test was attempted, but the maximum hop value is outside the specified range.
% Traceroute packets must be between 0 and 1500 bytes	A TraceRoute test was attempted, but the packet length is outside the specified range.
% Traceroute timeout must be between 1 and 30 seconds	A TraceRoute test was attempted, but the timeout value entered was outside the specified range.
% Unable to delete physical interface	Physical interfaces cannot be deleted; only sub-interfaces can be deleted.
% Unable to Transmit ping packet	A Ping cannot be performed because: ■ No ports are enabled for IP ■ The specified interface does not exist ■ The link is down
% Unable to Transmit traceroute packets	A traceroute cannot be performed.

Status Information

Status information is useful when monitoring the FrameSaver unit. The following illustration shows the Status menu for a central site CSU/DSU.

Status Menu

```
main/status                                                          9783-C-SLV
Device Name: Node A                                          2/26/2001  06:02

                                    STATUS

                            System and Test Status
                            PVC Connection Status
                            Network Interface Status
                            IP Routing Table (Management Traffic)
                            Performance Statistics
                            Trap Event Log
                            Display LEDs and Control Leads
                            Identity

--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

System and Test Status Messages

To access System and Test status information:

Main Menu→Status →System and Test Status

The following information is included on this screen:

- *Self-Test Results Messages*
- *Last Reset*
- *Health and Status Messages*
- *Test Status Messages*

NOTE:

Status messages in the following sections are in alphabetical order.

Self-Test Results Messages

Self-test result messages shown in Table 7-5, Self-Test Results Messages appear in the Self-Test Results field at the top of the System and Test Status screen.

Table 7-5. Self-Test Results Messages

Message	What It Indicates	What To Do
Failure *xxxxxxxx*	An internal failure occurred *(xxxxxxxx* represents an 8-digit hexadecimal failure code used by service personnel). Record the failure code before resetting the unit; otherwise, the error information will be lost.	1. Record the failure code. 2. Reset the unit. 3. If problem still exists, contact your service representative.
Passed	No problems were found during power-on.	No action needed.

Last Reset

The Last Reset field provides the last date and time that the FrameSaver unit was reset. This field is located after the Self-Test Results field at the top of the System and Test Status screen.

Main Menu→Status →System and Test Status

Health and Status Messages

Table 7-6, Health and Status Messages, provides Health and Status messages that apply to the FrameSaver unit.

Table 7-6. Health and Status Messages (1 of 2)

Message	What It Indicates
Back-to-Back Mode Active	The unit has been configured for back-to-back operation. *Main Menu*→*Control*→*Change Operating Mode* The FrameSaver unit can be connected to another FrameSaver unit without a frame relay switch between them. This feature is useful for product demonstrations or for a point-to-point configuration using a leased line.
COS*x* Down, Path*IP_ Address, Interface*DLCI*nnnn*	A Class Of Service associated with a path is down. COS*x* is the Class of Service ID associated with the path, *IP_Address* is the IP address of the path endpoint, *Interface* is P1 (Port 1) or N1 (Network 1), and *nnnn* is the DLCI which contains the path.
CTS down to Port 1 Device *(CSU/DSU only)*	The CSU/DSU's user data port CTS control lead is off.
DLCI *nnnn* Down, Port 1	The DLCI for the Port 1 frame relay link is down.
DSL Line Training, Network 1	The device is in the process of determining the right speed.
DTR Down from Port 1 Device *(CSU/DSU only)*	The device DTR control lead connected to the user data port is deasserted.
Ethernet Mgmt Down	The Ethernet management interface is down. The port is enabled and is the primary interface for management data, but communication between the management system and the unit is not currently possible.
Ethernet Port Down	The Ethernet link is down. The port is enabled and is the primary interface for user data, but communication between the unit and the far end is not currently possible.
Latency*IP_ Address,* COS*x,Interface*DLCI*nnnn*[1]	An IP SLV Latency Threshold has been exceeded for the specified COS of the Path. *IP_Address* is the IP address of the path endpoint, COS*x* is the Class of Service ID associated with the path, *Interface* is P1 (Port 1) or N1 (Network 1), and *nnnn* is the DLCI which contains the path.
Link Down Administratively, Port 1	CSU/DSU only. The specified frame relay link has been disabled by the unit due to LMI Behavior conditions or LMI Protocol on another link is in a failed state. This is not an alarm condition so **`System Operational`** appears as well.

Table 7-6. Health and Status Messages (2 of 2)

Message	What It Indicates
LMI Discovery In Progress, Port 1	LMI protocol discovery is being performed to determine the protocol to be used on the specified frame relay link. This is not an alarm condition so **`System Operational`** appears as well.
LMI Down, Port 1	The Local Management Interface has been declared down for Port 1.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. The condition is cleared as soon as a signal is detected. Possible reasons include: ■ Network cable problem. ■ No signal is being transmitted at the far-end unit.
Loss of Cell Delineation, *atm_link*	The ATM TC (Transmission Convergence) layer has been in a Loss of Cell Delineation (LCD) state for one minute, or the number of Out of Cell Delineation (OCD) delineation events has exceeded the user-specified threshold.
Network Com Link Down	The COM port communication link is down. The COM port is configured for Net Link.
Path*IP_ Address* Down, *Interface*DLCI*nnnn*	A path on the network interface is unavailable. *IP_Address* is the IP address of the path endpoint, *Interface* is P1 (Port 1) or N1 (Network 1), and *nnnn* is the DLCI which contains the path.
SLV Timeout, DLCI *nnnn*, Port 1	An excessive number of SLV communication responses from the remote FrameSaver SLV unit have been missed on the specified multiplexed DLCI; the DLCI is not suitable for user data. Does not apply to a TS Management Link DLCI. When a hardware-bypass capable device has been detected at the other end of the PVC and this condition exists, only EDLCI 0 user data will be transmitted.
SNR Margin Threshold Exceed, Network 1	The user-specified SNR margin threshold has been exceeded.
Two Level-1 Users Accessing Device	Two Level 1 users are already using the menu-driven user interface; only two sessions can be active at one time.

Test Status Messages

Test status messages, listed in Table 7-7, Test Status Messages, appear in the right column of the System and Test Status screen. You have the option to continue the test or to abort the test. See Chapter 8, *Troubleshooting*, for more information on tests, including how to start and stop them.

Table 7-7. Test Status Messages

Message	What It Indicates
511 Pattern Test Active, Network 1 *(9788 only)*	A 511 pattern test is active on the SHDSL network interface.
DTE External LB Active, Port-1 *(CSU/DSU only)*	External DTE Loopback is running on the user data port.
DTE Init. Ext LB Active, Port-1 *(CSU/DSU only)*	The DTE has initiated an external DTE Loopback on the user data port. This message remains as long as the LL lead is asserted.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the faceplate to flash on and off.
Monitor *Pttn* Active, DLCI *nnnn*, *frame_relay_link*	The unit is monitoring a test pattern on the specified frame relay link DLC1.
No Test Active	No tests are currently running.
PVC Loopback Active, DLCI *nnnn*, *frame_relay_link*	A PVC Loopback is active on the specified frame relay link DLCI.
Send *Pttn* Active, DLCI *nnnn*, *frame_relay_link*	The unit is sending the selected test pattern on the specified DLCI for the interface.
Tran. Pass-Thru Test Active, Network 1 *(9788 only)*	A Transparent Pass-Through Loopback Test is active on the specified SHDSL Network Interface.

IP Path Connection Status

IP Path Connection Status is selected from the Status menu.

Main Menu→Status→IP Path Connection Status

The IP Path Connection Status screen displays the IP Path List, a list of devices that can be reached by their IP addresses for Service Level Management purposes.

The list is displayed in IP address order and includes both static addresses entered using the IP Path List (Static) configuration screen (see *Configuring the IP Path List* in Chapter 4, *Configuration Options*) and paths discovered as packets are received from other FrameSaver units

This screen only appears when Service Type is set to Frame Relay.

IP Path Connection Status Screen Example

```
main/status/path                                                        9783
Device Name: Node A                                          09/11/2002 07:00

                    FR Link IP PATH CONNECTION STATUS              Page 1 of 2
                              DLCI: 201
        Device Name  IP Address      Status   Discovery Source
          Poughkeepsie 135.026.002.001 Active   135.026.002.005
              New York 135.026.002.002 InActive 135.026.002.005
                Boston 135.026.002.003 Active   135.026.002.005
           Los Angeles 135.026.002.004 Active   135.026.002.005
               Chicago 135.026.002.005 Active   135.026.002.005
         San Francisco 135.026.002.006 Active   135.026.002.005
             Milwaukee 135.026.002.007 Active   135.026.002.005
               Unknown 137.010.010.001 Active   Static
                 Miami 137.010.010.002 Active   Static
               Orlando 137.010.010.003 Active   Static




--------------------------------------------------------------------------------
                                  ESC for previous menu      MainMenu   Exit
 Refresh     PgUp   PgDn              NextDLCI      PrevDLCI
```

Table 7-8. IP Path Connection Status

Field	Status	What It Indicates
FR Link	Net1-FR1, Port-1	The frame relay link.
DLCI	16 through 1007	The IP Enabled DLCI.
Device Name	Up to 20 ASCII characters	The name of the device configured using the System Information screen of the Control branch, or Unknown if the device is not a FrameSaver.
IP Address	000.000.000.001 – 255.255.255.255	The IP address of the unit at the far end of the path.
Status	Active Inactive	The status of the path: ■ The path is operational. ■ The path is not operational.
Discovery Source	■ Static ■ 000.000.000.001 – 255.255.255.255	The source of the path definition: ■ The path was entered using the IP Path List (Static) screen ■ This is the IP address of the FrameSaver unit that provided the path.

PVC Connection Status

PVC Connection Status is selected from the Status menu.

Main Menu→Status→PVC Connection Status

PVC Connection Status Screen Example

```
main/status/connections                                              9783-C-SLV
Device Name: Node A                                          06/05/2001   06:03

                                                                     Page 1 of 2
                          PVC CONNECTION STATUS

      Source              Primary Destination
  Link    DLCI  EDLCI    Link      DLCI    EDLCI    Status

 Port-1    201          Net1-FR1    300      PM     Active
 Port-1    202          Net1-FR1   1001      0      Active
 Port-1    100          Net1-FR1   1001      2      Active
 Port-1    204          Net1-FR1   1001      2      Active
 Rrt-S0    204          Net1-FR1    206      0      Active
 Mgmt PVC               Port-1       16             Active
 Mgmt PVC  TS_Mgmt      Net1-ATM  (0, 35)           Active
 Mgmt PVC  Largo        Net1-ATM  (0, 33)           Active




--------------------------------------------------------------------------------
                           ESC for previous menu          MainMenu    Exit
 Refresh     PgUp   PgDn
```

Only PVC connections with an active Source DLCI configuration are shown. If the **No PVC Connections** message appears instead of a list of PVC connections, no PVC connections have been configured yet.

Table 7-9. PVC Connection Status Screen (1 of 2)

Field	Display	What It Indicates
Link		Identifies the cross-connection of source and primary destination DLCIs configured for the unit.
	■ Net1-FR1	■ The frame relay link 1 is the source/destination is on Network 1.
	■ Net1-ATM *(9783, 9788)*	■ The ATM link is the source/destination on Network 1.
	■ Port-1 *(CSU/DSUs only)*	■ The CSU/DSU's user data port is the source/destination.
	■ Mgmt PVC *Name*	■ The virtual circuit is a management link that terminates in the unit. *Name* is the link name.
	■ Rtr-S0 *(Routers only)*	■ The source link is the virtual router's frame relay link, internally connected to its Serial 0 interface.

Table 7-9. PVC Connection Status Screen (2 of 2)

Field	Display	What It Indicates
DLCI	■ *DLCI* (16–1007) ■ *VPI,VCI* (0–15 VPI, 31–255 VCI)	Identifies the source/destination of the specified virtual circuit. Management PVCs built on the ATM link display the VPI/VCI value in parentheses instead of a DLCI number.
EDLCI	0 to 62 IP PM	For multiplexed DLCIs, a number from 0 to 62 identifies an individual link embedded within a DLCI. For IP Enabled DLCIs, IP is displayed. For DLCIs not IP enabled that are the primary destination of a payload managed PVC, PM is displayed.
Status		Identifies whether the physical interfaces, LMIs, and DLCIs are all enabled and active for this PVC connection.
	■ Active	■ The PVC is currently active. Both Source and Destination Statuses must be Active for the circuit to be active.
	■ Inactive	■ The PVC is inactive because: – Alarm conditions and network and SLV communication status indicate that data cannot be successfully transmitted. – The unit has disabled the interface or frame relay link due to internal operating conventions.
	■ Disabled	■ The PVC cannot be activated as a result of how the unit was configured. The PVC may be disabled at one or both ends of: – The physical interface, or – The frame relay link.
	■ Invalid	■ Some portion of the PVC connection is not fully configured.

Network Interface Status

Network Interface Status can be viewed from the Status menu.

Main Menu→Status→Network Interface Status

Network Interface Status Screen Example

```
main/status/network                                                  9788-SLV
Device Name: Node A                                          06/05/2001  06:04


                        NETWORK 1 INTERFACE STATUS

                Operating Rate(Kbps):      2312
                                                              Threshold
                Receiver Attenuation(dB):  5                      3
                SNR Margin(dB):            39.6                   3









--------------------------------------------------------------------------------
                           ESC for previous menu          MainMenu    Exit
 Refresh     PgUp   PgDn
```

Table 7-10. Network Interface Status

Field	Display	What It Indicates
Operating Rate (Kbps)	0–2320	The DSL line rate in Kbps.
	Disconnected	The line is disconnected.
Receiver Attenuation(dB)	0–255 in 1 dB increments	Loss of signal strength of the received DSL network signal, assuming the far end was transmitting at 13.5 dB.
	Disconnected	The line is disconnected.
SNR Margin(dB)	9783: –64 to +63.5 dB in 0.5 dB increments 9788: 0–15 dB in 1 dB increments	The amount of increased noise the system can tolerate on the DSL network interface without exceeding a Bit Error Rate of 10^{-7}.
	Disconnected	The line is disconnected.
Receiver Attenuation Threshold *(9788 only)*	0–255 in 1 dB increments	The Loop Attenuation Threshold value as defined in ITU 991.2.
SNR Margin Threshold *(9788 only)*	0–15 dB in 1 dB increments	The SNR Margin Threshold as defined in ITU 991.2.

IP Routing Table (Management Traffic)

Use the IP Routing Table for Management Traffic to see all management traffic IP routes configured in the FrameSaver unit.

Main Menu→ Status→ IP Routing Table (Management Traffic)

IP Routing Table Screen Example

```
main/status/ip_route                                                  9783-C-SLV
Device Name: Node A                                                2/26/2001  06:05

                                                                      Page 1 of 2
                        IP ROUTING TABLE fOR MANAGEMENT TRAFFIC

  Destination          Mask              Gateway        Hop  Type   Interface     TTL
135.001.001.000  255.255.255.000  135.026.001.254    1   Tmp    PVCMgmt1001   130
135.001.002.111  FFF.EEE.FFF.FFF  135.026.001.254    1   NMS    PVCMgmt1002   130
135.001.220.000  255.255.255.000  135.042.001.254    1   Loc    Ethernet      999
135.001.221.000  255.255.255.000  135.042.001.254    1   Loc    COM           999
135.001.220.000  255.255.255.000  135.042.001.254    1   Loc    COM           999
135.001.222.111  255.255.255.000  135.026.001.254    1   RIP    Ethernet      830
135.001.222.113  255.255.255.255  135.026.001.254    1   RIP    PVCMgmt1003   830
135.001.002.111  255.255.255.255  135.026.001.254    1   NMS    PVCMgmt1004   782
135.001.002.111  255.255.255.255  135.026.001.254    1   NMS    PVCMgmt1005   748
135.026.002.036  255.255.255.255  000.000.000.000    1   Tmp    Ethernet      690




--------------------------------------------------------------------------------
                                ESC for previous menu        MainMenu    Exit
 Refresh     PgDn   PgUp
```

Table 7-11, IP Routing Table Values is sorted by Destination IP address, from the lowest number to the highest. If no routes exist, the **No Routes** message appears instead of IP routing information.

Table 7-11. IP Routing Table Values

Field	What It Indicates
Destination	The Destination IP Address for the route: 000.000.000.000 – 223.255.255.255
Mask	The Destination Subnet Mask for the route: ■ 000.000.000.000–225.255.255.255 for network routes ■ FFF.FFF.FFF.FFF for host routes ■ 127 may also appear; this is a reserved number.
Gateway	The Gateway IP Address for the route: 000.000.000.000 – 223.255.255.255.
Hop	The number of hops in the route to the destination (1–15). If 16 appears, the route is in the process of being aged out.
Type	The method used to add the route to the table. ■ ICM: The route was added because an Internet Control Management Protocol (ICMP) redirect message was received from a router, indicating a better route to the destination. ■ Loc: The route was added due to the FrameSaver unit's local configuration, a Default IP Address, or an SNMP Manager Initial Route Destination have been configured. The route remains until the unit's configuration changes. ■ NMS: The route was added by a Network Management System using SNMP. The route remains until there is a power reset. ■ RIP: The route was discovered through Routing Information Protocol. The route remains until its TTL (Time to Live) expires, a better route is provided via RIP, or there is a power reset. ■ Tmp: The route was added as a temporary route in order to respond to an IP packet that was received. The route remains until the TTL expires or there is a power reset. ■ –: Source of the route is not maintained within the device.
Interface	Specifies the interface to be used to reach the destination. ■ COM: Communications port ■ Ethernet: Ethernet port ■ PVCMgmt*name*: Name and number of the management PVC ■ Internal: Interface to be used for software loopbacks or internal device functions in order to reach the destination
TTL	The Time to Live that was set for the route: 1–999 seconds

Performance Statistics

Use the Performance Statistics menu to display statistical information for a selected interface. Statistical information is useful when researching the severity and frequency or duration of a condition.

Main Menu→ Status→ Performance Statistics

Physical and link layer statistics (Layers 1 and 2) are collected on the interface. The following menu shows performance statistics that can be selected.

Performance Statistics Menu

```
main/status/performance                                              978x-SLV
Device Name: Node A                                          6/05/2001  06:06

                          PERFORMANCE STATISTICS


                             Service Level Verification
                             DLCI
                             Frame Relay
                             ATM
                             VCC
                             xDSL Line (9788 only)
                             Ethernet
                             Clear All Statistics









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
```

Performance statistics counts continue to increment until the maximum value of (2^{32}–2) is reached, at which time, the count starts over. NextLink or PgDn and PrevLink or PgUp function keys appear when multiple displays are available.

Service Level Verification Performance Statistics

The statistics in Table 7-12, SLV Performance Statistics for Multiplexed DLCI, appear when Service Level Verification (SLV) is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics→ Service Level Verification

They only appear:

- For the network interface
- If DLCIs are multiplexed or IP Enabled
- When the Advanced SLM Feature Set is activated

Information displayed on the SLV Performance Statistics screen depends on DLCI type. See Table 7-12, SLV Performance Statistics for Multiplexed DLCI or Table 7-13, SLV Performance Statistics for IP Enabled DLCI.

On either screen, select PrevDLCI or NextDLCI to view statistics for the previous or next DLCI on the link. On the IP Enabled DLCI screen, select PrevPath or NextPath to view statistics for the previous or next path associated with the DLCI.

For standard or multiplexed DLCIs, the statistics collected by the unit depend upon the device at the far end of the connection. If the far-end device is a FrameSaver SLV unit, frame relay, latency, and FDR/DDR performance statistics are collected. The Frame Relay Delivery Ratio is the number of delivered frames/offered frames; the Data Delivery Ratio is the number of delivered octets/offered octets.

If the far-end device is a non-FrameSaver device, or a FrameSaver 9120 or 9620, only frame relay statistics are collected.

Table 7-12. SLV Performance Statistics for Multiplexed DLCI (1 of 3)

Statistic	What It Indicates
Far End Circuit	Number of the multiplexed DLCI or VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) at the other end of the connection. If the far-end circuit is a DLCI, the DLCI number (16–1007) appears. If a VPI/VCI, the number is displayed as *xx,yyy, xx* being the VPI number (0–15) and *yyy* being the VCI number (32–2047). **None** appears if the unit has not communicated with the other end.
Far End IP Addr	IP Address of the device at the other end of the multiplexed DLCI connection. **None** appears if the FrameSaver unit has not communicated with the other end, or if the device at the other end of the multiplexed DLCI does not have an IP Address configured.
Dropped SLV Responses	The number of SLV inband sample messages sent for which a response from the far-end device has not been received.

Table 7-12. SLV Performance Statistics for Multiplexed DLCI (2 of 3)

Statistic	What It Indicates
Inbound Dropped Frames	Total number of frames transmitted by the far-end device that were dropped in transit. This count continues to accumulate until the maximum count value has been reached, then the count is reset and starts to accumulate dropped frames again. The counts continue to increment until the maximum value is reached (2^{32}–2), then the count starts over. The SLV Delivery Ratio option (see Table 4-5, Service Level Verification Options) must be enabled for these statistics to appear.
■ Above CIR	■ The number of frames transmitted by the far-end device that were above the committed information rate and were dropped in transit.
■ Within CIR	■ The number of frames transmitted by the far-end device that were within the committed information rate, but were dropped in transit.
■ Between CIR&EIR	■ The number of frames transmitted by the far-end device that were between the committed information rate and excess information rate, and were dropped in transit.
■ Above EIR	■ The number of frames transmitted by the far-end device that were above the excess information rate and were dropped in transit.
Inbound Dropped Characters	Total number of bytes transmitted by the far-end device that were dropped in transit. The counts continue to increment until the maximum value is reached (2^{32}–2), then the count starts over. The SLV Delivery Ratio option (see Table 4-5, Service Level Verification Options) must be enabled for these statistics to appear. **NA** appears instead of a statistical count if FDR/DDR (Frame Delivery Ratio/Data Delivery Ratio) information is not being received from the far-end device . This count continues to accumulate until the maximum count value has been reached, then the count is reset and starts to accumulate dropped characters again.
■ Above CIR	■ The number of bytes transmitted by the far-end device that were above the committed information rate and were dropped in transit.
■ Within CIR	■ The number of bytes transmitted by the far-end device that were within within the committed information rate, but were dropped in transit.
■ Between CIR&EIR	■ The number of bytes transmitted by the far-end device that were between the committed information rate and excess information rate, and were dropped in transit.
■ Above EIR	■ The number of bytes transmitted by the far-end device that were above the excess information rate and were dropped in transit.

Table 7-12. SLV Performance Statistics for Multiplexed DLCI (3 of 3)

Statistic	What It Indicates
Latest RdTrip Latency	Current round trip latency, measured in milliseconds, between the FrameSaver unit and the device at the other end of the multiplexed DLCI connection. "--" appears if communication with the far-end device is not successful.
Avg RdTrip Latency	Average round trip latency, measured in milliseconds, between the FrameSaver unit and the device at the other end of the multiplexed DLCI connection. Average round trip latency is measured every SLV sampling interval and the average is computed (using packets with the configured SLV Packet Size (bytes), Table 4-5, Service Level Verification Options) over the previous 15 samples. If SLV Packet Size is changed, a new average is not available until a new sample has been received. "--" appears if communication with the far-end device over the last 15 samples has not been successful.
Max RdTrip Latency	Same as average (Avg RdTrip Latency), but storing the maximum value of latency over the previous 15 samples. "--" appears if communication with the far-end device over the last 15 samples has not been successful.

For an IP Enabled DLCI, statistics are shown for last, minimum, average, and maximum round trips, and for dropped SLV responses, for each of the seven classes of service.

Table 7-13. SLV Performance Statistics for IP Enabled DLCI (1 of 2)

Statistic	What It Indicates
Far End IP Addr	IP Address of the device at the other end of the DLCI connection. **None** appears if the FrameSaver unit has not communicated with the other end, or if the device at the other end of the DLCI does not have an IP Address configured.
Path Up Time	The number of days, hours, minutes, and seconds since the last transition of this DLCI from Inactive to Active.
Far End Circuit	Number of the DLCI at the other end of the connection. **None** appears if the unit has not communicated with the other end.
SLM Poll Type	The role played by the far-end FrameSaver in the collection of latency and availability statistics. **Initiator** – The far-end FrameSaver initiates the SLV packet used for statistics collection. **Responder** – The far-end FrameSaver returns the SLV packet sent by the Initiator.

Table 7-13. SLV Performance Statistics for IP Enabled DLCI (2 of 2)

Statistic	What It Indicates
Far End Name	The system name configured for the far-end FrameSaver device, obtained using its IP address. **Unknown** appears if the far end device is not a FrameSaver or if no response has been received since the last reset.
COS Type Mismatches	The number of SLV packets received that indicate a mismatch between the Class of Service definitions in the near-end and far-end devices.
Far End Type	The model type of the far-end FrameSaver device, obtained using its IP address. **Unknown** appears if the far end device is not a FrameSaver or if no response has been received since the last reset.
COS Name	The names for different Classes of Service defined using the Class of Service Definitions screen. See *Configuring Class of Service Definitions* in Chapter 4, *Configuration Options*.
COS ID	The ID numbers (1–7) of the Class of Service definitions.
Last RdTrip	Current round trip latency, measured in milliseconds, between the FrameSaver unit and the device at the other end of the DLCI connection. "--" appears if communication with the far-end device is not successful.
Min RdTrip	Minimum round trip latency measured over the last 15 samples between the FrameSaver unit and the device at the other end of the DLCI connection. "--" appears if communication with the far-end device over the last 15 samples has not been successful.
Avg RdTrip	Average round trip latency between the FrameSaver unit and the device at the other end of the DLCI connection. Average round trip latency is measured every SLV sampling interval and the average is computed (using packets with the configured SLV Packet Size, as shown in Table 4-5, Service Level Verification Options) over the previous 15 samples. If SLV Packet Size is changed, a new average is not available until a new sample has been received. "--" appears if communication with the far-end device over the last 15 samples has not been successful.
Max RdTrip	Same as average (Avg RdTrip), but storing the maximum value of latency over the previous 15 samples. "--" appears if communication with the far-end device over the last 15 samples has not been successful.
Dropped SLV Responses	The number of SLV inband sample messages sent for which no response from the far-end device has been received.

DLCI Performance Statistics

Access DLCI statistics from the Performance Statistics menu.

Main Menu → *Status* → *Performance Statistics* → *DLCI*

One page of DLCI performance statistics appear for each enabled frame relay link that has at least one DLCI. Link names may include:

- Net*n*-FR*n*: frame relay link
- Rtr-S0: DSL router's Serial port 0
- Port-1: Data port frame relay link

Table 7-14. DLCI Performance Statistics (1 of 2)

Field	What It Indicates
DLCI	Displays the DLCI for the selected frame relay link. Use the spacebar to cycle through the DLCI list. DLCI list may include: ■ 16–1007: DLCI number ■ Net1-ATM: Appears when the DLCI is configured on a VCC ■ 0–15, 32–255: The VPI,VCI numbers display when the DLCI is configured on a VCC
DLCI Up Since	Date/time the DLCI was declared Active after a period of inactivity. ■ Down is displayed if the DLCI is inactive. ■ If the DLCI was Down, this is the time that the DLCI recovered. ■ If the DLCI was never Down, this is the first time the unit discovered that the DLCI was active in the network.
DLCI Up Time	Days, hours, minutes, and seconds since the DLCI was last declared Active after a period of inactivity. ■ Down is displayed if the DLCI is inactive. ■ If the DLCI was Down, this is the time since the DLCI recovered. ■ If the DLCI was never Down, this is the amount of time since the unit discovered that the DLCI was active in the network.
Total Tx Frames/ Tx Octets	Total number of data frames and octets (8-bit bytes) transmitted for the selected frame relay link DLCI. The number of frames and octets:
■ Within CIR *	■ Received on the DLCI that were within the CIR.
■ Between CIR&EIR *	■ Sent by the far-end device that were between the committed information rate and excess information rate.
■ Above EIR *	■ Sent by the far-end device on the DLCI that were above the EIR.
■ With DE Set	■ Sent on the DLCI with the discard eligible bit set.
■ With BECN Set	■ BECNs sent to notify users that there is data traffic congestion in the opposite direction of the frame carrying the BECN indicator.

Table 7-14. DLCI Performance Statistics (2 of 2)

Field	What It Indicates
Total Rx Frames/ Rx Octets	Total number of data frames and octets (8-bit bytes) received for the selected DLCI on the frame relay link. The number of frames and octets received on the selected DLCI:
■ Within CIR *	■ That were within CIR.
■ Between CIR&EIR *	■ That were between CIR and EIR.
■ Above EIR *	■ That were above EIR.
■ With DE Set	■ With the discard eligible bit set.
■ With BECN Set	■ BECNs sent to notify users of data traffic congestion in the opposite direction of the frame carrying the BECN indicator.
■ With FECN Set	■ FECNs sent to notify users of data traffic congestion in the same direction of the frame carrying the FECN indicator.

* Advanced SLM Feature Set only.

Additional Performance Statistics for IP Enabled DLCI

If the selected DLCI is IP Enabled, the DLCI Performance Statistics screen has a second page listing statistics by Class of Service. On the first DLCI Performance Statistics page for an IP Enabled DLCI, PgUp and PgDn are shown as available commands in the function keys area of the screen. Select PgUp or PgDn to display the second page.

Table 7-15. Additional Performance Statistics for IP Enabled DLCI

Statistic	What It Indicates
Class of Svc Name	The names for different Classes of Service defined using the Class of Service Definitions screen. See *Configuring Class of Service Definitions* in Chapter 4, *Configuration Options*.
Class of Svc ID	The ID numbers (1–7) of the Class of Service definitions.
The following IP statistics are shown for: ■ The seven Classes of Service ■ **Unknown COS** – IP packets whose Type of Service values do not match those defined for any Class of Service ■ **Non-IP** – Packets that were not IP Version 4 ■ **Total** – The total for all packets	
Tx Packets	The number of packets transmitted
Tx Octets	The number of octets in the packets transmitted
Rx Packets	The number of packets received
Rx Octets	The number of octets in the packets received
Rx Errors	The number of packets received in error

Frame Relay Performance Statistics

Access frame relay statistics from the Performance Statistics menu.

Main Menu → *Status* → *Performance Statistics* → *Frame Relay*

Performance statistics are only displayed for enabled frame relay links. Link names may include:

- Net*n*-FR*n*: frame relay link
- Port-1: DSL CSU/DSU's user data port number
- Rtr-S0: DSL router's Serial port 0

Table 7-16. Frame Relay Performance Statistics (1 of 2)

Statistic	What It Indicates
Frame Relay Link	
Frames Sent	Number of frames sent over the frame relay interface.
Frames Received	Number of frames received over the interface.
Characters Sent	Number of data octets (bytes) sent over the interface.
Characters Received	Number of data octets (bytes) received over the interface.
FECNs Received	Number of FECNs received due to data traffic congestion in the same direction of the frame carrying the FECN indicator.
BECNs Received	Number of BECNs received due to data traffic congestion in the opposite direction of the frame carrying the BECN indicator.
Frame Relay Errors	
Total Errors	Total number of frame relay errors includes short frames, long frames, invalid DLCIs, unknown DLCIs, and unknown errors. This number does not include LMI errors. There may be a non-frame relay device on the other end of the link, or the units at either the far-end or both ends of the link may be configured incorrectly.
Invalid Rx Frames	Number of invalid frames received over the interface. There is a non-frame relay device on the other end of the link.
Short Rx Frames	Number of frames received over the interface that were less than 5 octets in length. The device on the far end of the link may be configured incorrectly.
Long Rx Frames	Number of frames received over the interface that were more than 8196 octets in length. The device on the far end of the link may be configured incorrectly.
Invalid DLCI	Number of frames sent to invalid DLCIs (not 16–1007).
Unknown DLCI	Number of frames received for unknown DLCIs.
Unknown Error	Number of frames received that do not fall into one of the other statistic categories. The unit cannot recognize the error.

Table 7-16. Frame Relay Performance Statistics (2 of 2)

Statistic	What It Indicates
Frame Relay LMI *(CSU/DSUs only)*	
LMI Protocol	The LMI protocol configured for the frame relay link. Normal condition.
Status Msg Received	Number of LMI status messages received over the interface. Normal condition.
Total LMI Errors	Number of LMI errors, including reliability errors, protocol errors, unknown report types, unknown information elements, and sequence errors.
Number of Inactives	Number of times the LMI has declared the frame relay link Inactive.
Frame Relay HDLC Errors	
Rx Total Errors	Total number of errors received on the interface, including: ■ Receive invalid frames (short frames, long frames, invalid DLCIs, unknown DLCIs, and unknown errors) ■ Rx Total Discards ■ Receive errors (non-octet aligned frames, frames with CRC errors, and Rx Overruns)
Rx Total Discards	Total number of discards received on the interface, including: ■ Resource errors ■ Rx Overruns ■ Frames received when the link was down ■ Inactive and disconnected DLCIs ■ Inactive destination DLCIs ■ Unknown EDLCIs
Rx Overruns	Number of Overruns received.
Rx Non-octet Frames	Number of Non-Octet frames received.
Rx CRC Errors	Number of Cycle Redundancy Check (CRC) errors received.
Tx Total Errors	Total number of errors transmitted on the interface, including transmit discards and transmit overruns.
Tx Total Discards	Total number of discards transmitted on the interface, including underrun flushes.
Tx Underruns	Number of underruns transmitted.

ATM Performance Statistics (9783, 9788)

Access Asynchronous Transfer Mode (ATM) statistics from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → ATM

ATM link, Net1-ATM, must be enabled for these statistics to appear.

Table 7-17. ATM Performance Statistics

Statistic	What It Indicates
AAL5 (ATM Adaption Layer)	
Tx PDUs	Number of AAL5 Common Part Convergence Sublayer (CPCS) Protocol Data Units (PDUs) passed to the lower layer for transmission.
Rx PDUs	Number of AAL5 PDUs received and passed to a higher layer.
Tx Octets	Number of AAL5 octets (bytes) passed to the lower layer for transmission.
Rx Octets	Number of AAL5 octets (bytes) received and passed to a higher layer.
Errored Tx PDUs	Number of AAL5 PDUs that could not be transmitted due to errors.
Errored Rx PDUs	Number of AAL5 CPCS PDUs received that contained errors.
OAM (Operations, Administration, and Maintenance)	
Total Tx OAM Cells	Number of OAM cells transmitted.
Total Rx OAM Cells	Number of OAM cells received.
TC (Transmission Convergence) Sublayer	
Total Tx Cells	Number of cells transmitted.
Total Rx Cells	Number of cells received.
Total Rx Cells Dropped	Number of cells received and dropped due to errors.
Rx HEC Errors	Number of cells received with HEC field errors.
Unknown Rx Cells	Number of cells received and discarded during cell header validation. These include cells with: ■ Unrecognized VPI/VCI values. ■ Invalid cell header patterns. ■ Undefined Payload Type Indicators.
Last Unknown VPI,VCI	The VPI,VCI of the last cell discarded due to an unrecognized VPI,VCI. If no such cells have been discarded, **None** appears.
OCD Events	Number of times OCD events have been detected (when seven consecutive cells with HEC violations are detected).
Cell Delineation State	Synchronization value (In Sync or Out of Sync) of the last cell received.

VCC Performance Statistics (9783, 9788)

Access Virtual Channel Connection (VCC) statistics from the Performance Statistics menu.

Main Menu → *Status* → *Performance Statistics* → *VCC*

ATM link, Net1-ATM, must be enabled and have at least one VCC for these statistics to appear.

Select a VPI,VCI. Format: VPI,VCI (Net*n*-FR*n*, DLCI)

- VPI: 0–15,
  VCI: 32–255
- Net*n*-FR*n*: frame relay link
- 16–1007: DLCI number

Table 7-18. VCC Performance Statistics (1 of 2)

Statistic	What It Indicates
VCC (Virtual Channel Connection)	
Tx Cells	Number of cells transmitted on the link for the VCC.
Rx Cells	Number of cells received on the link for the VCC.
Tx PDUs	Number of AAL5 Common Part Convergence Sublayer (CPCS) Protocol Data Units (PDUs) received from a higher layer for transmission.
Rx PDUs	Number of AAL5 PDUs received and passed to a higher layer.
Tx Octets	Number of AAL5 octets transmitted on the VCC.
Rx Octets	Number of AAL5 octets received on the VCC.
Errored Rx PDUs	Number of AAL5 PDUs received that contained errors. Errors include CRC-32 errors, SAR timeout errors, and oversized errors.
OAM (Operations, Administration, and Maintenance)	
Total Tx OAM Cells	Number of OAM cells transmitted on the VCC.
Total Rx OAM Cells	Number of OAM cells received on the VCC.
Tx Segment Loopback Cells	Number of OAM segment loopback cells transmitted on the VCC.
Rx Segment Loopback Cells	Number of OAM segment loopback cells received on the VCC.
Tx EndToEnd Loopback Cells	Number of OAM end to end cells transmitted on the VCC.
Rx EndToEnd Loopback Cells	Number of OAM end to end cells received on the VCC.
Tx AIS Cells	Number of OAM F5 Alarm Indication Signal (AIS) cells transmitted on the VCC.

Table 7-18. VCC Performance Statistics (2 of 2)

Statistic	What It Indicates
Rx AIS Cells	Number of OAM F5 AIS cells received on the VCC.
Tx RDI Cells	Number of OAM F5 Remote Defect Indication (RDI) cells transmitted on the VCC.
Rx RDI Cells	Number of OAM F5 RDI cells received on the VCC.

SHDSL Line Performance Statistics (9788)

Access SHDSL statistics from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → xDSL Line

These statistics account for all traffic on the DSL line.

Table 7-19. SHDSL Line Performance Statistics

Statistic	What It Indicates
CRC Anomalies (CV)	The number of CRC errors, also known as Code Violations (CVs), that occurred during the accumulation period.
Errored Seconds (ES)	Number of one-second intervals during which at least one CRC anomaly or LOSW defect is declared.
Severely Errored Seconds (SES)	Number of one-second intervals during which at least 50 CRC anomalies are declared or at least one LOSW defect is declared.
LOSW Seconds (LOSWS)	Number of one-second intervals during which at least one SHDSL Loss of Synchronization Word (LOSW) defects is declared.
Unavailable Seconds (UAS)	Number of one-second intervals during which the SHDSL line is unavailable. The line is declared unavailable after 10 contiguous Severely Errored Seconds, and declared available after 10 contiguous seconds with no SES.

Ethernet Performance Statistics

Access Ethernet port statistics from the Performance Statistics menu.

Main Menu → *Status* → *Performance Statistics* → *Ethernet*

These statistics account for all traffic on the Ethernet port.

Table 7-20. Ethernet Performance Statistics

Statistic	What It Indicates
Port Rate (Mbps)	Operating rate as detected on the Ethernet port. One of the following may appear for this statistic: ■ Disconnected – The line is not connected. ■ 10 Mbps or 100 Mbps – The Ethernet port's operating rate. ■ Disabled – The Ethernet port has been disabled.
Duplex	Duplex mode detected on the Ethernet port. One of the following may appear for this statistic: ■ Disconnected – The line is not connected. ■ Full – Ethernet port is operating in full-duplex mode (4-wire). ■ Half – Ethernet port is operating in half-duplex mode (2-wire). ■ Disabled – Ethernet port has been disabled.
Frames Transmitted	Number of successfully transmitted frames on the port.
Frames Received	Number of frames received on the port.
Errored Frames	Number of errors detected on the port. Possible errors include: ■ Alignment errors ■ Internal transmit and receive errors ■ Long frames ■ Receive checksum errors ■ Transmitter and receiver overruns
Excessive Collisions	Number of failed frame transmissions due to excessive collisions.
Carrier Sense Errors	Number of times the carrier sense condition was lost or was never asserted during frame transmissions.
Deferred Transmissions	Number of delayed first transmissions due to the line being busy.

Clearing Performance Statistics

Performance statistics counters can be reset to the baseline when using a directly-connected asynchronous terminal and your security Access Level is Level-1. This feature is useful when troubleshooting problems.

Statistic counters are not actually cleared using this feature, since true statistic counts are always maintained to verify SLAs and to be available to view from an SNMP NMS. Statistics viewed via the menu-driven user interface may be different from those viewed from the NMS, because statistics can be locally cleared.

▶ Procedure

To clear all statistics:

Main Menu→ Status→Performance Statistics → Clear All Statistics

▶ Procedure

To clear specific sets of statistics:

- To reset the SLV and DLCI performance statistic counters for the currently displayed DLCI, use the ClrSLV&DLCIStats function key from one of the following screens:

  Main Menu→ Status→Performance Statistics→
  Service Level Verification

  Main Menu→ Status→Performance Statistics → DLCI

- To reset frame relay link performance statistics, use the ClrLinkStats function key.

  Main Menu→ Status→Performance Statistics→ Frame Relay

- To reset Ethernet performance statistics, use the ClrStats function key.

  Main Menu→ Status→Performance Statistics→ Ethernet

Trap Event Log

The Trap Event Log displays all traps stored in the SNMP trap event log. The following log example describes the alarm conditions that will generate an SNMP trap for a physical interface, and for the frame relay LMIs and DLCIs. These alarm conditions also generate Health and Status messages seen on the System and Test Status screen.

Main Menu→ Status → Trap Event Log

Trap Event Log Screen Example

```
main/status/event_log                                              9783-C-SLV
Device Name: Node A                                          09/11/2002 23:32
                                TRAP EVENT LOG
                                                      Total Trap Events:  535

 Time of Day                          Event
09/09/02 21:21:20 Change in Frames Discarded due to Inbound Resource Errors on
                  Sync Data Port S01P1 frame relay link "Port-1" exceeded
                  threshold of 1 by 105.
09/09/02 23:59:59 Change in Total LMI Errors on Network DSL frame relay link
                  "Net1-FR1" exceeded threshold of 1 by 59.
09/09/02 23:59:59 DLCI 101 of Sync Data Port S01P1 frame relay link "Port-1" up.
09/09/02 23:59:59 DLCI 101 of Sync Data Port S01P1 frame relay link "Port-1"
                  down.
09/10/02 00:41:02 Primary clock failed.
09/10/02 00:59:59 Sync Data Port S01P1 frame relay link "Port-1" LMI down.
09/10/02 01:00:02 Network DSL frame relay link "Net1-FR1" LMI down.
09/10/02 01:00:02 Network DSL down.
09/10/02 01:03:23 Unit reset.


--------------------------------------------------------------------------------
                                ESC for previous menu        MainMenu    Exit
 Refresh     PgUp   PgDn
```

Up to 12 trap events can be displayed on a screen with the most current displayed first. Page down (PgDn) to view less current trap events. When no trap events have been logged, **`No Events in Log`** appears in the Event column.

ASCII trap strings used to describe trap events are provided in the tables contained in *Standards Compliance for SNMP Traps* in Appendix B, *SNMP MIBs, Traps, and RMON Alarm Defaults*.

FTP File Transfers

FrameSaver devices support a standard File Transfer Protocol (FTP) server over Transmission Control Protocol (TCP). To provide backup, a complete binary image of the configuration files can be copied to a host. To use this feature, the unit must be configured to support Telnet and FTP Sessions.

Using this feature, you can transfer configuration files **to/from** a FrameSaver node, program files **to** a FrameSaver node, and User History data **from** a FrameSaver node through the user data port (CSU/DSU only) or the network interface using a management PVC, or through the COM port.

Be aware of the following rules when doing a file transfer:

- You must have Access Level 1 permission to use the **put** and **get** commands. However, you can retrieve the data file for user history reports, regardless of your access level.
- You cannot **put** a configuration file to the factory.cfg or current.cfg files under the system directory. Configuration files should be put to a customer file (cust1.cfg or cust2.cfg), then loaded into the downloaded unit's Current Configuration via the menu-driven user interface.
- You can only **put** a NAM program file (nam.ocd) into a FrameSaver unit. You cannot **get** a program file from the FrameSaver unit to a host.
- Before you **put** a download file, you must use the **bin** binary command to place the data connection in binary transfer mode.
- When transferring SLV user history information to the NMS, you can only **get** a uhbcfull.dat file. It is recommended that you use the NMS application to get this information (see *Transferring Collected Data* on page 7-48).
- A data file (uhbcfull.dat or lmitrace.syc) cannot be **put** into a FrameSaver node.
- LMI packet capture data (lmitrace.syc) is not readable when the LMI Packet Capture Utility is active.
- The SLV user history file is only available to units with the SLV feature set.

To eliminate operation interruptions, FrameSaver SLV devices provide an additional feature that allows new software to be downloaded in the background, using the selected bandwidth and without interfering with normal operation. Downloads can be performed quickly, using the full line speed, or at a slower rate over an extended period of time.

Initiating an FTP Session

Initiate an FTP session to a FrameSaver node in the same way you would initiate an FTP to any other IP-addressable device.

NOTE:

Loading a configuration with many DLCIs from option area Customer Configuration 1 or 2 into the Current Configuration area takes time. Allow a minute or more for the downloaded file to be put into the unit's currently active configuration.

▶ Procedure

To initiate an FTP session:

1. Start the FTP client program on the host. For example, on a UNIX host, type **`ftp`**, followed by the FrameSaver unit's IP address.
2. If a login and password are required (see *Creating a Login for the User Interface* in Chapter 6, *Security and Logins*), you are prompted to enter them. If not, press Enter.

   The FTP prompt appears.

   The starting directory is the root directory (/). Use standard FTP commands during the FTP session, as well as the following remote FTP commands.

Command	Definition
bin	Places the FTP session in binary-transfer mode.
cd *directory*	Change the current directory on the FrameSaver node to the specified *directory*.
dir [*directory*]	Print a listing of the directory contents in the specified *directory*. If no directory is specified, the current one is used.
get *file1* [*file2*]	Copy a file from the remote directory of the FrameSaver node to the local directory on the host (for configuration files only).
ls [*directory*]	Print an abbreviated list of the specified directory's contents. If no directory is specified, the current one is used.
put *file1* [*file2*]	Copy *file1* from a local directory on the host to *file 2* in the current directory of the FrameSaver node. If *file2* is not specified, the file will be named *file1* on the FrameSaver node.
recv *file1* [*file 2*]	Same as a **get**.
remote or help [*command*]	Print the meaning of the command. If no argument is given, a list of all known commands is printed.
send *file1* [*file 2*]	Same as a **put**.

Upgrading System Software

If you need to upgrade the FrameSaver unit's program code, you need to download the software into the Alternate Release directory. Upgrades can be performed through the:

- Network using a Management PVC, or
- COM port, if Port Use is set to Net Link (see Table 4-25, Communication Port Options)

▶ Procedure

To download software:

1. Initiate an FTP session to the device that you are upgrading.
2. Type **bin** to enter binary transfer mode.
3. Type **hash** to enter hash mode if you want to monitor the progress of the upgrade, provided this function is supported by your equipment.
4. Type **cd system** to change to the system directory.
5. Perform a **put** of R*xxxxxx*.ocd (*xxxxxx* being the software release number) to the nam.ocd file to start the upgrade.

If the message displayed is . . .	Then . . .
nam.ocd: File Transfer Complete	The download was successful. The file is loaded into system memory.
nam.ocd: File Transfer Failed – Invalid file	The file is not valid for this FrameSaver unit. A different R*xxxxxx*.ocd file will need to be downloaded. Repeat the step or end the FTP session.

NOTE:

During the download, a series of hash marks (#) appear. When the hash marks stop appearing, there is a pause of about 30 seconds before the **`nam.ocd: File Transfer Complete`** message appears. Please be patient. Do not exit from FTP at this time.

See *Activating Software* on page 7-47 to activate the newly downloaded software.

Determining Whether a Download Is Completed

To verify download completion, check the Identity screen.

Main Menu→Status→Identity

Check Alternate Software Rev. under the NAM Identity column.

- If a software revision number appears, the file transfer is complete.
- If **`In Progress`** appears, the file is still being transferred.
- If **`Invalid`** appears, no download has occurred or the download was not successful.

See *Activating Software* to activate the newly downloaded software.

Activating Software

Once a software upgrade is downloaded to the Alternate Release location, it needs to be activated. When activated, the unit resets and then moves the downloaded software to the Current Firmware location. With this feature, you control when the upgrade software is implemented.

▶ Procedure

To switch to the new software:

1. Go to the Control menu and locate Select Software Release:

   Main Menu→Control→Select Software Release

   The currently loaded software version and the new transferred software release are shown.

   If the download failed, **`Invalid`** appears in the Alternate Release field instead of the new release number. Repeat the procedure in *Upgrading System Software* on page 7-46 if this occurs.

2. Select Switch&Reset.
3. Enter Yes to the **`Are you sure?`** prompt. The unit resets and begins installing the newly transferred software.
4. Verify that the new software release was successfully installed as the Current Software Revision.

   Main Menu→Status→Identity

   NOTE:

   If someone opens a Telnet session and accesses the unit's Identity screen while the unit is downloading software, the **`In Progress...`** message appears in the Alternate Software Revision field.

   See *Displaying Identity System Information* on page 7-2 to see what is included on the unit's Identity screen.

Transferring Collected Data

SLV user history statistics and LMI packet capture data can be uploaded to an NMS or a Network Associates Sniffer using FTP, which is faster than other methods. The rate at which the data file is transferred is the rate set by the FTP Max Transfer Rate (Kbps) option (see Table 4-21, Telnet and FTP Session Options, in Chapter 4, *Configuration Options*).

NOTES:

— Use your NMS application to FTP and view transferred statistics and packet data; the data files are not in user-readable format. LMI packet capture data can also be viewed via the LMI Trace Log (see *Viewing LMI Captured Packets from the User Interface* in Chapter 8, *Troubleshooting*, for additional information).

— Uploading SLV user history statistics is only available to units with Advanced SLM Feature Set activated.

▶ Procedure

To retrieve data:

1. Initiate an FTP session to the device from which SLV statistics or packet data will be retrieved.
2. Type **bin** to enter binary transfer mode.
3. Type **hash** to enter hash mode if you want to monitor the progress of the upgrade, provided this function is supported by your equipment.
4. Type **cd data** to change to the data directory.

If retrieving . . .	Then . . .
SLV statistics	Perform a **get** of the **uhbcfull.dat** file. ■ **`File Transfer Complete`** – Transfer was successful. ■ **`File Transfer Failed`** – Transfer was not successful. Try again or end the session.
LMI packet capture data	1. Stop the LMI Packet Capture Utility. *Main Menu→Control→LMI Packet Capture Utility* LMI packet capture data is not available (readable) when the LMI Packet Capture Utility is Active. 2. Perform a **get** of the **lmitrace.syc** file. One of the following will display for the file: – **`File Transfer Complete`** – **`File Transfer Failed`** – **`Permission Denied`** – The LMI Packet Capture Utility was not readable. Stop the LMI Packet Capture Utility and try again.

5. Close the FTP session.

SLV statistics and/or LMI Packet Capture data are now available for reporting.

Troubleshooting

8

This chapter includes the following:

Problem Indicators

The device provides a number of indicators to alert you to possible problems.

Indicators . . .	**See . . .**
LEDs	*Viewing LEDs and Control Leads* in Chapter 7, *Operation and Maintenance,* and the user interface screen. *Main Menu→Status→Display LEDs and Control LEDs*
Health and status	*Health and Status Messages* in Chapter 7, *Operation and Maintenance.* Messages appear at the bottom of any menu-driven user interface screen. *Main Menu→Status→System and Test Status*
Device messages	*Device Messages* in Chapter 7, *Operation and Maintenance*. Messages appear at the bottom of any menu-driven user interface screen.
Performance statistics	*Performance Statistics* in Chapter 7, *Operation and Maintenance*, to determine how long a problem has existed.
Alarm conditions	*Alarms* on page 8-8.
SNMP traps	Appendix B, *SNMP MIBs, Traps, and RMON Alarm Defaults*.

Resetting the Unit and Restoring Communication

You can reset the unit in one of four ways:

- Reset it from the Control menu.
- Cycle the power.
- Reset the configuration options for the COM port, or reload the factory default settings.
- Set the appropriate MIB object from NMS (refer to your NMS documentation).

The unit performs a self-test when it is reset.

Resetting the Unit from the Control Menu

Use this procedure to initiate a reset and power-on self-test of the unit.

▶ Procedure

To reset the unit from the Control menu:

1. From the Main Menu screen, select Control.
2. Select Reset Device and press Enter. The **`Are You Sure?`** prompt appears.
3. Type **y** (Yes) and press Enter. The unit reinitializes itself, performing a self-test.

Resetting the Unit By Cycling the Power

Disconnecting, then reconnecting the power cord resets the unit.

Restoring Communication with an Improperly Configured Unit

Configuring the unit improperly could render the menu-driven user interface inaccessible. If this occurs, connectivity to the unit can be restored via a directly connected asynchronous terminal.

▶ Procedure

To reset COM port settings:

1. Configure the asynchronous terminal to operate at 19.2 Kbps, using character length of 8 bits, with one stop-bit, and no parity. In addition, set Flow Control to None.
2. Reset the unit, then hold the Enter key down until the System Paused screen appears. (See *Resetting the Unit and Restoring Communication* on page 8-3 for other methods of resetting the unit.)
3. Tab to the desired prompt, and type **y** (Yes) at one of the prompts.

If selecting . . .	The following occurs . . .
Reset COM Port usage	■ Port Use is set to Terminal so the asynchronous terminal can be used. ■ Data Rate (Kbps), Character Length, Stop Bits, and Parity are reset to the factory defaults. ■ Unit resets itself.
Reload Factory Defaults	■ All configuration **and** control settings are reset to the Default Factory Configuration, overwriting the current configuration. ■ Unit resets itself. **CAUTION:** This causes the current configuration to be destroyed and a self-test to be performed.

If no selection is made within 30 seconds, or if No (**n**) is entered, the unit resets itself and no configuration changes are made.

Once the unit resets itself, connectivity is restored and the Main Menu screen appears.

Troubleshooting Management Link Feature

A dedicated troubleshooting management link is available to help service providers isolate device problems within their networks. This feature allows Telnet or FTP access to the unit on this link. Troubleshooting over this link is essentially transparent to customer operations. No alarms or SNMP traps are generated to create nuisance alarms for the customer.

See *Configuring Node IP Information* in Chapter 4, *Configuration Options*, for additional information about this feature.

LMI Packet Capture Utility Feature

The FrameSaver DSL CSU/DSU provides a packet capture utility to aid with problem isolation when LMI errors are detected. Using this utility, any enabled frame relay link on the user data port can be selected. The utility captures any LMI packets sent or received, and writes them to a data file called **lmitrace.syc** in the system's data directory so the data can be uploaded and transferred to a Network Associates Sniffer for analysis. This feature does not apply to the router.

The LMI Trace Log also provides access to captured packet information. See *Viewing LMI Captured Packets from the User Interface* on page 8-6 for additional information on this feature.

▶ Procedure

To use this utility:

1. Select the LMI Packet Capture Utility.

   Main Menu→Control→LMI Packet Capture Utility

2. In the first field, Capture Interface, select the enabled frame relay link, Port-1.
3. Start packet capture.

   While capturing data, the status is Active. Packets in Buffer indicates the number of packets that have been captured. Up to 8000 packets can be held. When the buffer is full, the oldest packets will be overwritten.

4. To stop the utility, press Enter. The field toggles back to Start.
5. Upload the data file holding the collected packets to a diskette so the information can be transferred to a Network Associates Sniffer for debugging/decoding.

See *Transferring Collected Data* in Chapter 7, *Operation and Maintenance*, for additional information about this feature.

Viewing LMI Captured Packets from the User Interface

The twelve most recent LMI events are stored in the trace log. Once the capture buffer or trace log is full, the oldest packets are overwritten. To view the most recently captured packets using the menu-driven user interface:

Control→LMI Packet Capture Utility→ Display LMI Trace Log

LMI Trace Log Example

```
main/control/lmi_capture/display_log                              9783-C-SLV
Device Name: Node A                                           2/26/2001 08:01

                              LMI TRACE LOG                     Page 1 of 3

Packets Transmitted to Net1-FR1          Packets Received from Net1-FR1
LMI Record #1 at 0 s
    Status Enquiry Message, 13 bytes
    LMI Type is Standard on DLCI 1023
    Sequence Number Exchange
    Send Seq #181, Rcv Seq #177
                                         LMI Record #2 at 0 s
                                             Status Enquiry Message, 13 bytes
                                             LMI Type is Standard on DLCI 1023
                                             Sequence Number Exchange
                                             Send Seq #181, Rcv Seq #177

--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu    Exit
 Refresh     PgUp   PgDn
```

Select Refresh to update the screen with the twelve most recently collected LMI messages.

The following information is provided for the LMI Trace Log:

- The internal LMI record number assigned to the packet (1–8000) and the amount of time the utility was running when the packet was captured.

  The maximum amount of time displayed is 4,294,967 **s** (seconds). The display is reset to 1 second when this amount of time is exceeded.

- The captured packet message, either Status Message or Status Enquiry Message and the number of packet bytes.

- The LMI Type identified in the Protocol Discriminator portion of the captured packet and the DLCI number for the packet.

- The type of information contained in the captured packet, either Sequence Number Exchange or Full Status Report.

- The Send and Receive (Rcv) sequence numbers from the captured packet (0–255).

- On the Packets Received side of the screen, PVC status for up to ten DLCIs can be shown; including the DLCI number, the active bit status, and if Standard LMI is running, the DLCI's CIR value.

Telnet

The Telnet feature allows you to initiate a Telnet session with a Telnet server on an IP aware device. Telnet is available with firmware release 2.1 and above:

Control→Telnet

Telnet Example

```
main/control/telnet                                                    9720
Device Name: Node A                                    09/11/2002 13:37

                                   TELNET

                  Target IP Address:     000.000.000.000  Clear
                  Destination Interface: Net1-FR1    DLCI: 1002

                  ---------------------------------------------------

                  Start    Escape Character is Ctrl-}

                  Status: Idle









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu    Exit
 Refresh     PgUp   PgDn
```

▶ Procedure

To initiate a Telnet session from the FrameSaver device:

1. Enter an IP address and select Use_Internal_Route, or select a destination interface (Net1-FR1 or Port-1).

   Clicking on Clear resets the IP address to 000.000.000.000.

2. Enter a DLCI, or, for ATM links, a VPI and VCI.
3. Click on Start. The prompt changes to Stop and the Telnet session is initiated.
4. The outbound data path is monitored for Ctrl-} (the Ctrl key pressed simultaneously with the } key). When you press Ctrl-}, the Telnet session is ended.

Alarms

The following table describes the alarm conditions that will generate an SNMP trap for a physical interface, and the frame relay LMIs and DLCIs. These alarm conditions also generate Health and Status messages seen on the System and Test Status screen. Major alarms are displayed on line 24 and force on the Alarm LED.

Main Menu→ Status →System and Test Status

Table 8-1. Alarm Conditions (1 of 3)

Alarm Condition	What It Indicates	What To Do
COS*x* Down, Path*IP_ Address,* DLCI*nnnn*[1]	A Class Of Service associated with a path is down.	Contact your service provider.
CTS down to Port-1 Device *(CSU/DSU only)*	The CTS control lead on the device's interface is off.	Check DTR and RTS from Port-1. ■ Verify that the port is enabled. ■ Check DTR for the user data port.
DLCI *nnnn* Down, Port-1 *(CSU/DSU only)*	The DLCI for Port 1 is down.	Contact your network service provider.
DSL Line Training Alarm at Network 1	The DSL interface is training.	Wait for training to complete.
DTR Down from Port-1 Device *(CSU/DSU only)*	The DTR control lead on the device connected to Port 1 is deasserted. The DTR control lead on the device connected to the specified port is off. This message applies to data ports that act as DCEs.	Examine the attached DTE and cable connected to the system's port. ■ Check that the port cable is securely attached at both ends. ■ Check the status of the attached equipment.
Ethernet Mgmt Down *(CSU/DSU only; minor alarm)*	The Ethernet management interface is down. The port is enabled and is the primary interface for management data, but communication between the management system and the unit is not possible.	Check the management system.
Ethernet Port Down *(Router only)*	The communication link for the Ethernet port is down and the Interface Status for the port is enabled.	Check the LAN connected to the Ethernet port.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

Table 8-1. Alarm Conditions (2 of 3)

Alarm Condition	What It Indicates	What To Do
LatExceed *IP_Address,* COS*x,*DLCI*nnnn*[1]	An IP SLV Latency Threshold has been exceeded for the specified Class Of Service of the path.	Contact your service provider.
Link Down Administratively *(CSU/DSU only; minor alarm)*	The DTE port is disabled through software.	Enable the port.
LMI Discovery in Progress *(CSU/DSU only; minor alarm)*	LMI protocol discovery is being performed.	Wait.
LMI Down, Port-1 *(CSU/DSU only)*	The Local Management Interface is down for the specified frame relay link.	For the user data port (not applicable to the router): ■ Check that the DTE cable is securely attached at both ends. ■ Verify that Transmit Clock Source and Invert Transmit Clock options are properly configured. ■ Verify that Frame Relay Performance Statistics show LMI frames being received. If no frames are being received: – Check the attached device. – Verify that the LMI Protocol setting reflects the LMI type being used.
Loop Attenuation Defect at Network 1 *(9788 only)*	The observed loop attenuation exceeds the configured threshold value.	Contact your network provider.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. ■ Network cable problem. ■ Network facility problem.	■ Check that the network cable is securely attached at both ends. ■ Contact your network provider.
Loss of Cell Delineation, *atm link*	The ATM Transmission Convergence (TC) layer has been in a Loss-of-Cell Delineation (LCD) state for one minute, or the number of Out-of-Cell Delineation (OCD) events has exceeded the user-specified threshold.	Contact your network provider.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

Table 8-1. Alarm Conditions (3 of 3)

Alarm Condition	What It Indicates	What To Do
LOSW Failure at Network 1 - hhh:mm:ss	Contiguous frames with LOSW defects have been detected for at least 2 seconds.	Contact your network provider.
Network Com Link Down *(minor alarm)*	The communication link for the COM port is down and the COM port is configured for Net Link.	Check the router connected to the COM port.
Path*IP_ Address* Down, DLCI*nnnn*[1]	A path on the network interface is unavailable.	Determine why the path went down.
Self-Test Failure	The unit did not pass its basic verification tests when it was powered on or reset.	■ Reset the unit. ■ Contact your service representative.
SLV Latency Exceeded, DLCI *nnnn*[1], Port-1	The measured latency of SLV communication responses from the remote unit on this DLCI is excessive, so the DLCI has been declared unsuitable for normal multiplexed PVC operation (DLCI Type is set to Multiplexed).	Wait until the DLCI is declared operational again.
SLV Timeout, DLCI *nnnn*[1], Port-1	An excessive number of SLV communication responses from the remote system have been missed on the specified multiplexed DLCI and link. When a hardware bypass-capable device has been detected at the other end of the PVC and this condition occurs, only user data for EDLCI 0 will be transmitted as long as the condition exists.	Verify that the network LMI is up. If it is, contact your network service provider.
SNR Margin Threshold Exceed, Network 1	The user-specified Signal-to-Noise Ratio (SNR) margin threshold for the network interface has been exceeded.	Contact your network provider.
Two Level-1 Users Accessing Device	Another user with Level-1 security access is currently accessing the unit. Be aware that actions of the other user may override your test commands and configuration changes.	Wait until no other Level-1 users are accessing the unit if testing or configuration will be performed.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

Viewing the Trap Event Log

The Trap Event Log displays all traps stored in the SNMP trap event log. ASCII trap strings used to describe trap events are provided in the tables contained in *Standards Compliance for SNMP Traps* in Appendix B, *SNMP MIBs, Traps, and RMON Alarm Defaults*.

See *Trap Event Log* in Chapter 7, *Operation and Maintenance*, for a screen example and additional information.

Troubleshooting Tables

The unit is designed to provide many years of trouble-free service. However, if a problem occurs, refer to the following tables for possible solutions.

- Table 8-2, Device Problems
- Table 8-3, ATM Problems
- Table 8-4, Frame Relay PVC Problems

Device Problems

Table 8-2. Device Problems

Symptom	Possible Cause	Solutions
Cannot access the unit or the menu-driven user interface.	Login/password is incorrect, COM port is improperly configured, or the unit is otherwise configured so it prevents access.	■ Reset the unit (see *Resetting the Unit and Restoring Communication* on page 8-3.) ■ Contact your service representative.
Failure *xxxxxxxx* appears at the top of the System and Test Status screen for Self-Test Results.	The unit has detected an internal software failure.	■ Record the 8-digit code from the System and Test Status screen. ■ Reset the unit and try again. ■ Contact your service representative and provide the 8-digit failure code.
No power or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle and the rear panel connector.	Check that the power cord is securely attached at both ends.
	The wall receptacle has no power.	■ Check the wall receptacle power by plugging in other working equipment. ■ Check the circuit breaker. ■ Verify that your site is not on an energy management program.
Power-On Self-Test fails. Only Alarm LED is on after power-on.	The unit has detected an internal hardware failure.	■ Reset the unit and try again. ■ Contact your service representative. ■ Return the unit to the factory (refer to *Warranty, Sales, Service, and Training Information* on page A of this document).
Receiving data errors on a multiplexed DLCI, but frame relay is okay.	Frame Relay Discovery is being used for automatic DLCI and PVC configuration. The equipment at the other end is not frame relay RFC 1490-compliant.	Change the DLCI Type for each network DLCI from Multiplexed to Standard, turning off multiplexing.

ATM Problems

Table 8-3. ATM Problems

Symptom	Possible Cause	Solutions
Out-of-Cell Delineation (OCD) events; loss of cell delineation.	Line impairments.	Check DSLAM statistics. Reduce the link rate.
The unit should be receiving data, but the ATM statistics indicate that the VCs are not receiving data.	The Virtual Circuit (VC) is improperly configured or not configured in the DSLAM.	Check DSLAM statistics. Configure the VC.

Frame Relay PVC Problems

Table 8-4. Frame Relay PVC Problems

Symptom	Possible Cause	Solutions
Losing Data	Frame relay network is experiencing problems.	Run PVC Loopback and Pattern tests to isolate the problem, then contact the service provider.
No receipt or transmission of data	Cross connections of the DLCI(s) are configured incorrectly.	Verify the PVC connections and DLCIs by checking the network-discovered DLCIs on the LMI Reported DLCIs screen.
	DTE is configured incorrectly.	Check the DTE's configuration.
	LMI is misconfigured for the DTE or network.	Configure LMI options to match those of the DTE or network.
	LMI link is inactive.	■ For the CSU/DSU, verify that the LMI link is active (the Status Msg Received counter on the Network Frame Relay Performance Statistics screen is incrementing). ■ For the router, verify that the Ethernet interface is active (the Frames Transmitted and Frames Received counters on the Ethernet Performance Statistics screen are incrementing).
Out of Sync	If Monitor Pattern was selected, it means the test pattern generator and receiver have not yet synchronized. CIR settings for the units at each end are mismatched. If the message persists, it means that 5 packets out of 25 are missing or are out of sequence.	■ Verify that the unit at the other end is configured to Send Pattern. Correct unit configurations. ■ Correct the CIR setting so both units are configured the same. ■ Check the line's error rate for physical line quality. Contact the service provider.

Tests Available

The following FrameSaver DSL tests are available.

CSU/DSU Test Menu Example

```
main/test                                                        978x-C-SLV
Device Name: Node A                                          6/05/2001 08:02

                                    TEST

                            Network PVC Tests
                            Data Port PVC Tests

                            Network ATM Loopback Tests

                            Network Physical Tests  (9788 only)
                            Data Port Physical Tests

                            IP Ping
                            Lamp Test

                            Abort All Tests




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu    Exit
```

Router Test Menu Example

```
main/test                                                        978x-RtrSLV
Device Name: Node A                                          6/05/2001 08:03

                                    TEST

                            Network PVC Tests

                            Network ATM Loopback Tests

                       9788: Network Physical Tests
                            IP Ping
                            Lamp Test

                            Abort All Tests









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu    Exit
```

Network and Data Port PVC Tests do not appear on the Test menu when no PVCs have been configured on the interface.

Network ATM Loopback Tests does not appear if no ATM links are enabled on the network interface.

Tests can be commanded from the OpenLane SLM system using its enhanced Diagnostic Troubleshooting graphical interface, as well as from the menu-driven user interface.

Test Timeout Feature

A Test Timeout feature is available to automatically terminate a test (as opposed to manually terminating a test) after it has been running a specified period of time.

It is recommended that this feature be used when the FrameSaver device is remotely managed through an inband data stream (PVC). If a test is accidently commanded to execute on the interface providing management access, control is regained when the specified time period expires, automatically terminating the test.

To use this feature, enable the Test Timeout configuration option, and set a duration for the test to run in the Test Duration (min) configuration option (see *Configuring General System Options* in Chapter 4, *Configuration Options*).

NOTE:

These configuration options do not pertain to tests commanded by the DTE, like a DTE-initiated External Loopback.

Starting and Stopping a Test

Use this procedure to start, monitor, or stop specific tests. To abort all active tests on all interfaces, see *Aborting All Tests*.

▶ Procedure

To start and stop a loopback or set-pattern test:

1. Follow this menu selection sequence:

   Main Menu→ Test

2. Select an interface and test (e.g., Network or Data Port PVC Tests) and press Enter. The selected test screen appears. **`Start`** appears in the Command column. **`Inactive`** appears in the Status column.

3. Select the DLCI number and press Enter if a PVC test has been selected.

   The cursor is positioned at Start in the Command column of the first available test. Start is highlighted.

4. Select the test you want to start and press Enter. **`Stop`** now appears and is highlighted, and the status of the test changes to **`Active`**.

5. Press Enter to stop the test. **`Start`** reappears and the status of the test changes back to **`Inactive`**.

6. View the length of time that the test has been running in the Result column.

Aborting All Tests

Use the Abort All Tests selection from the Test menu to abort all tests running on all interfaces. To abort individual tests that are active, see *Test Timeout Feature* on page 8-16 and *Starting and Stopping a Test*.

▶ Procedure

To abort all tests on all interfaces:

1. Follow this menu selection sequence:

   Main Menu→ Test

2. Select Abort All Tests and press Enter.

   `Command Complete` appears when all tests on all interfaces have been stopped.

   NOTE:

   Abort All Tests does not interrupt DTE-initiated loopbacks.

PVC Tests

PVC tests can be run on a requested DLCI for a selected interface. Data Port PVC tests do not apply to the DSL router.

- When PVC tests are on a multiplexed DLCI between FrameSaver devices, they are nondisruptive to data, so user data can continue to be sent during a test.
- If the device at one end of the circuit is not a FrameSaver device, PVC tests are on a standard DLCI and are disruptive to data. Also, the Connectivity test would not appear.

Loopback and send/monitor pattern tests are available for each interface on the selected DLCI. FrameSaver devices should be at each end of the circuit. If a PVC Loopback is started at one end of the circuit, the other end can send and monitor pattern tests.

The following example shows a FrameSaver DSL CSU/DSU's PVC Test screen, with the multiplexed DLCI 550 selected. If the DSL router or a standard DLCI was selected, (**Disruptive**) rather than (**Non-Disruptive**) displays after Test, and the Connectivity test does not appear.

PVC Tests Screen Example

```
main/test/network_pvc                                              9783-C-SLV
Device Name: Node A                                            2/26/2001 08:03

                              Net1-FR1 PVC TESTS

DLCI Number: 550

Test (Non-Disruptive)       Command   Status     Result

PVC Loopback:               Start     Inactive   0:00:00
Send Pattern:               Start     Inactive   0:00:00
Monitor Pattern:            Start     Inactive   0:00:00
                                                 Sequence Errors  99999+
                                                 Data Errors      99999+
Connectivity:               Start     Inactive   RndTrip Time(ms) 99999









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu        MainMenu    Exit
```

NOTE:

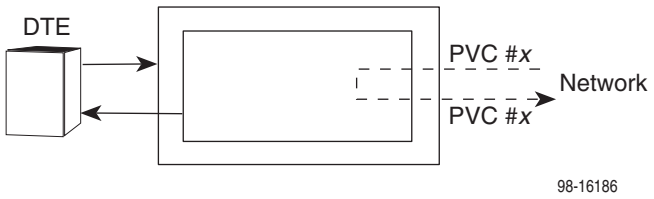
Errors encountered during these tests may be caused by mismatched CIRs in the two FrameSaver units. If errors are detected, verify the CIR configuration and retest.

PVC Loopback

The PVC Loopback loops frames back to the selected interface on a per-PVC basis. This test logically (not physically) loops back frames received from another FrameSaver device through the selected frame relay PVC to the same device.

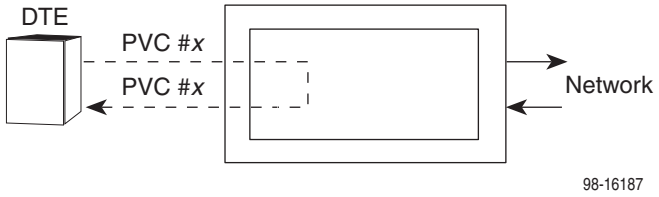
Main Menu→ Test→ Network PVC Tests

Network PVC Loopback



Main Menu→ Test→ Data Port PVC Tests

Port PVC Loopback



Send Pattern

This test sends packets filled with a hexadecimal 55 test pattern and sequence number over the selected interface and DLCI to another FrameSaver device. To send a pattern test on a link:

Main Menu→ Test→ [Network PVC Tests/Data Port PVC Tests]

If the selected DLCI is configured as . . .	Then . . .	And the default Rate (Kbps) setting is . . .
Standard	**(Disruptive)** appears after Test	100% of CIR
Multiplexed	**(Non-Disruptive)** appears after Test	10% of CIR

If the CIR is zero, the pattern will be sent at a rate of 1000 bps.

Monitor Pattern

This test monitors packets filled with a hexadecimal 55 test pattern and sequence number over the selected interface and DLCI to another FrameSaver device.

To monitor a pattern test on a link:

Main Menu→ Test→ [Network PVC Tests/Data Port PVC Tests]

The current number of sequence and data errors are shown under the Result column when the FrameSaver unit is in sync. An **`Out of Sync`** message appears when 5 frames out of 25 are missing or out of sequence.

These error counts are updated every second. If the maximum count is reached, **`99999+`** appears in these fields.

Connectivity

Connectivity is a proprietary method that determines whether the FrameSaver device at the other end of the frame relay PVC is active. This test stops automatically and can only be executed for circuit multiplexed PVCs.

To run a connectivity test on a link:

Main Menu→ Test→ Network PVC Tests

Selecting Connectivity sends a frame to the FrameSaver unit at the other end of the PVC. A **`RndTrip Time(ms)`** message appears in the Result column when a response is received within 5 seconds, indicating that the FrameSaver unit at the remote end is alive (operational and connected), and the round trip (RT) time is shown in milliseconds (ms), with a resolution of 1 ms. If a response is not received within 5 seconds, **`No Response`** appears in the Result column.

Network ATM Loopback

A Network ATM Loopback is a nondisruptive test that can be run on a Virtual Channel Connection (VCC) for an ATM link on the network interface.

Select an enabled ATM link so available VCCs can be selected for testing on the link.

Network ATM Loopback Tests Screen Example

```
main/test/network_atm                                              9783-C-SLV
Device Name: Node A                                          2/26/2001 08:03

                              Net1-ATM LOOPBACK TESTS
VPI,VCI: 0,35
Loopback Type: Segment
Destination Segment ID: FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF   Reset

Test            Command     Status      Result
ATM Ping:       Start       Inactive    RndTrip Time(ms)  99999









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu    Exit
```

The ATM Loopback causes the FrameSaver device to send either a segment or end-to-end loopback packet toward the network on the selected VCC, then wait for a response.

A **RndTrip Time(ms)** message appears in the Result column when a response is received within 5 seconds, indicating that the FrameSaver unit at the remote end is alive (operational and connected), and the round trip (RT) time is shown in milliseconds (ms), with a resolution of 1 ms. If a response is not received within 5 seconds, **No Response** appears in the Result column and the test is automatically stopped.

The following fields are explained below.

For . . .	Select or Enter . . .
VPI,VCI	From the VCCs configured for the ATM link.
Loopback Type	■ EndtoEnd – For Operations, Administration, and Maintenance (OAM) functions. The device defaults to this type of loopback. ■ Segment – For OAM functions, a segment loopback will be performed on the selected VCC on the link.
Destination Segment ID	■ ATM Segment ID for the loopback destination – The ID must be entered in 16 byte values, 2 hexadecimal characters each, separated by colons. – The first byte must be 00, 01, 02, 03, or FF. – If the first octet is FF, octets 2–16 must also be FF. – If the first octet is 00, octets 2–16 must also be 00. ■ Reset – Resets the ATM Destination Segment ID for the VCC. When selected, all octets in this segment are set to FF, as shown in the screen example. **NOTE:** Destination Segment ID and Reset do not appear if Loopback Type is EndtoEnd instead of Segment.
ATM Ping	Start or Stop commands begin or end the test.

The following messages can appear on line 24:

- If an ATM Location ID has not yet been configured, Loopback Type is set to Segment, an ATM Ping is started, and an **`ATM Location ID must be configured`** message is displayed.
- If the device is already performing an ATM Ping, an **`Invalid - Was Already Active`** message is displayed.
- If any physical test is active on the interface when the ATM Ping was started, the **`Invalid Test Combination`** message is displayed.
- If the ATM link is not active when the ATM Ping is started, the **`Link Inactive`** message is displayed.

This test cannot be run when a physical test is already active on the interface, and no physical test can be run on the interface when the ATM Loopback is active on the interface.

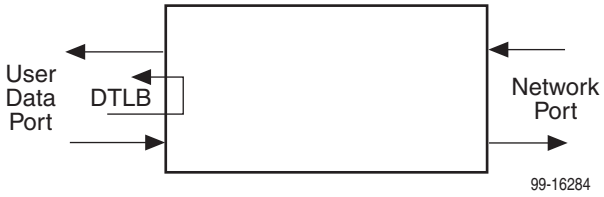
Data Port Physical Tests

The FrameSaver DSL CSU/DSU supports a single physical test for the data port, the DTE Loopback. This test does not appear for the router.

DTE Loopback

The local DTE external Loopback (DTLB) loops the received signal on the DTE interface back to the DTE without affecting the operation of the remaining ports. Use this test to isolate problems on the user data port.

Main Menu→ Test→ Data Port Physical Tests



An attached device or test equipment must generate the data to be looped back, and the Port (DTE) Initiated Loopback option must be enabled. Refer to *Configuring the CSU/DSU's Data Port Physical Interface* in Chapter 4, *Configuration Options.*

CAUTION:

This test may affect operation of frame relay PVCs for the port. Any data being sent while this test is active will be disrupted.

IP Ping Test

An IP Ping can test connectivity between the management data path and the FrameSaver unit and any FrameSaver unit, router, or NMS to which it has a route. In addition, the test can be run to access a remote unit for configuration purposes.

Times when you might want to run an IP Ping test are:

- To test connectivity between the FrameSaver unit and any FrameSaver unit in the network to verify that the path is operational. Select *IP Ping Test – Procedure 1* to ping any far-end FrameSaver unit.
- To verify the entire path between a newly installed remote site FrameSaver unit and the central site NMS. During a remote site installation, an IP Ping test is typically run from the remote site to ping the NMS at the central site. The remote FrameSaver unit must have SNMP trap managers configured, and one of those trap managers must be the central site NMS. Select *IP Ping Test – Procedure 2* on page 8-29 to ping the NMS at the central site.
- To test the path to the NMS trap managers during installation of the central site FrameSaver unit. The remote FrameSaver unit must have configured the SNMP trap managers to be sent the Ping. Select *IP Ping Test – Procedure 2* on page 8-29 to ping SNMP trap managers.

Ping Screen Example

```
main/test/ping                                                    9783-C-SLV
Device Name: Node A                                          09/11/2002 06:12

                                   IP PING
        Target IP Address:       000.000.000.000
        Destination Interface:   Use Internal Route  DLCI: 100 (Net1-ATM 15,255)
        Source IP Address:       Special           135.90.25.1
        Encapsulation:           Routed
        TOS Byte                 User Defined 001101
        Packet Size:             64
        Iteration Count:         1
        Inter-ping Delay (sec): 5
        Response Timeout (sec): 2
        Start
        ---------------------------------------------------
         Status:                  Alive
                             Transmit Receive   Lost    Loss Ratio
        Pings:                 000000  000000   000000     0000 %
                               Current  Minimum Maximum  Average
        Roundtrip Delay (ms):   0000     0000    0000     0000

--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

Table 8-5. Ping Options (1 of 2)

Target IP Address
Possible Settings: **000.000.000.001–126.000.000.000, 128.000.000.000–223.255.255.255** Default Setting: **000.000.000.000**
Specifies the IP address to which a ping will be sent. **000.000.000.001–126.000.000.000, 128.000.000.000–223.255.255.255** – Specifies the IP address.
Destination Interface
Possible Settings: **Use_Internal_Route, Port-*n*, Net1-FR1** Default Setting: **Use_Internal_Route**
Specifies the routing method or destination interface for the ping. **Use_Internal_Route** – When choosing which interface to send the ping, the unit first consults its routing table. If the address or subnet does not appear in the routing table, the ping will be sent to the Default IP Destination, if defined. (See *Configuring Node IP Information* in Chapter 4, *Configuration Options*.) **Port-*n*, Net1-FR1** – The ping is sent out the specified destination regardless of the internal route configuration.
DLCI
Possible Settings: **16–1007** Default Setting: [Lowest assigned DLCI on the selected interface]
Specifies the DLCI to be used for the ping. If the DLCI is configured on a Virtual Channel Connection (VCC), the VPI (0–15) and VCI (32–255) are displayed next to the DLCI. *Display Conditions* – This setting does not appear when Destination Interface is set to Use_Internal_Route. **16–1007** – Specifies the DLCI.
Source IP Address
Available Settings: **Automatic, Special** Default Setting: **Automatic**
Specifies the source IP address to be identified with the ping. *Display Conditions* – This setting does not appear when Destination Interface is set to Use_Internal_Route. **Automatic** – The source IP address is: – The interface IP address, if one exists, else – The node IP address if one exists, else – The first available address in the address table **Special** – The entered IP address is shown as the source. When Special is specified, and additional field is displayed that allows you to enter an IP address 000.000.000.001–126.255.255.255, or 128.000.000.000–223.255.255.255.

Table 8-5. Ping Options (2 of 2)

Encapsulation
Available Settings: **Routed** Default Setting: **Routed**
Specifies the IP encapsulation used by the data stream. This read-only field specifies that the IP encapsulation used is RFC 1490/RFC 2427 routed Network Level Protocol IDentifier (NLPID) encapsulation, and not SubNetwork Access Protocol (SNAP) encapsulation. *Display Conditions* – This setting does not appear when Destination Interface is set to Use_Internal_Route. **Routed** – The encapsulation is routed NLPID.
TOS Byte
Available Settings: **A predefined COS ID, or a user-defined binary value 0000–1111** Default Setting: **User Defined – 000000**
(Release 2.1.) Specifies the TOS (Terms Of Service) byte to be used with the ping packet. Select from COS (Class Of Service) definitions, if any exist, or specify a binary value. When a COS definition is selected, the TOS byte value is read-only. If you select a COS definition that has multiple COS IDs, the lowest value is used as the TOS byte. See *Configuring Class of Service Definitions* in Chapter 4, *Configuration Options*. **0000–1111** – The value of the TOS byte.
Packet Size
Available Settings: **36–4096** Default Setting: **100**
Specifies the size of the ping packet including the IP header (20 bytes) and the ICMP header (8 bytes). **1–4096** – Packet size.
Iteration Count
Available Settings: **1–999999** Default Setting: **5**
Specifies the number of pings to send. **1–999999** – Number of pings.
Inter-Ping Delay
Available Settings: **1–900** Default Setting: **1**
Specifies, in seconds, the amount of time to wait between pings. **1–900** – The ping wait time.
Response Timeout
Available Settings: **1–60** Default Setting: **2**
Specifies the amount of time, in seconds, to wait before a host that has not responded to a ping is declared unreachable. **1–60** – The response timeout period.

When the ping has completed normally, timed out, or been stopped using the Stop command, informational fields are displayed as shown in Table 8-6, Ping Responses.

Table 8-6. Ping Responses

Field	Possible Values	Description
Status	■ In Progress ■ Alive ■ Destination Unreachable ■ Ping Timed Out ■ No route in this device	■ Ping has been sent. ■ Ping was successful. ■ The host could not be reached. See RFC 792 for possible causes. ■ There was no response in the period specified in Response Timeout. ■ The IP address is not in the routing table, and no Default IP Destination is configured.
Ping Loss Ratio (%)	0–100	The ratio of pings received to pings transmitted.
Pings Transmitted	1–999999	The number of pings transmitted.
Pings Received	1–999999	The number of pings received.
Pings Lost	1–999999	The number of pings transmitted less the number of pings received.
Current Roundtrip Delay	■ 0 ■ 1–9999	■ No measurement exists. ■ The time in milliseconds that it took to complete the latest ping.
Minimum Roundtrip Delay	■ 0 ■ 1–9999	■ No measurement exists. ■ The least time in milliseconds that it took to complete a ping during this test.
Maximum Roundtrip Delay	■ 0 ■ 1–9999	■ No measurement exists. ■ The most time in milliseconds that it took to complete a ping during this test.
Average Roundtrip Delay	■ 0 ■ 1–9999	■ No measurement exists. ■ The average time in milliseconds that it took to complete a ping during this test.

IP Ping Test – Procedure 1

▶ Procedure

To ping any far-end FrameSaver device:

1. Select the IP Ping test.

   Main Menu→ Test→ IP Ping

2. Enter the IP Address to ping, then select Start.

   NOTE:

   If the FrameSaver unit or the far-end unit has just initialized, it may take about a minute for the units to learn the routes via the proprietary RIP.

3. Verify the results of the IP Ping test.

   — While the test is running, **`In Progress`** appears in the Status field.

   — When the test is finished, **`Alive`** should appear as the Status. If any other message is displayed, additional testing is required.

IP Ping Test – Procedure 2

▶ Procedure

To ping the NMS at the central site or an SNMP trap manager:

1. Verify that the central site NMS has the FrameSaver unit's IP address in its routing table so it can communicate with the FrameSaver unit.
2. Verify that the central site NMS's router has the FrameSaver unit's IP address in its routing table so it can communicate with the FrameSaver unit.
3. Verify that the central site NMS has been configured as an SNMP Trap Manager if the router is to route data, so a route has been configured within the FrameSaver unit.

   Main Menu→ Configuration→ Management and Communication→ SNMP Traps

   Or, for a local DLCI between the central site FrameSaver unit and its router, verify that a Default IP Destination route has been configured.

   Main Menu→ Configuration→ Management and Communication→ Node IP→ Default IP Destination

   Configure both SNMP Traps and a Default IP Destination when PVC Multiplexing is used.
4. Select the IP Ping test.

   Main Menu→ Test→ IP Ping
5. Enter the IP Address of the central site NMS, then select Start.
6. Verify the results of the IP Ping test.
   - — While the test is running, **`In Progress...`** appears in the Status field.
   - — When the test is finished, **`Alive`** should appear as the Status. If any other message is displayed, additional testing is required.

Lamp Test

The FrameSaver device supports a Lamp Test to verify that all LEDs are lighting and functioning properly. All LEDs flash or blink on and off at the same time every 1/2 second during execution of the test. When the test is stopped, the LEDs are restored to their normal condition.

Main Menu→ Test→ Lamp Test

If the Test Timeout configuration option is enabled and a Test Duration is set, the Lamp Test stops when the test duration expires. See *Test Timeout Feature* on page 8-16 for additional information.

Setting Up OpenLane for FrameSaver Device

9

This chapter includes:

OpenLane Support of FrameSaver Devices

The OpenLane Service Level Management (SLM) system provides the following features:

- Web and database services
- Web access to health and status information
- Web access to real-time, as well as historical graphs and reports
- Web access to SLV reports, for units with the Advanced SLM Feature Set activated
- On-demand polling of FrameSaver devices
- SNMP polling and reporting
- Web-based diagnostic tests: end-to-end, PVC loopbacks, connectivity, and physical interface tests
- Basic device configuration, including RMON alarm and threshold configuration when the unit has the Advanced SLM Feature Set activated
- Automatic device and PVC discovery for devices with the SLV Delivery Ratio configuration option enabled
- Easy firmware downloads to an entire network or parts of the network
- Remote Advanced SLM Feature activation for units with the Diagnostic Feature Set
- Multiple maintenance schedules for scheduling more than one maintenance period, with a report for each scheduled task
- Multiple Circuit IDs for multiple access levels so customers, as well as network service providers, have access to network management information
- Device reset capability
- HP OpenView adapters for integrating OpenLane with the OpenView Web interface

Setting Up the OpenLane SLM System

Instructions for installing the OpenLane SLM system are found in the *OpenLane SLM Administrator's Guide*.

In addition to installation instructions, the Administrator's Guide contains instructions for:

- Starting and stopping the OpenLane Web and database services
- Accessing the OpenLane application
- Adding a FrameSaver device
- Adding a Customer ID

OpenLane SLM also has an extensive online Help system.

Setting Up FrameSaver Support

With OpenLane SLM's extensive online Help, the application is self-documenting and you have access to the most current system information.

▶ Procedure

To set up FrameSaver support:

1. Start the OpenLane services, then access the application.
2. Log in as **Admin** for access to customer profiles, frame relay access facilities components, and PVC components.
3. Add FrameSaver devices.
4. Create customer profiles.
5. Set up historical data collection.
6. Set up SLV report filters for Web access to report data for FrameSaver devices with the Advanced SLM Feature Set activated.

See the *OpenLane SLM Administrator's Guide* and OpenLane online Help to learn how to perform these steps and for additional information.

Ordering Advanced SLM Feature Set Activations

When advanced SLV functionality is needed at a site, an Activation Certificate (Feature No. 9720-C1-220, 9783-C1-220, or 9788-C1-220) can be ordered, which will allow you to activate Advanced SLM features in FrameSaver devices with the Diagnostic Feature Set. You must have the OpenLane SLM system, Release 5.3 or later, to activate Advanced SLV capability in FrameSaver devices and to manage your certificates.

NOTE:

If you have a combination of models in your network, a separate Activation Certificate must be ordered for each model number. Each certificate can be ordered for a single unit or for many units.

Contact one of the following to request an Activation Certificate:

- If you are an end user and managing your own network, contact your sales representative or distributor.
- If your network service provider (NSP) manages the network, contact the service provider.
- If you are a network service provider or distributor, contact Paradyne at 1-800-727-2396, **www.paradyne.com**, via a purchase order, or your Electronic Data Interchange (EDI). If submitting a purchase order by fax, send it to 1-727-532-5270.

  An Activation Certificate can also be ordered through the Paradyne store at **www.paradyne.com/store**.

Provide the following information:

- Model
- Number of units to be activated
- Your OpenLane SLM system license key number

To Find Your License Key Number

Your license key number was entered into your system when your OpenLane SLM system was installed and is available from the OpenLane Administration screen. However, to access the screen with your license key number, you must log in as a user with Administrative system access.

▶ Procedure

To find your OpenLane license key number:

1. Open the OpenLane SLM application and log in as a user with Administrative access.
2. A bottom of the OpenLane Administration screen, select **`About OpenLane SLM`**.

   The license key is shown mid-screen, below the copyright and build information.

The Activation Certificate

An Activation Certificate will be sent to you via Federal Express.

NOTE:

If you ordered an Activation Certificate via e-mail, Activation Certificate information will be e-mailed to you so you can start activating units immediately. The actual certificate will arrive the next day.

When the certificate arrives, it will include the following information:

- Activation Certificate number
- Your OpenLane License Key number
- Model Prefix (9783 or 9788)
- Feature Group: Advanced SLV
- Number of device activations ordered (included on this certificate)
- Sales order number
- Customer purchase order number
- Customer or company name
- Contact (sent to the attention of)
- Shipping address
- Phone number
- E-mail address
- Date the certificate was generated

Administering and Managing Advanced SLM Activations

The OpenLane SLM system provides the following features that allow you to administer and manage your Activation Certificates and Advanced SLM activations. From the Firmware/Feature Maintenance menu, you can:

- Add or view the status of activations, and see how many activations remain on each certificate.
- Schedule when activations are to take place, and verify that the activations occurred as scheduled.
- View activations that are scheduled, cancel activations, or change the FrameSaver devices that are scheduled for activation, as needed.
- Generate and print a report that summarizes the activity on all Activation Certificates in your system, which includes the number of activations ordered, the number of activations remaining on the certificate, and the date the certificate was ordered.

  The report also includes information about each activated unit: its system name, IP address, location, model, serial number, and date of activation.

The sections that follow describe what you need to do to get Activation Certificate information into your OpenLane SLM system, and to activate Advanced SLM capability in units with the Diagnostic Feature Set.

Entering an Activation Certificate

Once you receive an Activation Certificate, enter the Activation Certificate number into your OpenLane SLM system's database.

▶ Procedure

To enter the Activation Certificate number:

1. Open the OpenLane SLM application and provide your access level, which must be **Admin**.
2. Select **`Firmware/Feature Maintenance`** from the OpenLane Administration screen.
3. In the Feature Activations area, select **`View/Add activation certificates`**, located near the bottom of the Firmware/Feature Maintenance menu.
4. If no Activation Certificates have been entered into the system, or if adding another certificate:
   - — Click inside the New certificate box under **`Add certificate`**.
   - — Enter the Activation Certificate number from the certificate.
   - — Click on the prompt below it. The frame at the bottom of the screen is refreshed to display information about the new certificate.

See the OpenLane SLM system's online Help for additional information.

Checking Activation Certificate Status

You can view the status of certificates and activations at any time by selecting **`View/Add activation certificates`** from the Firmware/Feature Maintenance menu, and clicking on the prompt below **`Display certificates`**.

See the OpenLane SLM system's online Help for additional information.

Scheduling Activations

You can activate one, many, or all FrameSaver devices at any time, until all the activations ordered for the certificate have been completed.

NOTE:

Once Advanced SLV capability is activated in a FrameSaver device, the unit cannot be returned to the Diagnostic Feature Set.

▶ Procedure

To schedule device activations:

1. Open the OpenLane SLM application and provide your access level, which must be **Admin**, and select **`Firmware/Feature Maintenance`** from the OpenLane Administration screen.
2. In the Feature Activations area, select **`Schedule feature verifications/activations`**.
3. Follow the steps included on this screen.
   - — Select the FrameSaver devices to be activated at this time by model, device name, or IP address, and click on the prompt below the selection table.

     Entering an asterisk (*) in the Name or Device IP field will display all FrameSaver devices in your system, so you can pick and choose devices that will be activated.
   - — Select whether to activate selected devices.
4. Select the FrameSaver devices to be activated at this time under **`Select devices`** by model, device name, or IP address, then click on the prompt below the device selection table. The table in the lower frame lists all the devices in the selected category.

   Entering an asterisk (*) in the Name or Device IP field will display all FrameSaver devices in your system, so you can pick and choose devices that will be activated.
5. In the lower frame, click on the box in the Activate column to select or deselect a specific FrameSaver device for activation. Proceed through the list until you have selected all the devices to be activated at this time.
6. Proceed through the other steps included on this screen, then click on the prompt under **`Perform the scheduled verification/activation`** to verify what you scheduled. The Verify/Schedule Feature Activations screen appears so you can verify the scheduling information.
   - — If the information is correct, click on Apply.
   - — If not, or if you want to verify or change the devices that will be activated or the time the activations are to occur, click on the prompt to return to the previous screen and reselect you options.

Checking the Status of Scheduled Activations

You can check the status of scheduled activations or cancel activations at any time prior to the activations taking place by selecting **View/Abort scheduled task status** from the Firmware/Feature Maintenance menu. You can select all tasks, or select tasks by model, device name, or IP address. When you click on the prompt below the **Select tasks** table, the table in the lower frame lists all the devices in the selected category scheduled for activation.

See the OpenLane SLM system's online Help for additional information.

Canceling Scheduled Activations

To cancel scheduled activations, select **View/Abort scheduled task status** from the Firmware/Feature Maintenance menu, select the desired tasks, and click on the prompt to display the FrameSaver devices scheduled for activation.

Click on the box in the Abort column to select the FrameSaver devices that will not be activated, then click on the prompt under **Abort verifications/ activations** to verify your selections, and Apply. Activations for the selected devices will be cancelled.

See the OpenLane SLM system's online Help for additional information.

Accessing and Printing the Certificate Summary Report

The Certificate Summary Report provides information about the Activation Certificate and the activated devices. Select **Generate certificate summary report** from the Firmware/Feature Maintenance menu.

The report lists all Activation Certificates in your OpenLane SLM system and all the FrameSaver devices activated using each certificate.

- Activation Certificate information includes the model, feature, the number of activations ordered, the number of activations still covered by the certificate, and the date the certificate was ordered.
- Device activation information includes the device's name, IP address, its location, model, serial number, and the date the device was activated.

We recommend that you print and save this report. However, before printing change the orientation of the report to Landscape so no information is truncated.

See the OpenLane SLM system's online Help for additional information.

Setting Up Network Health for FrameSaver Device

10

FrameSaver units are compatible with Concord Communication's Network Health software.

For FrameSaver units with the Advanced SLM Feature Set, Network Health has released the first in a series of software modules that integrate FrameSaver SLV enhanced performance statistics into its reporting package (see the example in *FrameSaver SLV Plus At-a-Glance Report* on page 10-9). To generate this report, you need Network Health R4.01 or higher.

This chapter includes Network Health information as it relates to FrameSaver DSL devices. It includes the following:

For additional information about applicable reports, refer to your Concord Communications documentation. For document numbers and titles, see *Product-Related Documents* in *About This Guide*.

Installation and Setup of Network Health

Refer to the *Network Health Installation Guide* for installation instructions applicable to your network platform. Once Network Health is installed, the application must be configured to support FrameSaver devices.

Each Network Health application provides a different set of functions, called a module. Each module used requires a separate license to gain access to those features and functions. Make sure you license the Poller application so you can poll FrameSaver devices and collect data.

▶ Procedure

To use the Network Health application:

1. Discover network elements, units, and interfaces in the network.
2. Configure the Network Health applications, and save them.
3. Organize elements into groups for reporting purposes.
4. Set up and run reports.

Setup and operation information is contained in the *Network Health User Guide*. The sections that follow address only the minimal procedural steps needed once you have access to the applications.

See the Network Health User and Reports Guides for additional startup information and a full discussion of the application's features and how to use them.

Discovering FrameSaver Elements

Once licenses are entered and you have access to the applications, the Discover dialog box opens. Use this dialog box to search for FrameSaver devices in your network and discover their DLCIs.

IP addresses and the Community String for the FrameSaver devices must be entered for Network Health to find the FrameSaver devices on the network and discover their elements. These *elements* are resources that can be polled (e.g., LAN/WAN interfaces, frame relay circuits, routers, and servers).

The two types of statistics that can be polled are:

- **Statistics elements** – Provide counters and other gauges for information gathered about your network for statistical and trend analysis.
- **Conversation elements** – Provide RMON2 and similar data for information gathered about network traffic between nodes.

▶ Procedure

To locate FrameSaver device elements in your network:

1. Select the LAN/WAN radio button to specify the element type to be found. Network Health treats frame relay element discovery as a WAN element type.
2. Enter the IP Addresses of the FrameSaver devices to be located, and the Community String (Community Name in the FrameSaver device). The Community String is case-sensitive.
3. Select the Discover button.

   The Discover dialog box closes and the Discovering dialog box opens, showing the results of the discovery process. A message indicates the number of elements discovered and the number of existing elements updated when the discovery process is complete.

   Depending upon the number of devices entered and the size of your network, it could take anywhere from a few minutes to an hour or longer to discover all elements in the network.
4. Save the search results.

   Saving the search results creates poller configuration definitions to be used to poll the devices.

See *Discovering Elements* in the *Network Health User Guide* for additional information and to learn how to schedule automatic element discovery updates to the database.

Configuring the Discovered Elements

Network Health sets the speed for discovered elements when it polls the device for the first time. For a FrameSaver device, the speed set would be the unit's CIR. No additional configuration should be required, but verify that all appropriate information has been retrieved.

NOTE:

If a FrameSaver device does not have CIR configured, or if it is not configured correctly, Network Health sets the unit's CIR to 0 Kbps. For this reason, you should reconfigure the unit's CIR before Network Health polls it. If 0 Kbps is the speed setting, you will need to edit the unit's CIR from Network Health.

See *Discovering Elements* in the *Network Health User Guide* for additional information, configuration and editing.

▶ Procedure

To change the FrameSaver device's CIR unit elements from Network Health:

1. Select the Edit Before Saving button at the bottom of the Discovering dialog box once the discovery process is completed.

   The Poller Configuration window opens.

2. Double-click on the first element discovered. The Modify Element dialog box opens.

3. In the Speed box, select the Override radio button and enter the device's CIR in the text box.

   Letters **k** and **m** can be used as shortcuts (e.g., enter 56 k for 56 Kbps, or 16 m for 16 Mbps.

4. Apply your changes:

   — Select the Apply/Next button to save your change and bring up the next element to be edited. Continue until all newly discovered frame relay elements have been modified before selecting the OK button.

   — Select the OK button.

   The Modify Element dialog box closes.

5. Select the OK button at the bottom of the Poller Configuration window. The modified elements are saved to the database, and the devices are polled.

Allow Network Health to continue polling for about a half an hour to allow time for data to be gathered before running any reports.

Grouping Elements for Reports

Once the discovery process is completed and required changes are made, the newly discovered elements (DLCIs) should be organized into a group for Health reporting. Grouping makes for easier monitoring and management of similar node types (e.g., all FrameSaver and SLV elements). Once grouped, you can then run reports on all DLCIs in the network, as well as reports on individual DLCIs.

▶ Procedure

To group elements:

1. From the console, select Edit Groups from the Reports menu. The Add Groups dialog box opens.
2. Enter a name in the Group Name field. Up to 64 characters can be entered. A through Z, a through z, 0 through 9, dashes (–), periods (.), and underscores (_) can be used. No spaces can be included, and the word All cannot be used.
3. Select the WAN radio button (above the Available Elements list).
4. Highlight the DLCIs listed on the Available Elements list, or select specific DLCIs, then select the left arrow button.

   The highlighted DLCIs move from the Available Elements list to the Group Members list.
5. Select the OK button when all appropriate DLCIs have been moved to the Group Members list.

   The Add Groups dialog box closes and the newly created group appears on the Groups dialog box.

See *Managing Groups and Group Lists* in the *Network Health Reports Guide* for additional information on grouping elements and customizing reports.

Generating Reports for a Group

Once Network Health has had sufficient time to gather data from the polled DLCIs and the DLCIs have been grouped, you can start generating reports. When selecting a report Section, select WAN from the drop-down list. See *Running Reports from the Console* in the *Network Health Reports Guide* for additional information. That section also tells you how to schedule automatic report generation.

NOTE:

Network Health provides information with each chart or table, generally referred to as a report. Click on the hyperlink (Explanation of...) for an explanation of the report and its features. You can also refer to the *Network Health Reports Guide*.

About Service Level Reports

For long-term analysis and reporting, you will want to license the Service Level Reports application. This application analyzes data collected over months, or by quarters, and provides service level information about an enterprise, a region, department, or business process. Executive, IT Manager, and Customer Service Level reports are provided.

Using these reports, you can measure service performance against goals and agreements. Ranges for service level goals can be set for up to five variables: availability, bandwidth, bytes, health exceptions, and latency. These ranges need to be set before reports are scheduled.

About At-a-Glance Reports

At-a-Glance Reports consolidate various important DLCI and network performance indicators onto a single page. Up to ten DLCIs can be included in an At-a-Glance Report.

For FrameSaver units with the SLV and SLM reporting feature set, using the FrameSaver SLV report you can compare a DLCI's volume with the network's performance over a specified period of time. Ranges for service level goals can be set for up to five variables: availability, bandwidth, bytes, health exceptions, and latency. These ranges need to be set before reports are scheduled. In addition, all the enhanced network statistics that only an SLV enhanced device can accurately collect is provided so you can truly monitor the health of the frame relay network and see the effects of the customer's utilization on network efficiency.

About Trend Reports

By specifying specific variables like bandwidth, trend analysis can be performed and shown on Trend Reports. Up to ten variables for a DLCI, or ten DLCIs on one variable can be generated on a single trend report. Information can be presented in a line graph, pie chart, bar chart, or table format. Any amount of time can be specified for the reporting period.

These reports can help identify the reasons a DLCI has acquired a poor Health Index rating. See the Exceptions Report for information about Health Index ratings.

Printed Reports

All of the charts and tables seen online can also be provided on printed reports.

Reports Applicable to FrameSaver Devices

The following frame relay reports support FrameSaver devices:

- **Exception Reports** – Provide summary and detail information that identifies DLCIs with the highest incidence of errors, high bandwidth utilization, and trends.

  These reports identify those DLCIs that have exceeded a specified number of accumulated *exception points*. It is a good idea to run this report daily so that DLCIs having the most problems can be attended to first. DLCIs contained on this report need immediate attention.

  If a DLCI suddenly shows up on these reports, check whether any new equipment has been added to the network and whether it is properly configured. If its configuration is correct, the equipment could be faulty.

- **Summary Reports** – Provide summary information for the network, volume and error leaders, and DLCI traffic.

  — **Network Summary Report** – Provides an overall view of the network. Use this report for planning and to predict when a DLCI might run into problems.

  — **Leaders Summary Report** – Identifies DLCIs having the highest volume and errors. High traffic volume may be increasing latency, and the high Health Index rating indicates problems. It is a good idea to run these reports daily so a norm can be established. The same DLCIs should appear.

  Use this chart and table to alert you to possible problems. Problems to look for include: a normally high-volume DLCI is dropped from the list, a new DLCI appears on the list (check Element Summaries), a DLCI has a high Health Index rating, but low volume, significant differences between a DLCI's average and peak Health Index rating.

- **Elements Summary Report** – Compares DLCI traffic with volume and the baseline, bandwidth utilization, and errors.

  Use this report for DLCI detail information and comparison, to identify DLCIs with above or below average volume so they can be investigated when there are any significant changes.

- **Supplemental Report** – Shows DLCI availability and latency. The information shown in this report is also on other Health reports. However, these charts show more than ten DLCIs at a time so you have a broader view of the service provided by the network.

- **Service Level Reports** – Provide summary information for a group list for a longer reporting period than other reports.

  - **Executive Service Level Report** – Provides service level performance for an enterprise on a single page. Use this report to assess whether IT service levels are meeting availability and service goals.

  - **IT Manager Service Level Report** – Provides service level information for various groups. Using this report, you can compare service level performance of various groups. The report summarizes service levels for a group of DLCIs, along with details on individual DLCIs within that group.

  - **Customer Service Level Report** – Provides service level information for customers. This report is used to provide service level information to service customers to help them determine optimum service levels needed based upon their own traffic data, as well as provide documented evidence for increasing CIR. It combines daily volume, daily Health exceptions, bandwidth distribution, average Health Index ratings and availability for each DLCI onto a single page.

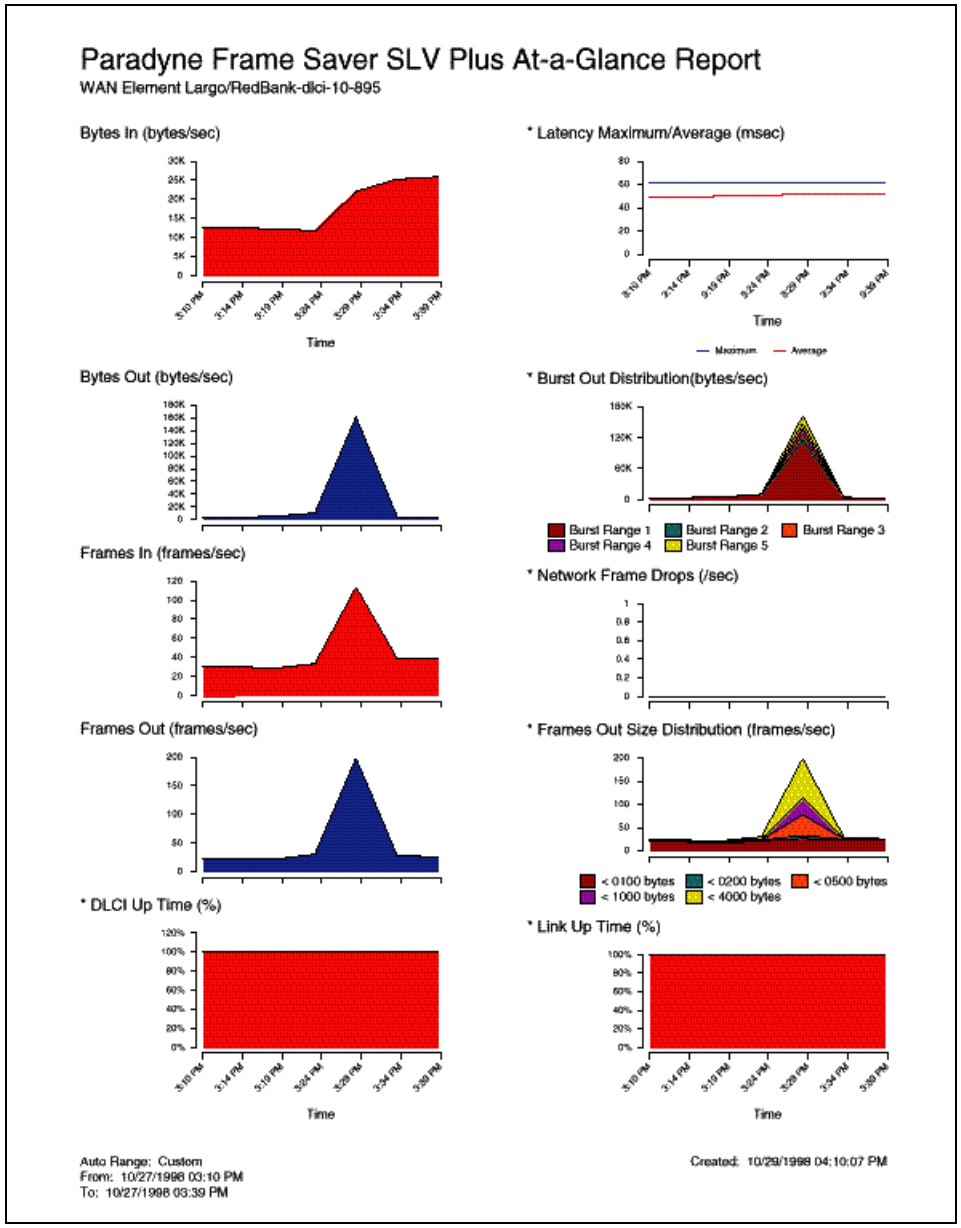
- **At-a-Glance Reports** – Provides consolidated DLCI and network performance information onto a single page.

  - **At-a-Glance Report** – Consolidates bandwidth utilization, network traffic, events occurring over the reporting period, and availability and latency levels information. Variables other than bandwidth can be selected for a trend report (e.g., burst octets), but a bandwidth trend report should be generated when investigating problems that appear on Exceptions Reports, Supplemental Reports, and Health reports.

    Use trend reports to view individual variables for DLCIs having a high Health Index rating to help locate which variable is causing a problem leading to a DLCI's poor Health Index rating.

— **FrameSaver SLV Plus At-a-Glance Report**

For FrameSaver units with the SLV and SLM reporting feature set, performs trend analysis on up to ten specified variables for DLCIs. This is the first Network Health report to integrate the FrameSaver device's unique monitoring capabilities, using the unit's SLV-advanced network statistics.



- **Trend Reports** – Perform trend analysis on up to ten specified variables for DLCIs. Variables other than bandwidth can be selected for a trend report (e.g., burst octets), but a bandwidth trend report should be generated when investigating problems that appear on Exceptions Reports, Supplemental Reports, and Health reports.

  Use trend reports to view individual variables for DLCIs having a high Health Index rating to help locate which variable is causing a problem leading to a DLCI's poor Health Index rating.

See the *Network Health Reports Guide* for more information about these reports.

Menu Hierarchy

Menus

The following table show the FrameSaver DSL devices' menu organizations.

NOTE:

Actual menus may vary based on the model, current configuration settings, and feature set installed in the device.

FrameSaver DSL CSU/DSUs Menu Structure

Status	**System and Test Status**	Self-Test Results Last System Reset Health and Status Test Status
	LMI Reported DLCIs	DLCI Status CIR (bps)
	IP Path Connection Status	Device Name IP Address Status Discovery Source
	PVC Connection Status	Source Link, DLCI, EDLCI Primary Destination Link, DLCI, EDLCI Status
	IP Routing Table	Destination Mask Gateway Hop Type Interface TTL
	Performance Statistics	Service Level Verification DLCI Frame Relay ATM (9783, 9788) VCC (9783, 9788) xDSL Line (9788) Ethernet Clear All Statistics
	Trap Event Log	Number of Trap Events Time of Day Event
	Display LEDs and Control Leads	
	Identity	System NAM
Test	**Network PVC Tests**	PVC Loopback Send Pattern Monitor Pattern Connectivity (9783, 9788)
	Data Port PVC Tests	PVC Loopback Send Pattern Monitor Pattern Connectivity
	Data Port Physical Tests	DTE Loopback
	Network ATM Loopback Tests (9783, 9788)	ATM Ping
	IP Ping	
	Lamp Test	
	Abort All Tests	

Configuration	**System**	Frame Relay and LMI Class of Service Definitions Service Level Verification General
	Network	Physical Frame Relay DLCI Records (9720) Circuit Records (9783, 9788) ATM (9783, 9788)
	Data Ports	Physical Frame Relay DLCI Records
	PVC Connections	Source Link, DLCI, EDLCI Primary Destination Link, DLCI, EDLCI
	IP Path List	Add and Display Static Paths
	Management and Communication Options	Node IP Management PVCs General SNMP Management Telnet and FTP Session SNMP NMS Security SNMP Traps Ethernet Management Communication Port External Modem (on Com Port)
Control	**System Information**	Device Name System Name, Location, Contact Date Time
	Administer Logins	Login ID Password Access Level
	Change Operating Mode	Back-to-Back Mode Standard Mode
	Select Software Release	Current Release Alternate Release Switch & Reset
	LMI Packet Capture Utility	Capture Interface Packet Capture Start/Stop Status Packets in Buffer Display LMI Trace Log
	Telnet (Release 2.1)	
	Reset Device	
Easy Install		DSLAM Type (9783) Node IP Address Node Subnet Mask TS Access Create Dedicated Network Management Link Ethernet Port Options Screen Network 1 Operating Rate (9720) Network 1 DSL Line Rate (9783, 9788) Network 1 FRF.8 Encapsulation Mode (9783, 9788) Port-1 Port Type (9788)

FrameSaver DSL Routers Menu Structure

Status	**System and Test Status**	Self-Test Results Last System Reset Health and Status Test Status
	LMI Reported DLCIs	DLCI Status CIR (bps)
	IP Path Connection Status	Device Name IP Address Status Discovery Source
	PVC Connection Status	Source Link, DLCI, EDLCI Primary Destination Link, DLCI, EDLCI Status
	IP Routing Table	Destination Mask Gateway Hop Type Interface TTL
	Performance Statistics	Service Level Verification DLCI Frame Relay ATM VCC xDSL Line Ethernet Clear All Statistics
	Trap Event Log	Number of Trap Events Time of Day Event
	Display LEDs and Control Leads	
	Identity	System NAM
Test	**Network PVC Tests**	PVC Loopback Send Pattern Monitor Pattern
	Network ATM Loopback Tests	ATM Ping
	IP Ping	
	Lamp Test	
	Abort All Tests	

Configuration	**System**	Class of Service Definitions Service Level Verification General
	Network	Physical Frame Relay Circuit Records ATM
	Virtual Router Ports	DLCI Records
	PVC Connections	Source Link, DLCI, EDLCI Primary Destination Link, DLCI, EDLCI
	IP Path List	Add and Display Static Paths
	Management and Communication Options	Node IP Management PVCs General SNMP Management Telnet and FTP Session SNMP NMS Security SNMP Traps Ethernet Management Communication Port External Modem (on Com Port)
Control	**System Information**	Device Name System Name, Location, Contact Date Time
	Administer Logins	Login ID Password Access Level
	Change Operating Mode	Back-to-Back Mode Standard Mode
	Select Software Release	Current Release Alternate Release Switch & Reset
	Telnet (Release 2.1)	
	Reset Device	
Easy Install		DSLAM Type (9783) Node IP Address Node Subnet Mask TS Access Create Dedicated Network Management Link Ethernet Management Options Screen Network 1 DSL Line Rate Network 1 FRF.8 Encapsulation Mode

SNMP MIBs, Traps, and RMON Alarm Defaults

B

This appendix contains the following:

MIB Support

The FrameSaver unit supports the SNMP Version 1, and has the capability of being managed by any industry-standard SNMP manager and accessed by external SNMP managers using the SNMP protocol.

The following MIBs are supported:

- MIB II (RFC 1213 and RFC 1573)
- Frame Relay DTEs MIB (RFC 2115)
- RS-232-Like MIB (RFC 1659)
- Frame Relay Service MIB (RFC 1604)
- EtherLike MIB (RFC 2665)
- RMON Version 1 MIB (RFC 1757)
- RMON Version 2 MIB (RFC 2021)

Downloading MIBs and SNMP Traps

Paradyne standard and enterprise MIBs are available from the Paradyne World Wide Web site at **www.paradyne.com**.

▶ Procedure

To access Paradyne MIBs:

1. From the Paradyne World Wide Web site, select:

   Support→Online Technical Support

2. Under Technical Information, select MIBs.
3. Select FrameSaver Frame Relay Devices.
4. Select the desired MIB.

The download procedure may vary depending upon your browser or NMS application software. Refer to your browser or OpenLane NMS instructions for additional download information.

System Group (mib-2)

This section provides the system description and system object identifier for the System Group for the FrameSaver DSL device, which is an SNMPv1 MIB.

FrameSaver Unit's sysDescr (system 1)

The following is an example of the format for the system description (sysDescr [system 1]) for the NMS subsystem in the FrameSaver DSL device:

PARADYNE DSL FrameSaver; Model: *[model number-C or R]*; S/W Release: *(MM.mm.bb [MM=Major.mm=minor.bb=build] format)*; NAM CCA number: *(hardware version in hhhh-hhh format)*; Serial number: *ssssss*

FrameSaver Unit's sysObjectID (system 2)

The following are the system object identifier (sysObjectID [system 2]), or OIDs, for the NMS subsystem in the FrameSaver DSL CSU/DSU and router:

- Diagnostic Feature Set:
  - 9720 CSU/DSU: 1.3.6.1.4.1.1795.1.14.2.4.9.3.1
  - 9783 CSU/DSU: 1.3.6.1.4.1.1795.1.14.2.4.9.2.1
  - 9788 CSU/DSU: 1.3.6.1.4.1.1795.1.14.2.4.9.4.1
  - 9783 Router: 1.3.6.1.4.1.1795.1.14.2.4.11.1.1
  - 9788 Router: 1.3.6.1.4.1.1795.1.14.2.4.11.3.1
- Advanced SLM Feature Set:
  - 9720 CSU/DSU: 1.3.6.1.4.1.1795.1.14.2.4.9.3.2
  - 9783 CSU/DSU: 1.3.6.1.4.1.1795.1.14.2.4.9.2.2
  - 9788 CSU/DSU: 1.3.6.1.4.1.1795.1.14.2.4.9.4.2
  - 9783 Router: 1.3.6.1.4.1.1795.1.14.2.4.11.1.2
  - 9788 Router: 1.3.6.1.4.1.1795.1.14.2.4.11.3.1

NOTE:

The Diagnostic Feature Set OID appears until the Advanced SLM Feature Set is activated from the OpenLane SLM system.

Interfaces Group (mib-2)

Clarification for objects in the Interfaces Group, as defined in RFC 1573 and RFC 1213, which is an SNMPv1 MIB, is provided in this section.

Paradyne Indexes to the Interface Table (ifTable)

Table B-1, Paradyne Interface Objects Information, provides the ifName for each interface type, the ifDescr, and the ifIndex that Paradyne has assigned to each.

Table B-1. Paradyne Interface Objects Information

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Physical Layer			
Network SDSL	DSL Network Interface	Network SDSL; DSL FR NAM; Hardware Version: *hhhh-hhh*	101020001
Ethernet	Ethernet Port	Ethernet Port; DSL FR NAM; Hardware Version: *hhhh-hhh*	101006001
Sync Data Port S01P1	Synchronous Data Port-1	Synchronous Data Port, Slot: 1, Port: 1; DSL FR NAM; Hardware Version: *hhhh-hhh*	101003001
COM	Communications Port	COM Port; DSL FR NAM; Hardware Version: *hhhh-hhh*	101004001
Frame Relay Logical Layer			
FR UNI	Frame relay logical link on the DSL network interface	For the DTE side: Network SDSL of FR DTE; DSL FR NAM; Hardware Version: *hhhh-hhh*	101023001
		For the DCE side: Network SDSL of FR SERVICE; DSL FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on Synchronous Data Port-1	For the user side: Synchronous Data Port of FR DTE, Slot: 1, Port: 1; DSL FR NAM; Hardware Version: *hhhh-hhh*	101016001
		For the network side: Synchronous Data Port of FR SERVICE, Slot: 1, Port: 1; DSL FR NAM; Hardware Version: *hhhh-hhh*	
ATM Cell Logical Layer			
ATM	ATM on the DSL network interface	Network SDSL of ATM; DSL FR NAM; S/W Release: MM.mm.bb; Hardware Version: *hhhh-hhh*	101028001

NetScout Probe Indexes to the Interface Table (ifTable)

For remote monitoring at sites where FrameSaver units are operating with NetScout Probes, use the ifName, ifDescr, and ifIndex provided in Table B-2, NetScout Interface Objects Information.

Table B-2. NetScout Interface Objects Information

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Frame Relay Logical Layer			
Frame Relay 1 Network	Frame relay logical link on the network interface	For the DTE side: RMON (IN/OUT); Network SDSL of FR DTE; DSL FR NAM; Hardware Version: *hhhh-hhh*	1
		For the DCE side: RMON (IN/OUT); Network SDSL of FR SERVICE; DSL FR NAM; Hardware Version: *hhhh-hhh*	
RMON Logical Layer			
RMON Virtual Interfaces	These values are calculated based on the probe's internal circuit index: circuit index + 65.	ALL – VIRTUAL PVC [*interface number*] [*DLCI number*] ALL	65–99,999,999

Standards Compliance for SNMP Traps

This section describes the FrameSaver unit's compliance with SNMP format standards and with its special operational trap features.

All traps have an associated string to help you decipher the meaning of the trap. Strings associated with an interface with a substring containing $ifString have the following format:

'DLCI $dlciNumber "$circuitId" of $ifName frame relay link "$linkName".'

— $dlciNumber is the DLCI number. DLCI $dlciNumber "$circuitId" only appears when a DLCI is associated with the trap.

— $circuitId is the name given to the circuit. It can be an empty string, or a 1–64 byte string within quotes (e.g., "Chicago to New York"), and only appears when a DLCI with "circuitID" is associated with the trap.

— $linkName is the name given to the link. Frame relay $linkName only appears when a frame relay link has been named and is associated with the trap.

— $ifName is the string returned for the SNMP ifName variable.

Examples:
'DLCI 100 "Chicago to New York" of Network DSL frame relay link'
In this example, a DLCI and a frame relay link are associated with the trap.

Typically, the $circuitId is a coded string encoded by the network service provider. The following shows an example.
'DLCI 100 "cc0402–dec0704.RG21" of Network DSL frame relay link'

The unit supports the following traps:

- *Trap: warmStart*
- *Trap: authenticationFailure*
- *Trap: linkUp and linkDown*
- *Trap: enterprise-Specific*
- *Trap: RMON-Specific*

These traps are listed in alphabetical order within each table.

Trap: warmStart

This trap indicates that the FrameSaver unit has been reset and has stabilized.

Table B-3. warmStart Trap

Trap	What It Indicates	Possible Cause
warmStart	FrameSaver unit has just reinitialized and stabilized itself.	■ Reset command sent. ■ Power disruption. *String:* 'Unit reset.'
	Variable-Binding	
	devLastTrapString (devHealthAndStatus.mib)	

Trap: authenticationFailure

This trap indicates that access to the FrameSaver unit was unsuccessful due to lack of authentication.

Table B-4. authenticationFailure Trap

Trap	What It Indicates	Possible Cause
authenticationFailure	Access to the FrameSaver unit was attempted and failed.	■ SNMP protocol message not properly authenticated. ■ Three unsuccessful attempts were made via a Telnet session or locally at the asynchronous terminal to enter a correct login user ID/password combination. ■ IP Address security is enabled and a message was received from the SNMP Manager whose address was not on the list of approved managers. *String:* 'Unauthorized access attempted.' (e.g., 'Unauthorized access attempted from COM port.')
	Variable-Binding	
	devLastTrapString (devHealthAndStatus.mib)	

Trap: linkUp and linkDown

These traps are supported on the following interfaces:

- Physical sublayer interfaces: Network and synchronous data ports
- Logical link layer interfaces: Frame relay

Table B-5. linkUp and linkDown Traps

Trap	What It Indicates
linkDown	A failure on one of the communication interfaces has occurred.
linkUp	One of the failed communication interfaces is up and operational.

The linkUp and linkDown variable-bindings are in Table B-6, linkUp and linkDown Variable-Bindings.

Physical and logical sublayers are represented by the entry in the MIB II Interfaces Table. It is supported by a combination of the Frame Relay Extension MIB and either the Frame Relay Services MIB or the Frame Relay DTEs MIB.

Table B-6. linkUp and linkDown Variable-Bindings (1 of 3)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer		
Network (Supported by an entry in the MIB-II Interfaces Table.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.mib)	■ linkDown – One or more alarm conditions are active on the interface. Alarm conditions include: – Loss of Signal (LOS) – Signal-to-Noise (S/N) Net Margin Threshold exceeded *Strings:* '$ifString down.' (e.g., 'Network DSL down due to LOS.') '$ifString administratively shut down.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the interface. *String*: '$ifString up.'

Table B-6. linkUp and linkDown Variable-Bindings (2 of 3)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer *(continued)*		
Synchronous Data Port (Supported by the media-specific RS232-like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.mib)	■ linkDown – One or more alarm conditions are active on the port. Alarm conditions include: – DTR off. The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state. – RTS off. The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state. – Not DTR or RTS, but link is down. *Strings:* '$ifString $alarmString down.' (e.g., `Sync Data Port S01P1 DTR and RTS down.') '$ifString administratively shut down.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the port. *String:* '$ifString up.'
Ethernet Port (Supported by an entry in the MIB-II Interfaces Table.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.mib)	■ linkDown – Communication is not possible over the Ethernet port. – Loss of Signal (LOS) – Loss of Frame (LOF) – Loss of Link (LOL) – Loss of Signal Quality – LPR Events *Strings:* '$ifString down.' '$ifString administratively shut down.' (Due to an intentional shutdown.) ■ linkUp – Communication on the Ethernet port is restored. *String:* '$ifString up.'

Table B-6. linkUp and linkDown Variable-Bindings (3 of 3)

Interface	Variable-Bindings	Possible Cause
Frame Relay Logical Link Sublayer – Represented by entry in MIB II Interfaces Table.		
Synchronous Data Port *(CSU/DSU only)* Service Side of the Frame Relay UNI (Supported by the Frame Relay Extension MIB and media-specific Frame Relay Services MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.mib)	■ linkDown – LMI is down for the LMI Protocol configured, or Frame Relay link is disabled. If LMI Protocol is not configured, a linkUp/linkDown trap is based solely on whether the interface is enabled or disabled. *Strings:* '$ifString LMI down.' (No alarms exist on the link.) '$ifString administratively shut down.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$ifString up.'
Network (Supported by the Frame Relay Extension MIB and media-specific Frame Relay DTE's MIB.)		
ATM Logical Link Sublayer		
Network (Supported by an entry in the MIB-II Interfaces Table.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.mib)	■ linkDown – One or more alarm conditions are active on the link. – Loss of Cell Delineation *Strings:* '$ifString down.' (The physical link is down.) '$ifString down due to Loss of Cell Delineation.' '$ifString administratively shut down.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the link. *String:* '$ifString up.'

Trap: enterprise-Specific

These traps indicate that an enterprise-specific event has occurred. Supported enterprise-specific traps are listed alphabetically below.

Table B-7. enterprise-Specific Traps and Variable-Bindings (1 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseCIR-Change(15)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciCIR (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.mib)	CIR has changed due to the LMI report. LMI Protocol is set to Standard and the network's CIR changed. *String:* 'CIR on $ifString changed to $CIR bps.'
enterpriseConfig-Change(6)	■ devLastTrapString (devHealthAndStatus.mib)	Configuration has been changed via the menu-driven user interface, an SNMP Manager, or auto-configuration after 60 seconds has elapsed without another change. *String:* 'Device configuration change.'
enterpriseDLCI-delete(17)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.mib)	The DLCI has been deleted. The network no longer supports the DLCI, and it was removed. *String:* '$ifString deleted by Auto-DLCI delete.'
enterpriseDLCI-Down(11)		DLCI Status is set to Inactive; the DLCI is down. *Strings:* '$ifString down.' (Due to LMI or physical failure.) '$ifString administratively shutdown.' (Due to an intentional shutdown.)
enterpriseDLCI-Up(12)		DLCI Status is set to Active; DLCI is up again. *String:* '$ifString up.'
enterpriseLatency-Exceeded(21)	■ ifIndex (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib	An IP SLV latency threshold has been exceeded for a particular Class of Service for a path. *String:* 'Latency exceeded *xxx.xxx.xxx.xxx*, COS *nn*, DLCI *nnnn*'

Table B-7. enterprise-Specific Traps and Variable-Bindings (2 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseLatency-Restored(121)	■ ifIndex (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib	An IP SLV latency value has gone back below a threshold for a particular Class of Service for a path. *String:* 'Latency restored *xxx.xxx.xxx.xxx*, COS *nn*, DLCI *nnnn*'
enterpriseMissed-SLVDown(16)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciMissedSLVs (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.mib)	SLV Timeout Error Event Threshold has been exceeded. *String:* 'SLV down on $ifString due to excessive SLV packet loss. Total SLV packets lost is $numLost.'
enterpriseMissed-SLVUp(116)		SLV Timeout Error Event has been cleared. *String:* 'SLV up on $ifString because SLV communication was reestablished. Total SLV packets lost is $numLost.'
enterprisePath-Down(19)	■ ifIndex (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib	A path on the network interface has become unavailable. *String:* 'Path *xxx.xxx.xxx.xxx* Down, DLCI *nnnn*'
enterprisePath-Up(20)	■ ifIndex (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib	A path on the network interface has become available. *String:* 'Path *xxx.xxx.xxx.xxx* Up, DLCI *nnnn*'
enterpriseRmon-ResetToDefault(13)	■ devLastTrapString (devHealthAndStatus.mib)	All RMON-related option changes have been reset to their default values. Default Factory Configuration settings have been reloaded, returning RMON-related options to their original settings. *String:* 'RMON database reset to defaults.'
enterpriseSelfTest-Fail(2)	■ devLastTrapString (devHealthAndStatus.mib)	Unit has completed (re)initialization and a hardware failure was detected. *String:* 'Self test failed: $*s*.' ($*s* is the contents of devSelfTestResult.)

Table B-7. enterprise-Specific Traps and Variable-Bindings (3 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseTest-Start(5)	For physical interfaces and frame relay links: ■ ifIndex (RFC 1573) ■ .0.0 (placeholder) ■ devLastTrapString (devHealthAndStatus.mib)	At least one test has been started on an interface or virtual circuit. *String:* '$testString test started on $ifString.' (e.g., 'DTE Loopback test started on Sync Data Port S01P1.')
enterpriseTest-Stop(105)	For virtual circuits (DLCIs): ■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.mib)	All tests have been halted on an interface or virtual circuit. *String:* '$testString test stopped on $ifString.' (e.g., 'Disruptive PVC Loopback test stopped on DLCI 100 of Sync Data Port S01P1 frame relay.')

Trap: RMON-Specific

Two traps are defined to support the Alarm and Events Groups of RMON. See *RMON Alarm and Event Defaults* on page B-14 for the default values that will generate RMON-specific traps.

Table B-8. RMON-Specific Traps and Variable-Bindings

Trap	Variable-Bindings	Possible Cause
risingAlarm	■ alarmIndex (RFC 1757) ■ alarmVariable (RFC 1757) ■ alarmSampleType (RFC 1757) ■ alarmValue (RFC 1757) ■ alarmRisingThreshold or alarmFalling Threshold (RFC 1757) ■ devLastTrapString (devHealthAndStatus.mib)	Object being monitored has risen above the set threshold. *String:* 'Change in $variableName $typeString threshold of $alarmRisingThreshold by $ (alarmValue – AlarmRisingThreshold.')
fallingAlarm	■ alarmIndex (RFC 1757) ■ alarmVariable (RFC 1757) ■ alarmSampleType (RFC 1757) ■ alarmValue (RFC 1757) ■ alarmFallingThreshold (RFC 1757) ■ devLastTrapString (devHealthAndStatus.mib)	Object being monitored has fallen below the set threshold. *String:* 'Change in $variableName $typeString threshold of $alarmRisingThreshold by $ (alarmValue – AlarmRisingThreshold.')

RMON Alarm and Event Defaults

The FrameSaver unit supports automatic generation of RMON alarm and event information. Each alarm sets an SNMP variable to monitor. Thresholds are set using the OpenLane SLM System. When the threshold set for the monitored variable is exceeded, an SNMP trap is sent or an event is logged.

Event Defaults

Since all events sent are under the control of the FrameSaver unit, there is no need to define multiple events for each alarm type, so only the following two events need to be generated:

eventIndex	eventDescription	eventType
1	Default SLV Rising Event	log-and-trap(4)
2	Default SLV Falling Event	log-and-trap(4)

The following alarm default tables show how each RMON default alarm is set by the FrameSaver unit, alarm and event types, interval used when generating alarms, and alarm thresholds.

- Table B-9, Network Physical Interface Alarm Defaults
- Table B-10, Frame Relay Link Alarm Defaults
- Table B-11, DLCI Alarm Defaults

See *Standards Compliance for SNMP Traps* on page B-6 for information about how traps work, and *Trap: RMON-Specific* on page B-13 for traps specific to remote monitoring.

Rising Event Operation

If a rising threshold is crossed during the interval shown in a table (e.g., frames dropped by the network), the event is armed and an alarm is generated at the end of the interval. Only one alarm per event per interval is generated. The alarm condition persists until the event has been disarmed (reset).

The event is disarmed when a falling threshold has been crossed and the rising threshold has not been crossed during an interval, allowing the event to return to its original disarmed state.

Network Physical Interface Alarm Defaults

This alarm only applies to the FrameSaver unit's network interface.

Table B-9. Network Physical Interface Alarm Defaults

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Threshold Default	
					Rising	Falling
Unavailable Seconds	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* pdnIfExtTotalUASs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.12.1.1.1.4.**I**	900 secs (15 mins)	Rising	1	1

[1] D = Delta: The calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID for the frame relay link.

Frame Relay Link Alarm Defaults

These alarms apply to the FrameSaver unit's frame relay link interfaces. They are created during RMON initialization.

Table B-10. Frame Relay Link Alarm Defaults (1 of 2)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Threshold Default	
					Rising	Falling
Invalid Frames	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxIlFrames *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.18.**I**	900 secs (15 mins)	Rising	1	1
Short Frames	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxShort *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.6.**I**	900 secs (15 mins)	Rising	1	1
Long Frames	D	MIB: pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxLong *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.7.**I**	900 secs (15 mins)	Rising	1	1
Rx Discards	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxDiscards *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.15.**I**	900 secs (15 mins)	Rising	1	1

[1] D = Delta: The calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID for the frame relay link.

Table B-10. Frame Relay Link Alarm Defaults (2 of 2)

Item	Sample Type[1]	MIB/Tag/OID[2]	Interval	Event Type	Threshold Default	
					Rising	Falling
Tx Discards	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTxDiscards *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.14.**I**	900 secs (15 mins)	Rising	1	1
Rx Total Errors	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotRxErrs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.20.**I**	900 secs (15 mins)	Rising	1	1
Tx Total Errors	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotTxErrs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.19.**I**	900 secs (15 mins)	Rising	1	1
Rx Overruns	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxOverruns *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.28.**I**	900 secs (15 mins)	Rising	1	1
Tx Underruns	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTxUnderruns *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.29.**I**	900 secs (15 mins)	Rising	1	1
Rx Non-octet Aligns	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxNonOctet *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.16.**I**	900 secs (15 mins)	Rising	1	1
Rx CRC Errors	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxCrcErr *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.17.**I**	900 secs (15 mins)	Rising	1	1
Total LMI Errors	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotalLMIErrs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.32.**I**	900 secs (15 mins)	Rising	1	1

[1] D = Delta: The calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID for the frame relay link.

DLCI Alarm Defaults

These alarms apply to all DLCIs on the network interface and can be created during RMON initialization or when a DLCI is created. They are placed in the Paradyne alarm area and are listed alphabetically in Table B-11, DLCI Alarm Defaults.

Table B-11. DLCI Alarm Defaults (1 of 2)

Item	Sample Type[1]	MIB/Tag/OID[2]	Interval	Event Type	Threshold Default	
					Rising	Falling
Average Latency	A	MIB: pdn_FrExt.mib (Enterprise) Tag: devFrExtLatencyAvg OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.5.**I.D**	900 secs (15 mins)	None	Must be configured	0
Congested Seconds	D	MIB: pdn_FrExt.mib (Enterprise) Tag: devFrExtDlciStsCongestedSecs OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.6.**I.D**	60 secs (1 min)	Rising	5	5
Current Latency	A	MIB: pdn_FrExt.mib (Enterprise) Tag: devFrExtLatencyLatest OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.7.**I.D**	60 secs (1 min)	None	Must be configured	0
DLCI Inactive Seconds	D	MIB: pdn_FrExt.mib (Enterprise) Tag: devFrExtDlciStsInactiveSecs OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.2.**I.D**	900 secs (15 mins)	Rising	1	1
Frames Dropped by Network	D	MIB: pdn_FrExt.mib (Enterprise) Tag: devFrExtDlciNetDropFr OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.20.**I.D**	60 secs (1 min)	Rising	1	1
Frames Received	D	MIB: Frame Relay DTE MIB (RFC 2115) Tag: frCircuitReceivedFrames OID: .1.3.6.1.2.1.10.32.2.1.8.**I.D**	60 secs (1 min)	None	Must be configured	0
Frames Sent	D	MIB: Frame Relay DTE MIB (RFC 2115) Tag: frCircuitSentFrames OID: .1.3.6.1.2.1.10.32.2.1.6.**I.D**	60 secs (1 min)	None	Must be configured	0

[1] D = Delta: The calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID for the frame relay link.
D = DLCI number.

Table B-11. DLCI Alarm Defaults (2 of 2)

Item	Sample Type[1]	MIB/Tag/OID [2]	Interval	Event Type	Threshold Default	
					Rising	Falling
Maximum Latency	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLatencyMax *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.6.**I.D**	60 secs (1 min)	0	Maximum capability	0
Missing Latency Responses	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciMissedSLVs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.23.**I.D**	900 secs (15 mins)	Rising	5	5
Rx BECNs	D	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs *OID:* .1.3.6.1.2.1.10.32.2.1.5.**I.D**	60 secs (1 min)	Rising	1	1
Rx DLCI Link Utilization	D	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets *OID:* .1.3.6.1.2.1.10.32.2.1.9.**I.D**	60 secs (1 min)	Rising	70% of link capability	65% of link capability
Rx FECNs	D	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs *OID:* .1.3.6.1.2.1.10.32.2.1.4.**I.D**	60 secs (1 min)	Rising	1	1
Tx CIR Utilization	D	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets *OID:* .1.3.6.1.2.1.10.32.2.1.7.**I.D**	60 secs (1 min)	None	Must be configured	0
Tx DLCI Link Utilization	D	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets *OID:* .1.3.6.1.2.1.10.32.2.1.7.**I.D**	60 secs (1 min)	Rising	70% of link capability	65% of link capability
Tx Frames Exceeding CIR	D	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciTxFrOutCIR *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.17.**I.D**	60 secs (1 min)	None	Must be configured	0

[1] D = Delta: The calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID for the frame relay link.
D = DLCI number.

OID Cross-References

The FrameSaver unit supports automatic generation of RMON alarm and event information. Each alarm sets an SNMP variable to monitor. When the threshold set for the monitored variable is exceeded, an SNMP trap is sent and/or a log entry is made.

See Table B-12, History OID Cross-Reference, for an RMON history OID cross-reference and Table B-13, Alarm OID Cross-Reference, for an RMON alarm OID cross-reference.

Table B-12. History OID Cross-Reference (1 of 4)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.2.1.2.2.1. . .		
.1.3.6.1.2.1.2.2.1.**5.I**	SDSL Interface Rate (Link Speed)	*MIB:* MIB II (RFC 1573) *Tag:* ifSpeed
.1.3.6.1.2.1.2.2.1.**10.I**	All DLCI + LMI Rx Octets	*MIB:* MIB II (RFC 1573) *Tag:* ifInOctets
.1.3.6.1.2.1.2.2.1.**11.I**	Received Frames	*MIB:* MIB II (RFC 1573) *Tag:* ifInUcastPkts
.1.3.6.1.2.1.2.2.1.**16.I**	All DLCI + LMI Tx Octets	*MIB:* MIB II (RFC 1573) *Tag:* ifOutOctets
.1.3.6.1.2.1.2.2.1.**17.I**	Sent Frames	*MIB:* MIB II (RFC 1573) *Tag:* ifOutUcastPkts
.1.3.6.1.2.1.2.10.32.2.1. . .		
.1.3.6.1.2.1.10.32.2.1.**4.I**.**D**	Rx FECNs	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.**5.I**.**D**	Rx BECNs	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.**6.I**.**D**	Tx Frames	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.**7.I**.**D**	Tx Octets	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**8.I**.**D**	Rx Frames	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.**9.I**.**D**	Rx Octets	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets

[1] D = DLCI number
I = Interface ID for the frame relay link
P = Protocol index
H = Host control index
N = Additional numeric index used by tables, like frame/burst size
T = Time mask

Table B-12. History OID Cross-Reference (2 of 4)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.**3.I**.**D**	DLCI CIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciCIR
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.**7.I**.**D**	Tx DEs	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciTxDE
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.**8.I**.**D**	Tx BECNs	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrCircuitTxBECN
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.**17.I**.**D**	Tx Frames Above CIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciTxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.**18**.I.**D**	Rx Frames Above CIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciRxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.**20.I**.**D**	Network Frames Lost	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciNetDropFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**22.I** .**D**	Rx DEs	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciRxDE
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**37.I**.**D**	Network Frames Offered	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciRmtOffFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**39.I**.**D**	Network Frames Offered In CIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciRmtOffFrInCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**41.I**.**D**	Network Frames Dropped In CIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciDropOffFrInCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**43.I.D**	Network Frames Offered Above CIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciRmtOffFrOutCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**45.I.D**	Network Frames Lost Above CIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciRmtDropFrOutCir
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.**55.I .D**	Network Frames Offered Above CIR Within EIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciDropFrCirToEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**57.I .D**	Network Frames Dropped Above CIR Within EIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciRxFrNetDropCirToEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**59.I .D**	Network Frames Offered Above EIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciOfferedFrOverEir

[1] D = DLCI number
I = Interface ID for the frame relay link
P = Protocol index
H = Host control index
N = Additional numeric index used by tables, like frame/burst size
T = Time mask

Table B-12. History OID Cross-Reference (3 of 4)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**61.I .D**	Network Frames Dropped Above EIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciRxFrNetDropOverEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.**63.I .D**	DLCI EIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.**I**	Unavailable Seconds	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* pdnIfExtTotalUASs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.2.I.D**	Inactive Seconds	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciStsInactiveSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.5.I.D**	Average Latency	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.6.I.D**	Maximum Latency	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLatencyMax
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.8.I.D**	Latency Packet Size	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLatencyPacketSz
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.2 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.2.**1.2.I.D.N**	Frame Size Upper Limit (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtFrameSzUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.2.**1.3.I.D.N**	Frame Size Count (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtFrameSzCount
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1.**2.I.D.N**	Burst Upper Limit (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtBurstUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1.**3.I.D.N**	Burst Octets (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtBurstOctets
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1.**4.I.D.N**	Burst Frames (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtBurstFrames

[1] D = DLCI number
I = Interface ID for the frame relay link
P = Protocol index
H = Host control index
N = Additional numeric index used by tables, like frame/burst size
T = Time mask

Table B-12. History OID Cross-Reference (4 of 4)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**2.I**	LMI Unavailable Seconds	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkNoLMISecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**6.I**	Rx Short Frames	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxShort
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**7.I**	Rx Long Frames	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxLong
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**11.I**	LMI Sequence Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkSeqErr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**15.I**	Rx Discards	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**16.I**	Rx Non-octet Aligns	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxNonOctet
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**17.I**	Total Rx CRC Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxCrcErr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**18.I**	Rx Illegal Frames	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxIlFrames
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**19.I**	Total Tx Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**20.I**	Total Rx Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**32.I**	Total LMI Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotLMIErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1.**2.I.N**	Port Burst Upper Limits (1–4)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkUtilUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1.**3.I.N**	Rx Port Burst Octets (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) Tag: devFrExtLinkUtilRxOctets
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1.**4.I.N**	Tx Port Burst Octets (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkUtilTxOctets

[1] D = DLCI number
I = Interface ID for the frame relay link
P = Protocol index
H = Host control index
N = Additional numeric index used by tables, like frame/burst size
T = Time mask

See Table B-13, Alarm OID Cross-Reference, for an RMON alarm OID cross-reference.

Table B-13. Alarm OID Cross-Reference (1 of 2)

Object ID (OID)[1]	Item	MIB/Tag
.1.3.6.1.2.1.10.32.2.1. . .		
.1.3.6.1.2.1.10.32.2.1.**4.I.D**	Rx FECNs	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.**5.I.D**	Rx BECNs	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.**6.I.D**	Frames Sent	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx CIR Utilization	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx DLCI Link Utilization	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**8.I.D**	Frames Received	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.**9.I.D**	Rx DLCI Link Utilization	*MIB:* Frame Relay DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.17.I.D**	Tx Frames Exceeding CIR	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciTxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.20.I.D**	Frames Dropped by Network	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* frFrExtDlciNetDropFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.23.I.D**	Missing Latency Responses	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciMissedSLVs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.6.I.D**	Congested Seconds	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciStsCongestedSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.2.I.D**	Inactive Seconds	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtDlciStsInactiveSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.5.I.D**	Average Latency	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.7.I.D**	Current Latency	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLatencyLatest

[1] D = DLCI number
I = Interface ID for the frame relay link
N = Additional numeric index used by tables, like frame/burst size

Table B-13. Alarm OID Cross-Reference (2 of 2)

Object ID (OID)[1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**4.2.1.2.I.N**	Frame Size Upper Limits (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtFrameSzUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**4.2.1.3.I.N**	Frame Size Count (1–5)	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtFrameSzCount
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**6.I**	Rx Short Frames	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxShort
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**7.I**	Rx Long Frames	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxLong
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**11.I**	LMI Sequence Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkSeqErr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**14.I**	Tx Discards	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**15.I**	Rx Discards	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**16.I**	Rx Nonoctet Aligns	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxNonOctet
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**17.I**	Rx CRC Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxCrcErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**18.I**	Rx Illegal Frames	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxIlFrames
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**19.I**	Tx Total Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**20.I**	Rx Total Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**28.I**	Rx Overruns	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkRxOverruns
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**29.I**	Tx Underruns	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTxUnderruns
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**32.I**	Total LMI Errors	*MIB:* pdn_FrExt.mib (Enterprise) *Tag:* devFrExtLinkTotalLMIErrs

[1] D = DLCI number
I = Interface ID for the frame relay link
N = Additional numeric index used by tables, like frame/burst size

Router CLI Commands, Codes, and Designations

C

CLI Commands

The FrameSaver DSL Router is managed with text commands from the Command Line Interface (CLI). The CLI can be accessed:

- Locally via a PC or asynchronous terminal connected to the COM port.
- Remotely via a Telnet session.

The conventions used in the command line syntax are shown below.

Convention	Translation
[ ]	Brackets indicate an optional element.
{ }	Braces indicate a required entry.
|	Vertical bars separate mutually exclusive elements. Enter one element only.
[{ }]	Braces within brackets indicate a required choice within an optional element.
Italics	Entry is a variable, which must be supplied by the operator.
Bold	Entry, or the minimum characters that can be entered, must be typed as shown.
x.x.x.x	32-bit IP address and mask information where *x* is an 8-bit weighted decimal notation.
xx:xx:xx:xx:xx:xx	MAC address information where *x* is a hexadecimal notation.

With the exception to the Login ID and Password, the CLI is not case-sensitive.

Refer to *Navigating the Router's CLI* in Chapter 2, *User and Command Line Interfaces, and Basic Operation,* for additional information.

This appendix contains the following tables for commands:

- Table C-1, Pager Command
- Table C-2, Access Control Commands
- Table C-3, Configuration Commands
- Table C-4, Interface Commands
- Table C-5, IP Routing Commands
- Table C-6, Bridge Commands
- Table C-7, ARP Commands
- Table C-8, NAT Commands
- Table C-9, DHCP Server Commands
- Table C-10, DHCP Relay Agent Commands
- Table C-11, Filter Commands
- Table C-12, Diagnostic Commands
- Table C-13, Show Commands

In addition, the following tables are used in the commands above.

- Table C-12, Diagnostic Commands
- Protocol and Port Designations
  - Table C-15, ICMP Designations
  - Table C-16, TCP Port Designations
  - Table C-17, UDP Port Designations

Pager Command

The pager command allows you to enable or disable screen paging for a CLI session, and enter comments at the command line, which is useful when adding comments within scripts.

Table C-1. Pager Command

[no] pager
Minimum Access Level modes: **Operator** Command Mode: **All modes**
Allows you to control the flow of uninterrupted output to the screen. Information added after the **!** at the command line is ignored. **pager** – Enables display paging. When enabled and there are more than 23 lines to display, **more** displays on line 24. This is the default each time a session is started. – Press the Spacebar to view the next screen. – Press the Enter key to display the next line. – Press the **q** key, **Ctrl-c**, or any other key to return to the command line. **no pager** – Disables paging, and the entire output is sent to the screen without interruption.

Access Control Commands

Access control commands allow you to end a session. For password and changing access commands, see *Controlling Router CLI Access* in Chapter 6, *Security and Logins*.

Table C-2. Access Control Commands

end
Minimum Access Level: **Administrator** Command Mode: **All config modes**
Allows you to exit any configuration mode and return to standard operating mode.
exit
Minimum Access Level: **Operator** Command Mode: **All modes**
Allows you to exit the current mode or end the session. If configuration changes have been made when **exit** is entered, the **There are unsaved configuration changes. Are you sure you want to exit? (no, yes)** prompt appears. – If **yes** is entered, the router leaves configuration mode and any configuration changes are lost. – If **no** is entered, the configuration prompt is returned to so you can save your changes. If in standard operating mode when **exit** is entered, the session is ended and you are returned to the Main Menu.

Configuration Commands

Configuration control commands put the router in configuration mode and allows you to save configuration changes. To show a configuration, see Table C-13, Show Commands.

Table C-3. Configuration Commands

configure {terminal | factory}
Minimum Access Level: **Administrator** Command Mode: **config**
Causes the router to enter configuration mode. The router stays in configuration mode until the **exit** command is entered or the session times out. Example: **configure terminal** NOTES: When in configure mode: – SNMP **set** commands or changes saved from the menu-driven user interface for router configuration are prevented; an in use message is generated. – Router sub-interfaces and/or DLCIs cannot be added or deleted via the menu-driven user interface's CreatePVC function key. – The number of configuration commands that can be entered without performing a **save** is limited; a warning message is generated. – The only **show** command available is **show configuration**. **terminal** – Enter configuration mode and a copy of the currently running configuration is loaded into the edit buffer. Any changes made in the buffer overwrite the copied current configuration when the **save** command is entered, the configuration is saved to the currently running configuration (terminal), and an automatic reset is performed. **factory** – Enter configuration mode and a copy of the factory default settings is loaded into the edit buffer. Any changes made in the buffer overwrite the copied default settings when the **save** command is entered, the configuration is saved to the currently running configuration (terminal), and an automatic reset is performed. This is the default.
save
Minimum Access Level: **Administrator** Command Mode: **All config modes**
Causes configuration changes to be saved to the currently active configuration, and the router to be reset. If the **save** command is entered and changes made require a reboot of the device, a prompt states that a reset is required for the changes to take effect. – If **yes** is entered, changes are stored and the device resets automatically. A message displays when the save is complete. – If **no** is entered, you stay in configuration mode.

Interface Commands

Interface commands allow you to configure the Ethernet and network interfaces, and their sub-interfaces.

Table C-4. Interface Commands (1 of 3)

`interface` *intf-type intf-num* **`no interface`** *intf-type intf-num.sub-intf-num* **`[point-to-point]`**
Minimum Access Level: **Administrator** Command Mode: **config, config-if, config-subif**
Allows you to enter interface or sub-interface configuration mode and create sub-interfaces. All commands entered while in interface or sub-interface configuration mode are applied to the specified interface or sub-interface. No sub-interfaces are enabled by default. Example: **`interface serial 132.53.4.2 132.53.4.250`** Use the **`no interface`** command to delete sub-interfaces while in **config** mode. The command does not delete interfaces. When a sub-interface that is currently in use is deleted, all sub-interface uses are automatically removed from the system configuration. This includes all route entries destined for the sub-interface; ip addresses and subnets for the sub-interface; and all frame relay DLCIs, bridge group assignments, and ip nat inside/outside assignments configured on the sub-interface. ***intf-type*** – Serial interface is supported, the frame relay serial interface (SDSL network interface). ***intf-num*** – Interface index number for the Serial interface. Valid range is from 0 up to the maximum number of serial interfaces, minus one. ***sub-intf-num*** – Sub-interfaces are only supported on the network interface (Serial 0). Valid range for the sub-interface is 0–4,294,967,295. **point-to-point** – Specifies a point-to-point sub-interface. By default, all sub-interfaces are point-to-point.

Table C-4. Interface Commands (2 of 3)

`ip address` *ip-addr subnet-mask* **`no ip address`** **[***ip-addr subnet-mask***]**
Minimum Access Level: **Administrator** Command Mode: **config-if** (Ethernet), **config-subif** (Serial)
Assigns an IP address to the Ethernet interface or a Serial port sub-interface. No IP addresses are assigned to interfaces or sub-interfaces by default. Example: **`ip address 132.53.4.2 255.255.255.255`** Use the **`no ip address`** command to remove an IP address assigned to an interface or sub-interface, and disable IP processing on the interface. The following rules apply: ■ Each sub-interface must be assigned to a different subnet. ■ A customer data IP address and subnet mask must be different from any IP address used for management. ■ When an IP address and subnet mask are assigned to an interface or sub-interface, the device automatically creates a routing table entry with the same destination address and subnet mask, saying that IP addresses within that range are directly reachable on the interface. This is the *interface route*. ■ If the maximum number of static routes have already been configured, you cannot assign an IP address to the interface or sub-interface. ■ When an interface address and subnet mask are deleted, any routing entries with a Next Hop Router address that fall within the interface's address range are deleted automatically. ***ip-address*** – IP address of the interface or sub-interface. ***subnet-mask*** – Subnet mask to be used when the IP address is being compared during route table lookups. The subnet mask cannot be 0.0.0.0 and only contiguous, left-justified subnet masks are allowed.
`encapsulation` *encapsulation-type encapsulation-protocol*
Minimum Access Level: **Administrator** Command Mode: **config-if** (Serial)
Specifies the type of encapsulation on an interface. Example: **`encapsulation frame-relay ietf`** ***encapsulation-type*** – Specifies Frame Relay encapsulation on the serial interface. The default is **frame-relay**. ***encapsulation-protocol*** – Specifies RFC 1490 encapsulation protocol on the serial interface. The default is **ietf**.

Table C-4. Interface Commands (3 of 3)

[no] ip unnumbered [null 0]
Minimum Access Level: **Administrator** Command Mode: **config-subif**
Enables or disables IP processing on a serial sub-interface without assigning an explicit address. The **no ip unnumbered** command removes any IP address assigned to the interface and disables IP processing on the interface. The default is that IP processing is disabled. Example: **ip unnumbered** When an interface IP address and subnet mask are deleted via the **no ip unnumbered** command, any routing entries with a Next Hop Router address that fall within the interface's address range are deleted automatically.
[no] frame-relay interface-dlci *dlci-num*
Minimum Access Level: **Administrator** Command Mode: **config-subif**
Specifies or removes a DLCI on a sub-interface configured for frame relay encapsulation. Only one DLCI may be configured per sub-interface. Example: **frame-relay interface-dlci 103** ***dlci-num*** – Any valid DLCI number that is not already in use on the interface. Range for DLCI numbers is 16–1007. The default is None.

IP Routing Commands

Internet Protocol (IP) routing commands are used to enable and disable IP routing, and to create or delete static routes in the routing table.

To show IP routing and performance statistics, see Table C-13, Show Commands.

Table C-5. IP Routing Commands

ip route *dest-ip dest-mask* **{***next-hop-ip* **|** ***i****ntf-type intf-num* **[.***sub-intf-num***] }** **no ip route** *dest-ip dest-mask* **[***next-hop-ip* **|** *intf-type intf-num* **[.***sub-intf-num***]]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows manual creation or deletion of static route entries. There are no route entries by default. A default gateway destination route may be specified by entering a destination IP address and mask of "0.0.0.0 0.0.0.0" with a default gateway IP address or interface. Example: **ip route 132.53.4.2 255.255.255.255 serial 0.*x*** NOTE: Generally, routes are specified using a next hop address. However, routes over unnumbered point-to-point sub-interfaces should specify the sub-interface to reach the destination. ***dest-ip*** – IP address of the destination host or network or "0.0.0.0" if a default destination gateway is specified. ***dest-mask*** – The subnet mask to be used when the destination IP address is compared during route table lookups. The dest-mask cannot be 0.0.0.0 unless a dest-ip address of 0.0.0.0 has been specified, and only contiguous, left-justified masks are allowed. ***next-hop-ip*** – IP address of the next-hop router used to reach the destination. ***intf-type*** – Two interface types are supported: – **Ethernet** – IEEE 802.3 interface – **Serial** – Frame relay serial interface (SDSL network interface) ***intf-num*** – Valid interface index number for both the Ethernet and Serial interfaces is **0**. ***sub-intf-num*** – Sub-interfaces are only supported on the network interface (Serial 0). If a serial interface is specified, a sub-interface must also be specified. Valid range for a sub-interface is 0–4,294,967,295.
[no] ip routing
Minimum Access Level: **Administrator** Command Mode: **config**
Enables or disables IP routing in the device. The IP routing default is Enable. NOTE: When IP routing is disabled, all static route entries are deleted. However, adding new route entries while IP routing is disabled is not prevented.
[no] ip multicast-routing
Minimum Access Level: **Administrator** Command Mode: **config**
Enables or disables the forwarding of IP multicast packets. The default is Disable.

Bridge Commands

Bridge commands are used to enable or disable simultaneous bridging and routing, configuration of bridge groups and their attributes, and apply or remove bridge groups from an interface or sub-interface.

To show the bridge database or spanning-tree topology, see Table C-13, Show Commands.

Table C-6. Bridge Commands (1 of 2)

bridge {crb | *bridge-group* **{acquire | aging-time** *aging-time* **| protocol** *span-tree-protocol* **| priority** *span-tree-priority* **| route** *route-protocol***}}** **no bridge {crb |** *bridge-group* **{acquire | aging-time[***aging-time***] | priority[***span-tree-priority***] | route [***route-protocol* **] }}**
Minimum Access Level: **Administrator** Command Mode: **config**
A user can enable or disable simultaneous bridging and routing and configure attributes associated with a bridging group. Bridge group 1 is created by default with a priority of 32768 and configured as a learning bridge utilizing the IEEE 802.1 spanning tree protocol. Simultaneous routing and bridging is disabled by default. Once concurrent routing/ bridging is enabled, you must configure an explicit bridge route for any protocol to be routed on interfaces in a bridge group. Example: **bridge crb 1 route ip** **crb** – Enable or disable concurrent routing and bridging on the device. ***bridge-group*** – Bridge group 1 is created by default. If a bridge-group is specified, one of the following attributes **must** be specified: **acquire** – Configure a learning bridge that is capable of dynamically learning new stations. This argument is configured by default on all bridge groups. The **no bridge** command is not accepted for this argument. **aging-time** – Specifies the length of time that an unused dynamic entry is maintained in the bridge table. The **no bridge** command resets the aging-time to the default value. ***aging-time*** – Valid range is 10–1,000,000 seconds. The default is 300. **protocol** – Specify a spanning tree protocol. ***span-tree-protocol*** – Valid spanning tree protocol for IEEE 802.1 protocol is ieee. **priority** – Specify the priority ranking for this bridge. The higher the number, the less likely this bridge will be selected as the spanning tree root. ***span-tree-priority*** – Valid priority values when spanning tree protocol is IEEE.802.1 are: 0–65535. The default is 32768. **route** – Specify a protocol to be routed in this bridge group when concurrent routing and bridging are enabled. ***route-protocol*** – Valid routing protocol is IP.

Table C-6. Bridge Commands (2 of 2)

[no] bridge-group *bridge-group*
Minimum Access Level: **Administrator** Command Mode: **config-if, config-subif**
Allows a user to apply or remove a set of bridge group parameters to/from an interface or sub-interface. When a set of bridge group parameters is applied or removed at the interface level, the command also applies to all sub-interfaces on the interface. Example: **no bridge-group** NOTE: If the bridge group is only required on specific sub-interfaces, remove the bridge group from an interface and apply it at the sub-interface level. ***bridge-group*** – Valid bridge group number **1** is applied to all interfaces by default. Any sub-interfaces created on interfaces where the bridge group is applied inherit the bridge group.
[no] bridge-group *bridge-group* **{input-type-list** *in-access-list-200num* **|** **output-type-list** *out-access-list-200num***}**
Minimum Access Level: **Administrator** Command Mode: **config-if**
Allows a user to specify or remove an input or output Ethernet type code filter for an interface. No bridge group filters are applied to interfaces by default. Example: **bridge-group 1 input-type-list 8069** NOTE: The order in which access-list filters are entered affects the order in which the filters are applied. Each filter is applied in succession until all filters have been applied. If no conditions match, a frame is discarded. ***bridge-group*** – Valid bridge group number **1** is applied to all interfaces by default. Any sub-interfaces created on interfaces where the bridge group is applied inherit the bridge group. **input-type-list** – Specify the filter applied to incoming Ethernet packets by type code. Refer to Table C-14, Ethernet Type Codes (Hex). ***in-access-list-200num*** – The input type access list valid range for protocol type-code access lists: 200–299. **output-type-list** – Specify the filter applied to outgoing Ethernet packets by type code. Refer to Table C-14, Ethernet Type Codes (Hex), Ethernet Type Codes (Hex). ***out-access-list-200num*** – The output type access list number valid range for protocol type-code access lists: 200–299.

ARP Commands

Address Resolution Protocol (ARP) commands are used to create entries in the ARP table, specify how long the information will be retained, and remove dynamic entries in the table.

Table C-7. ARP Commands

arp *ip-address mac-address arp-type* **no arp** *ip-address* **[***mac-address arp-type***]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to create or delete a single, static ARP table entry. Static ARP entries created with this command are permanent and are retained across resets/power cycles. Up to the maximum number of static ARP entries specified may be entered. There are no static ARP entries by default. ***ip-address*** – The IP address of the ARP entry to be created or deleted. ***mac-address*** – MAC address. ***arp-type*** – Specifies the ARP type. Valid ARP type is **arpa**, the standard Ethernet-style ARP (RFC 826).
arp timeout *time* **no arp timeout [***time***]**
Minimum Access Level: **Administrator** Command Mode: **config-if** (Ethernet)
Allows you to specify the amount of time that ARP information is retained in the ARP cache. The **no arp timeout** command restores the default ARP timeout value. Example: **arp timeout 28000** NOTES: – The amount of time the device waits before reattempting to acquire ARP information for incomplete entries is 5 seconds and is not configurable. – The internal ARP timeout timer has one minute precision, so the ARP timeout is implemented by rounding up to the nearest minute. ***time*** – The ARP timeout value in seconds. Valid range is 1–4294967 seconds. The default is 14400.
clear arp-cache
Minimum Access Level: **Administrator** Command Mode: **Standard**
Deletes all dynamic ARP table entries from the ARP cache.

NAT Commands

Network Address Translation (NAT) commands are used to enable or disable NAT on an interface or sub-interface and specify whether IP addresses on the interface are public or private.

Table C-8. NAT Commands (1 of 3)

[no] ip nat {inside | outside}
Minimum Access Level: **Administrator** Command Mode: **config-if, config-subif**
Allows you to specify if Network Address Translation (NAT) is performed on an interface or sub-interface and whether IP addresses on the interface are private or public addresses. NAT is disabled by default. Example: **ip nat inside** **inside** – Specifies inside (private) IP addresses on this interface. **outside** – Specifies outside (public) IP addresses on this interface.
ip nat translation timeout [*time***]** **no ip nat translation timeout [***time***]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to specify the amount of time that a dynamically configured standard NAT (non-port translation) mapping can remain unused before the mapping is automatically deleted. The default is 24 hours. To reset the timeout to the default, use the **no nat translation timeout** command. Example: **ip nat translation timeout 604800** NOTE: When NAPT is enabled, mappings are automatically deleted based on a separate set of non-configurable timeouts: – UDP translations timeout: 5 minutes. – TCP translations timeout: 24 hours. – ICMP translations timeout: 1 minute. ***time*** – The timeout value in seconds. The valid range is 1–2147483647. The default is 86400 seconds (24 hours).

Table C-8. NAT Commands (2 of 3)

ip nat pool *pool-name start-ip-addr end-ip-addr* **{netmask** *netmask* **| {prefix-length | /}** *prefix-length***}** **no ip nat pool** ***pool-name*** **[***start-ip-addr end-ip-addr* **{netmask** *netmask* **| {prefix-length | /}** *prefix-length***}]**
Minimum Access Level: **Administrator** Command Mode: **config**
Defines a pool of addresses for Network Address Translation. Addresses can then be allocated from the pool as needed. Up to 30 NAT pools can be supported. To remove a pool, use the **no ip nat pool** command. No NAT pools are configured by default. Example: **ip nat pool Largo 132.53.4.2 132.53.4.250 / 24** ***pool-name*** – Name of the pool comprised of 1–20 ASCII printable characters. ***start-ip-addr*** – Starting IP address of the range of addresses in the address pool. ***end-ip-addr*** – Ending IP address of the range of addresses in the address pool. **netmask** – Specify a network mask that indicates which address bits belong to the network and subnet fields, and which bits belong to the host field. ***netmask*** – Network mask of the network for the pool addresses. **prefix-length** or **/** – Specify the number of bits in a network mask address that are ones and define the network and subnet fields. ***prefix-length*** – The number of bits in a network mask address that are ones. Valid range is 1–32.
[no] ip nat inside source **{list** *access-list-1-99num* **pool** *pool-name* **[overload] |** **list** *access-list-1-99num* **interface** ***i****ntf-type intf-num* **[.***sub-intf-num***] overload |** **Static {***static-ip-addr1 static-ip-addr2* **|** *protocol static-ip-addr1 static-port-num static-ip-addr2***}}**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows a user to specify or remove Network Address Translation rules. Both dynamic and static address translations may be specified. Command forms that include an access list are used to specify dynamic translation rules. Packets from addresses that match the access list are translated using addresses allocated from the named pool or the IP address assigned to the interface. No NAT rules are configured by default. Example: Refer to Chapter 4, *Configuration Options*. **inside** – Inside address translation converts an inside (private) IP address to an outside (public) IP address (and port, if overload is specified for NAPT). **source** – Specifies source address translation. **list** – Specify the access list number for *dynamic* address translation. For inside source translation, this access list describes local addresses. If no rules have been created for the specified access list, no translations based on this rule will occur. ***access-list-1-99num*** – A standard IP Access list. The valid range is 1–99. *(Continued on next page)*

Table C-8. NAT Commands (3 of 3)

(Continued from previous page)

pool – Specify the name of a pool of addresses available for dynamic address translation. For inside source translation, this is the pool of local addresses.

pool-name – The name of a NAT pool comprised of 1–20 ASCII printable characters.

interface – For dynamic address translation, specifies an interface or sub-interface that provides the address for the translation. For inside source translation, specifies the interface that provides the global address. If there is no address on the interface, the interface has not been specified as an outside interface, or the interface is not operational, no translations based on this rule will occur. If a public IP address is specified for NAPT on this interface, that address is used instead of the interface's assigned IP address.

intf-type – Two interface types are supported:

Ethernet – IEEE 802.3 interface

Serial – Frame relay serial interface (SDSL network interface)

intf-num – Interface index number for both the Ethernet and Serial interfaces, 0 or 1.

sub-intf-num – Sub-interface number. Sub-interfaces are only supported on the network interface (Serial 0). If a Serial interface is specified, a sub-interface must also be specified. Sub-interface number range is 0–4,294,967,295.

overload – Specifies that Network Address Port Translation (NAPT), also known as Port Address Translation (PAT), is to be used for UDP and TCP.

static – Specifies a fixed, one-to-one mapping between an inside (private) IP address (and port for PAT) and a outside (global) IP address (and port for PAT). For inside source translation, a private address (and port for PAT) is mapped to a global address (and port for PAT). Static inside and outside destination translations are not supported.

static-ip-addr1 – Specifies the first IP address in the *static route*. For inside source translation, this is the local address to be mapped.

static-ip-addr2 – Specifies the second IP address in the *static route.* For inside source translation, this is the global address to be mapped.

protocol – Protocol that applies to this *static* route, which include:

tcp – Transmission Control Protocol

udp – User Datagram Protocol

static-port-num – Specifies the second TCP/UDP port in a *static protocol* route. For inside source translation, this is the local port. It should only be specified when a static protocol translation is specified. Only one static route per protocol can specify a *static-port-num*. The valid range of TCP/UDP ports is 1–65535.

`clear ip nat translation *`

Minimum Access Level: **Administrator**
Command Mode: **Standard**

Allows you to clear all *dynamic* NAT translations from the translation table.

DHCP Server Commands

Dynamic Host Configuration Protocol (DHCP) server commands are used to enable or disable the DHCP server, and create or delete a DHCP pool.

Table C-9. DHCP Server Commands (1 of 3)

[no] service dhcp
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to enable or disable the DHCP server. The DHCP server is enabled by default but is not active until other DHCP server options are configured. When an IP address is assigned to a host by the DHCP Server and there is no matching routing table entry, a host entry for that IP address is created. This entry is deleted from the routing table when the lease expires or the IP address is relinquished. When an IP address is assigned to a host on the local Ethernet by the DHCP Server, an ARP table entry is created mapping that IP address to the corresponding host MAC address. This entry is deleted from the ARP table when the lease expires or the IP address is relinquished. This entry is not deleted according to the timeout mechanism that applies to normal ARP entries. NOTE: The DHCP Relay and DHCP Server cannot be enabled at the same time.
[no] ip dhcp pool *pool-name*
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to create or delete a DHCP pool and places it in DHCP pool configuration mode to configure IP DHCP pool parameters. All commands entered while in DHCP pool configuration mode are applied to the specified DHCP pool. No DHCP pools are configured by default. Example: **ip dhcp pool pool17** ***pool-name*** – The name of the DHCP pool, as 1–20 ASCII printable characters.
[no] ip dhcp excluded-address *ip-addr* **[***end-ip-addr***]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to specify a single IP address, or a range of IP addresses, that the DHCP server should not distribute to clients. The **no ip dhcp excluded-address** command allows you to release previously excluded IP addresses for distribution to clients. No IP addresses are excluded by default. Up to 30 individual or ranges of IP addresses are supported. Example: **ip dhcp excluded-address 132.53.4.2** ***ip-addr*** – Specifies an IP address to exclude, or the first IP address in a range of excluded IP addresses. ***end-ip-addr*** – Specifies the last IP address in a range of excluded IP addresses.

Table C-9. DHCP Server Commands (2 of 3)

lease {*days*[*hours*] [*minutes*]| infinite} **no lease [*days*[*hours*] [*minutes*]|infinite]**
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to specify or clear the lease time for an IP address assigned to a DHCP client. After the lease time has expired, the address assignment is no longer valid. The default lease time is one day. Example: **lease 120 23 0** ***days*** – Number of days the lease is valid. The default is1. Valid range of days is 0–365. ***hours*** – Number of hours the lease is valid. The default is 0. Valid range for hours is 0–24. ***minutes*** – Number of minutes the lease is valid. The default is 0. Valid range for minutes is 0–59. **infinite** – Specifies an infinite lease time. The IP address assignment does not expire.
default-router *ip-address* **no default-router [***ip-address***]**
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to configure or remove the default router IP address provided to clients by the DHCP server. The default router address is provided to the clients in the DHCP reply message from the DHCP server and as the next hop router by the clients. The IP address for the default router should be on the same subnet as the client. Example: **default-router 132.53.4.2** ***ip-address*** – Specifies the IP address of the default router. The default is None.
domain-name *domain-name* **no domain-name [***domain-name***]**
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to specify or remove the domain name provided to clients by the DHCP server. This domain name is provided to the clients in the DHCP reply message from the DHCP server. ***domain-name*** – Specifies a string defining the domain name. The domain name string contains 255 ASCII printable characters. The default is None.
dns-server *ip-address* **no dns-server [***ip-address***]**
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to specify or remove the Domain Name System (DNS) IP address provided to clients by the DHCP server. Example: **dns-server 132.53.4.2** ***ip-address*** – Specifies the IP address of the DNS server.

Table C-9. DHCP Server Commands (3 of 3)

network *network-num* **[[netmask]** *netmask* **| {prefix-length | /}** *prefix-length***]** **no network [***network-num* **[[netmask]** *netmask* **| {prefix-length | /}** *prefix-length***]]**
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to specify or remove a subnet and subnet mask to a DHCP server pool. The configured subnet and subnet mask will specify the range of IP addresses that will be allocated to clients by the DHCP server. Only one network or subnet may be specified for a server pool. Example: **network 8** ***network-num*** – The IP address of the DHCP address pool. **netmask** – Specify a network mask that indicates which address bits belong to the network and subnet fields and which bits belong to the host field. ***netmask*** – The network mask for the pool of IP addresses. **prefix-length** or **/** – Specify the number of bits in a network mask address that are ones and define the network and subnet fields. ***prefix-length*** – Number of ones bits in a network mask address. Valid range is 1–32. NOTES: – If the mask or prefix-length is not specified, the class A, B, or C natural mask is used. – When the DHCP address range is changed, all binding entries and dynamic routes for the clients configured with the old address range are removed.

DHCP Relay Agent Commands

Dynamic Host Configuration Protocol (DHCP) relay agent commands

Table C-10. DHCP Relay Agent Commands

ip dhcp relay max-clients *max-dhcp-clients* **no ip dhcp relay max-clients [***max-dhcp-clients***]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to limit the number of DHCP clients supported. The **no dhcp relay max-agents** command resets the maximum number of DHCP clients supported to the default of 1. Example: **ip dhcp relay max-clients 1** ***max-dhcp-clients*** – Number of DHCP clients supported: 1–256.
[no] ip dhcp-server *ip-address*
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to specify or remove the address of the DHCP server where DHCP requests received on the Ethernet interface are forwarded. When no server address is assigned, the DHCP Relay agent is effectively disabled. NOTE: The DHCP Relay agent cannot be enabled if either the DHCP server or NAT are enabled. ***ip-address*** – IP address of the DHCP server.

Filter (access-list) Commands

Filter commands are used to create or delete Access Lists.

Table C-11. Filter Commands (1 of 4)

access-list *access-list-num* **[{permit | deny}**
{{*source-ip* **[***source-wildcard***] | any | host** *source-host-ip***} |**
{*protocol* **{***source-ip source-wildcard* **| any | host** *source-host-ip***}**
[*src-operator src-port* **[***src-end-port***]]**
{*dest-ip dest-wildcard* **| any | host** *dest-host-ip***}**
[[*icmp-msg-type* **[***icmp-msg-code***]] |**
[*dest-operator dest-port* **[***dest-end-port***]]] }|**
{*type-code* **[range** *end-type-code***] } }**

no access-list *access-list-num* **[{permit | deny}**
{{*source-ip* **[***source-wildcard***] | any | host** *source-host-ip***} |**
{*protocol* **{***source-ip source-wildcard* **| any | host** *source-host-ip***}**
[*src-operator src-port* **[***src-end-port***]]**
{*dest-ip dest-wildcard* **| any | host** *dest-host-ip***}**
[[*icmp-msg-type* **[***icmp-msg-code***]] |**
[*dest-operator dest-port* **[***dest-end-port***]]] } |**
{*type-code* **[range** *end-type-code***] } }**

Minimum Access Level: **Administrator**
Command Mode: **config**

Allows a user to create or delete a rule for an access list. Access lists default to an implicit deny statement for everything. Access lists are terminated by an implicit deny.

access-list-num – The access list number. Valid ranges for access lists are:

1–99 – Standard IP access lists.

100–199 – Extended IP access lists.

200–299 – Protocol type-code access lists.

permit – Specifies to permit access and forward packets matching the criteria.

deny – Specifies to deny access and discard packets matching the criteria.

For Standard IP Access Lists:

Example: **`access-list 1 permit 10.1.1.1`**

source-ip – The source IP Address to match.

source-wildcard – Specifies a 32-bit wildcard mask indicating the bit positions in the source IP address to ignore during matches. This argument must be supplied when a source-ip address is specified.

any – Specifies to match any source host. A source-ip of 0.0.0.0 and a source-wildcard of 255.255.255.255 are specified.

host – Specify a single host source address to match.

source-host-ip – The source host IP address to match.

(Continued on next page)

Table C-11. Filter Commands (2 of 4)

(Continued from previous page)

For Extended IP Access Lists:

Example: **`access-list 100 permit tcp 10.1.1.1 0.0.0.255 20.1.1.1 0.0.0.255`**

protocol – The IP protocol to which the filter will be applied. The following protocols are supported:

ip – Filter applies to all IP packets (including but not limited to ICMP, TCP, and UDP).

icmp – Internet Control Message Protocol.

tcp – Transmission Control Protocol.

udp – User Datagram Protocol.

source-ip – The source IP Address to match.

source-wildcard – Specifies a 32-bit wildcard mask indicating the bit positions in the source IP Address to ignore during matches. This argument must be supplied when a *source-ip* address is specified.

any – Match any source host. A source-ip of 0.0.0.0 and a source-wildcard of 255.255.255.255 are specified.

host – Specify a single host source address to match.

source-host-ip – The source host IP address to match.

dest-ip – The destination IP Address to match.

dest-wildcard – Specifies a 32-bit wildcard mask indicating the bit positions in the destination IP Address to ignore during matches. This argument must be supplied when a dest-ip address is specified.

any – Specifies to match any destination host. A dest-ip of 0.0.0.0 and a dest-wildcard of 255.255.255.255 are specified.

host – Specify a single host address to match.

dest-host-ip – The destination host IP address to match.

icmp-msg-type – Specify a specific ICMP message type to be filtered. Valid if the protocol *s*pecified is icmp. For valid ICMP message types, refer to Table C-15, ICMP Designations. Valid ICMP message type range is 0–255.

icmp-msg-code – Specify a specific ICMP message code to be filtered. Valid if an icmp-msg-type has been specified and the protocol specified is icmp. For valid ICMP message codes, refer to Table C-15, ICMP Designations. Valid ICMP message type range is 0–255.

src-operator – Specifies how the source port is evaluated. This argument may only be specified if the protocol specified is tcp or udp. Valid values are:

eq – Match only packets with a port number equal to the source port number input.

gt – Match only packets with a port number greater than the source port number.

lt – Match only packets with a port number less than the source port number input.

neq – Match only packets with a port number not equal to the source port number.

range – Match only packets in the range of port numbers specified by src-port and src-end-port. If range is specified, enter both a src-port and a src-end-port.

(Continued on next page)

Table C-11. Filter Commands (3 of 4)

For Extended IP Access Lists: *(continued)*

src-port – Specify a TCP or UDP port number to be filtered. Valid if the protocol specified is tcp or udp. Refer to Table C-16, TCP Port Designations, and Table C-17, UDP Port Designations. Valid port number range is 0–65535.

src-end-port – Specifies last TCP or UDP port number in a range of port numbers to be filtered. Valid if the protocol specified is tcp or udp and if src-operator value is range. Refer to Table C-16, TCP Port Designations, and Table C-17, UDP Port Designations. Valid port number range is 0–65535.

dest-operator – Specifies how the destination port is evaluated. This argument may only be specified if the protocol specified is tcp or udp. Valid values are:

eq – Match only packets with a port number equal to the destination port number.

gt – Match only packets with a port number greater than the destination port number.

lt – Match only packets with a port number less than the destination port number.

neq – Match only packets with a port number not equal to the destination port number.

range – Match only packets in the range of port numbers specified by dest-port and dest-end-port. If range is specified, enter both a dest-port and dest-end-port.

dest-port – Specifies a specific TCP or UDP port number to be filtered. This option only applies to a protocol of tcp or udp. Many of the valid TCP and UDP ports are described in Table C-16, TCP Port Designations, and Table C-17, UDP Port Designations. Valid TCP or UDP port number range is 0–65535.

dest-end-port – Specifies last TCP or UDP port number in a range of port numbers to be filtered. This option only applies to a protocol of tcp or udp with dest-operator set to range. Many of the valid TCP and UDP ports are described in Table C-16, TCP Port Designations, and Table C-17, UDP Port Designations. Valid TCP or UDP port number range is 0–65535.

For Protocol Type Access Lists:

Example: **`access-list 200 permit 0x200 range 0x210`**

type-code – Specifies the 16-bit hexadecimal number written with a leading “0x” that specifies either an Ethernet type code or the first Ethernet type code in a range of Ethernet type codes to filter. If a user attempts to a type code that is not a 16-bit hexadecimal number written with a leading “0x”, it will be treated as a syntax error. Many of the Ethernet Type codes distributed by the Xerox Corporation are listed in Table C-14, Ethernet Type Codes (Hex). This option only applies to protocol type-code access lists.

range – Specifies a range of ether-type codes. This option only applies to protocol type-code access lists.

end-type-code – The last ethernet type code included in the filter range. A 16-bit hexadecimal number written with a leading “0x” used to specify one of the Ethernet type codes. This option only applies for protocol type-code access lists.

Table C-11. Filter Commands (4 of 4)

[no] ip access-group *access-list-1-199num* **[in | out]**
Minimum Access Level: Administrator Command Mode: config-if
Allows you to control access to an interface by allowing you to designate (or delete) a set of access rules to be applied to either incoming or outgoing packets. By default, no access lists are applied to interfaces. Example: ip access-group 17 in NOTE: A user may specify that an access list is applied to either inbound packets, outbound packets, or both inbound and outbound packets (two commands). If a specified access list does not exist, all packets are passed. access-list-1-199num – The access list number. The valid ranges for access lists are: **1–99** – Standard IP access lists. **100–199** – Extended IP access lists. **in** – Specifies that filters will be applied to inbound packets. **out** – Specifies that filters will be applied to outbound packets. If no direction (in or out) is specified, the filter is applies to outbound packets by default.

Diagnostic Commands

Diagnostic commands allow you to ping or trace the route to a specified destination.

Table C-12. Diagnostic Commands (1 of 2)

`ping` **[***protocol***]** *dest-ip* **[`source`** *source-ip***] [`length`** *bytes***] [`timeout`** *time***] [`interface`** *intf-type intf-num* **[.***sub-intf-num***]]**
Minimum Access Level: **Operator** Command Mode: **Standard**
Pings the specified destination address. For a successful ping, the results are shown as: Ping reply [*x.x.x.x*]: bytes of data = *packet-length* Where *packet-length* is the length of echo packets sent. For a timeout, the results are shown as: Ping reply [*x.x.x.x*]: REQUEST TIMED OUT For an ICMP echo response of unreachable destination, the results are shown as: Ping reply [*x.x.x.x*]: DESTINATION UNREACHABLE ***protocol*** – The protocol of the IP echo message: ip. ***dest-ip*** – Address of the device to ping. **source** – Specify the source IP address. ***source-ip*** – The source IP address used in the ping request. The default source IP address is the IP address for the interface on which packets are routed to the destination IP address. The source IP address specified must be an IP address assigned to an interface or sub-interface. **length** – Specify the length of echo packets sent. ***bytes*** – Number of data bytes. Range = 0–1500. Default = 64. **timeout** – Specify the time in seconds before the ping test is abandoned. ***time*** – Number in seconds before the ping test is abandoned. Maximum is 30 seconds. Default = 5 seconds. **interface** – Specify the target interface. The default target interface is the interface on which packets are routed to the destination IP address. ***intf-type*** – Two interface types are supported: **Ethernet** – IEEE 802.3 interface **Serial** – Frame relay serial interface (SDSL network interface) ***intf-num*** – The interface index number for the Ethernet and the Serial interfaces: 0. ***sub-intf-num*** – The sub-interface number. Sub-interfaces are only supported on the Network interface (Serial 0). Sub-interface number range is 0–4,294,967,295.

Table C-12. Diagnostic Commands (2 of 2)

`traceroute` **[`protocol`]** *dest-ip* **[`source`** *source-ip*] **[`length`** *bytes*] **[`timeout`** *time*] **[`hops`** *hops*] **[`interface`** *intf-type intf-num* **[.***sub-intf-num***]]**

Minimum Access Level: **Operator**
Command Mode: **Standard**

This command performs the TraceRoute test to the specified destination IP address. The general format of the TraceRoute results is seen as follows:

Tracing route to *x.x.x.x* over a max of *nn* hops, with *nnn* byte packet:

1 <100ms <100ms <100ms *x.x.x.x*

2 <100ms <100ms <100ms *x.x.x.x*

3 <200ms <200ms <200ms *x.x.x.x*

4 <200ms <200ms <200ms *x.x.x.x*

The first column is the hop number, which is the Time to Live (TTL) value set in the IP packet header. Each of the three next columns contains the round-trip time in 100ms intervals for each attempt to reach the destination with that TTL value. If no response is received, an * (asterisk) is displayed in place of the roundtrip time. The fifth column is the IP address of the responding system. If no response is received for a hop, the last column is blank.

protocol – The protocol of the echo message for TraceRoute: ip.

dest-ip – Address of the device to TraceRoute.

source – The source IP address. The default source IP address is the IP address for the interface on which packets are routed to the destination IP address.

source-ip – The source IP address used in the TraceRoute test. The default source IP address will be the IP address for the interface on which packets are routed to the destination IP address. The source IP address specified must be an IP address assigned to an interface or sub-interface.

length – Specify the length of packets sent.

bytes – Number of data bytes. Range = 0–1500. Default = 64.

timeout – Specify the time in seconds before the TraceRoute test is abandoned.

time – Number of seconds before the TraceRoute test is abandoned. Range = 1–30. Default = 5 seconds.

hops – Specify the maximum number of hops to be tested.

hops – The maximum number of hops to be tested. Range = 1–128. Default = 8.

interface – Specify the target interface. The default target interface is the interface on which packets are routed to the destination IP address.

intf-type – Two interface types are supported:

Ethernet – IEEE 802.3 interface

Serial – Frame relay serial interface (SDSL network interface)

intf-num – The interface index number for the Ethernet and the Serial interfaces: 0.

sub-intf-num – The sub-interface number is only supported on the Network interface (Serial 0). The following sub-interface numbers are supported: 0–4,294,967,295.

Show Commands

Show commands allow you to display information.

Table C-13. Show Commands (1 of 4)

show arp

Minimum Access Level: **Operator**
Command Mode: **Standard**

Displays the devices in the ARP table.

The general format of the **show arp** command is:

IP Address	Timeout (min)	MAC address	Type	Interface
x.x.x.x	STATIC	*xx:xx:xx:xx:xx:xx*	ARPA	
x.x.x.x	*time*	*xx:xx:xx:xx:xx:xx*	ARPA	*Interface*

The first column displays the IP address. The second column displays the actual time left for the specific entry, or "STATIC" for configured static entries. The third column displays the MAC address for the ARP entry. The fourth column displays the ARP type (only ARPA is currently supported). The fifth column displays the Interface or sub-interface for the ARP table entry.

show bridge

Minimum Access Level: **Operator**
Command Mode: **Standard**

Displays entries in the bridge forwarding database.

show configuration

Minimum Access Level: **Operator**
Command Mode: **Standard**

Displays/outputs a sequence of commands in the form of ASCII strings that have the effect of setting all configurable parameters to the current values in memory.

Passwords are write-only and not output. The text file can be used with a terminal emulation program. Refer to *Configuring the Router Using Terminal Emulation* in Chapter 5, *Configuring the FrameSaver DSL Router.*

The general format of the **show config** command is:

```
global commands

  !
  interface n
   interface n commands....
  !
  interface n sub-interface n
   interface n sub-interface n commands...
  !
  interface n sub-interface n+1
   interface n sub-interface n+1 commands...
  interface n+1
```

Table C-13. Show Commands (2 of 4)

show configuration {saved | unsaved}
Minimum Access Level: **Administrator** Command Mode: **All config modes**
Displays/outputs a sequence of commands in the form of ASCII strings that have the effect of setting all configurable parameters to the current values, either saved in memory or entered during a current configuration session. Passwords are write-only and not output. The text file can be used with a terminal emulation program. Refer to *Configuring the Router Using Terminal Emulation* in Chapter 5, *Configuring the FrameSaver DSL Router*. The general format of the show config command is the same as the previous command, show configuration, in Standard mode. **saved** – Displays the command sequence for saving parameters currently saved in memory. **unsaved** – Displays the command sequence for saving parameters entered during the current configuration session.
show frame-relay map
Minimum Access Level: **Operator** Command Mode: **Standard**
Displays the status of all frame relay DLCIs seen on the router's frame relay interface. The general format of the **show frame-relay map** command is: *interface* **(***interface-status***):** dlci *dlci-number***,** *dlci-status* Where the *interface* (or sub-interface) shall be displayed in the standard format shown in the Interface Commands. The *interface-status* is up or down. The *dlci-number* is in the range 16–1007. Frame relay map statements are only displayed for DLCIs configured on both the router and on the devices user interface. The *dlci-status* is active or inactive.
show interface [*intf-type intf-num* **[.***sub-intf-num***]]**
Minimum Access Level: **Operator** Command Mode: **Standard**
Shows the status of the named interface, sub-interface, or all interfaces and sub-interfaces on the device. ***intf-type*** – The interface type. The following two types are supported: **Ethernet** – IEEE 802.3 interface **Serial** – Serial interface ***intf-num*** – The interface index number for the Ethernet and the Serial interfaces: 0. ***sub-intf-num*** – The sub-interface numbers are only supported on the Network interface (Serial 0). Sub-interface numbers supported: 0–4,294,967,295.

Table C-13. Show Commands (3 of 4)

show ip dhcp binding [*ip-address***]**
Minimum Access Level: **Operator** Command Mode: **Standard**
Allows users to display address bindings associated with the DHCP server. If the IP address is not specified, all DHCP server bindings are displayed. If an IP address is specified, only the DHCP server binding for the specified client is displayed. ***ip-address*** – Specifies the DHCP client's IP address for the binding to be displayed. The general format of the **show ip dhcp bindings** command is as follows: IP Address MAC address Lease Expires *x.x.x.x* *xx:xx:xx:xx:xx:xx* ddd:hh:mm The first column displays the IP addresses in use. The second column displays the MAC address bound to each IP address. The third column displays the remaining lease time in days, hours, and minutes or "Infinite".
show ip nat translations
Minimum Access Level: **Operator** Command Mode: **Standard**
Shows the active Network Address Translation (NAT) translations. The general format of the **show ip nat translations** command is: Pro Inside global Inside local Outside local Outside global udp *x.x.x.x*:*port* *x.x.x.x*:*port* *x.x.x.x*:*port* *x.x.x.x*:*port* The first column, Pro, displays the Protocol of the port identifying the address. The second column displays the Inside global IP address for one or more inside local IP addresses to the outside world. The third column displays the Inside local IP address assigned to a host on the inside network. The fourth column displays the Outside local IP address of an outside host as it appears to the inside network. The fifth column displays the Outside global IP address assigned to a host on the outside network by its owner. Whenever one of the IP addresses or the Protocol designation does not apply to a NAT table entry, "---" is displayed. A protocol port is appended to IP addresses when NAPT is specified for that NAT entry.
show ip route [*ip-address***]**
Minimum Access Level: **Operator** Command Mode: **Standard**
This command shows the IP route table entry for the specified IP address. If no IP address is specified, the entire table is shown. When the Next Hop IP Address is 0.0.0.0, the host is directly reachable on the interface. The general format of the **show ip route** command will be as follows: Dest. IP Address Dest. Subnet Mask Next Hop IP Addr Interface *x.x.x.x* *x.x.x.x* *x.x.x.x* *interface* *x.x.x.x* *x.x.x.x* *x.x.x.x* *interface* **ip-address** – Specific IP address for route information display.

Table C-13. Show Commands (4 of 4)

show ip traffic
Minimum Access Level: **Operator** Command Mode: **Standard**
Displays the IP statistics for the device.
show spanning-tree
Minimum Access Level: **Operator** Command Mode: **Standard**
Displays the devices spanning-tree topology.

Ethernet Type Codes

Use Table C-14, Ethernet Type Codes (Hex), when specifying the filter applied to incoming Ethernet packets by Type Code. Many of the Type Codes listed below are distributed by Xerox Corporation.

Table C-14. Ethernet Type Codes (Hex) (1 of 2)

Type Code	Description	Type Code	Description
0000–05DC	IEEE802.3 Length Field	803E	DEC Unassigned
010101FF	Experimental	803F	DEC LAN Traffic Monitor
0200	Xerox PUP (see 0A00)	8040–8042	DEC Unassigned
0201	PUP Addr Trans (see 0A01)	8044	Planning Research Corp.
0600	Xerox NS IDP	8046–8047	AT&T
0800	DOD IP	8049	ExperData
0801	X.75 Internet	805B	Stanford V Kernel exp.
0802	NBS Internet	805C	Stanford V Kernel prod.
0803	ECMA Internet	805D	Evans & Sutherland
0804	Chaosnet	8060	Little Machines
0805	X.25 Level 3	8062	Counterpoint Computers
0806	ARP	8065–8066	University of Mass. at Amherst
0807	XNS Compatibility	8067	Veeco Integrated Auto.
081C	Symbolics Private	8068	General Dynamics
0888–088A	Xyplex	8069	AT&T
0900	Ungermann-Bass net debugger	806A	Autophon
0A00	Xerox IEEE802.3 PUP	806C	ComDesign
0A01	PUP Addr Trans	806D	Computgraphic Corp.
0BAD	Banyan Systems	80E–E8077	Landmark Graphics Corp.
1000	Berkeley Trailer nego	807A	Matra
1001–100F	Berkeley Trailer encap/IP	807B	Dansk Data Elektronik
1600	Valid Systems	807C	Merit Internodal
4242	PCS Basic Block Protocol	807D–807F	Vitalink Communications
5208	BBN Simnet	8080	Vitalink TransLAN III
6000	DEC Unassigned (Exp.)	8081–8083	Counterpoint Computers
6001	DEC MOP Dump/Load	809B	Appletalk
6002	DEC MOP Remote Console	809C–809E	Datability
6003	DEC DECNET Phase IV Route	809F	Spider Systems Ltd.

Table C-14. Ethernet Type Codes (Hex) (2 of 2)

Type Code	Description	Type Code	Description
6004	DEC LAT	80A3	Nixdorf Computers
6005	DEC Diagnostic Protocol	80A4−80B3	Siemens Gammasonics Inc. (Xerox)
6006	DEC Customer Protocol	80C0−80C3	DCA Data Exchange Cluster (Xerox)
6007	DEC LAVC, SCA	80C6	Pacer Software
6008−6009	DEC Unassigned	80C7	Applitek Corporation
6010−6014	3Com Corporation	80C8−80CC	Intergraph Corporation
7000	Ungermann-Bass download	80CD−80CE	Harris Corporation
7002	Ungermann-Bass dia/loop	80CF−80D2	Taylor Instrument
7020−7029	LRT	80D3−80D4	Rosemount Corporation
7030	Proteon	80D5	IBM SNA Service on Ether
7034	Cabletron	80DD	Varian Associates
8003	Cronus VLN	80DE−80DF	Integrated Solutions TRFS
8004	Cronus Direct	80E0−80E3	Allen-Bradley
8005	HP Probe	80E4−80F0	Datability
8006	Nestar	80F2	Retix
8008	AT&T	80F3	AppleTalk AARP (Kinetics)
8010	Excelan	80F4−80F5	Kinetics
8013	SGI diagnostics	80F7	Apollo Computer
8014	SGI network games	80FF−8103	Wellfleet Communications
8015	SGI reserved	8107−8109	Symbolics Private
8016	SGI bounce server	8130	Waterloo Microsystems
8019	Apollo Computers	8131	VG Laboratory Systems
802E	Tymshare	8137−8138	Novell, Inc.
802F	Tigan, Inc.	8139−813D	KTI
8035	Reverse ARP	814C	SNMP
8036	Aeonic Systems	9000	Loopback
8038	DEC LANBridge	9001	3Com(Bridge) XNS Sys Mgmt
8039−803C	DEC Unassigned	9002−9003	3Com(Bridge) TCP-IP Sys & loop detect
803D	DEC Ethernet Encryption	FF00	BBN VITAL-LanBridge cache

Protocol and Port Designations

The following tables are used for filtering.

ICMP Designations

Use the Internet Control Management Protocol (ICMP) designations in Table C-15, ICMP Designations, when specifying a specific ICMP message to be filtered.

Table C-15. ICMP Designations (1 of 2)

Type	Code	ICMP Message	Description
0	0	echo-reply	Echo (ping) reply
All 3*n* = Destination unreachable			
3	0	net-unreachable	Network unreachable
3	1	host-unreachable	Host unreachable
3	2	protocol-unreachable	Protocol unreachable
3	3	port-unreachable	Port unreachable
3	4	packet-too-big	Fragmentation needed and do not fragment (DF) bit set
3	5	source-route-failed	Source route failed
3	6	network-unknown	Destination network unknown
3	7	host-unknown	Destination host unknown
3	8	host-isolated	Source host isolated
3	9	dod-net-prohibited	Destination network admin prohibited
3	10	dod-host-prohibited	Destination host admin prohibited
3	11	net-tos-unreachable	Network unreachable for TOS (Type of Service)
3	12	host-tos-unreachable	Host unreachable for TOS
3	13	Administratively-prohibited	Communication admin. prohibited by filtering
3	14	host-precedence-unreachable	Host precedence violation
3	15	precedence-unreachable	Precedence cutoff in effect
4	0	source-quench	Source quench (flow control)

Table C-15. ICMP Designations (2 of 2)

Type	Code	ICMP Message	Description
All 5*n* = All redirects			
5	0	net-redirect	Redirect for network
5	1	host-redirect	Redirect for host
5	2	net-tos-redirect	Redirect for Type of Service (TOS) & network
5	3	host-tos-redirect	Redirect for Type of Service (TOS) & host
8	0	echo	Echo request (ping)
9	0	router-advertisement	Router discovery advertisements
10	0	router-solicitation	Router discovery solicitations
11	0	ttl-exceeded	TTL (Time to Live) = 0 & exceeded during transit (Traceroute)
11	1	reassembly-timeout	TTL (Time to Live) = 0 & exceeded during reassembly
12	0	general-parameter-problem	IP header bad
12	1	option-missing	Parameter required but not present
12	2	no-room-for-option	Parameter required but no room
13	0	timestamp-request	Timestamp request
14	0	timestamp-reply	Timestamp reply
15	0	information-request	Information request
16	0	information-reply	Information reply
17	0	mask-request	Address mask request
18	0	mask-reply	Address mask reply

TCP Port Designations

Use the Transmission Control Protocol (TCP) port designations in Table C-16, TCP Port Designations, when specifying a specific TCP port to be filtered.

Table C-16. TCP Port Designations

TCP Port #	TCP Port Table	Description
7	echo	Echo
9	discard	Discard
13	daytime	Daytime
19	chargen	Character generator
20	ftp-data	FTP data connections
21	ftp	File Transfer Protocol
23	telnet	Telnet
25	smtp	Simple Mail Transport Protocol
37	time	Time
43	whois	Nicname
49	tacacs	TAC Access Control System
53	domain	Domain Name Service
70	gopher	Gopher
79	finger	Finger
80	www	World Wide Web (HTTP)
101	hostname	NIC hostname server
109	pop2	Post Office Protocol v2
110	pop3	Post Office Protocol v3
111	sunrpc	Sun Remote Procedure Call
119	nntp	Network News Transport Protocol
179	bgp	Border Gateway Protocol
194	irc	Internet Relay Chat
512	exec	Exec (rsh)
513	login	Login (rlogin)
514	cmd	Remote commands (rcmd)
514	syslog	Syslog
515	lpd	Printer service
517	talk	Talk
540	uucp	UNIX-to-UNIX Copy Program
543	klogin	Kerberos login
544	kshell	Kerberos shell

UDP Port Designations

Use the User Datagram Protocol (UDP) port designations in Table C-17, UDP Port Designations, when specifying a specific UCP port to be filtered.

Table C-17. UDP Port Designations

UDP Port #	UDP Port Name	Description
7	echo	Echo
9	discard	Discard
37	time	Time
42	nameserver	IEN116 name service (obsolete)
49	tacacs	TAC Access Control System
53	domain	Domain Name Service (DNS)
67	bootpc	Bootstrap Protocol (BOOTP) client
68	bootps	Bootstrap Protocol (BOOTP) server
69	tftp	Trivial File Transfer Protocol
111	sunrpc	Sun Remote Procedure Call
123	ntp	Network Time Protocol
137	netbios-ns	NetBios name service
138	netbios-dgm	NetBios datagram service
161	snmp	Simple Network Management Protocol
162	snmptrap	SNMP Traps
177	xdmcp	X Display Manager Control Protocol
195	dnsix	DNSIX security protocol auditing
434	mobile-ip	Mobile IP registration
512	biff	Biff (mail notification, comsat)
513	who	Who service (rwho)
514	syslog	System Logger
517	talk	Talk
520	rip	Routing Information Protocol

Router Command Line Summaries and Shortcuts

D

CLI Summaries

For summaries of Command Line Interface commands, see:

- Table D-1, Show Commands
- Table D-2, Access Control and System Level Commands
- Table D-3, CLI Commands

  For default settings, see *CLI Command Default Settings* on page D-6.

The minimal characters that must be typed when entering commands are shown in **bold** for these tables.

For details on each command and the conventions used for command line syntax, see Appendix C, *Router CLI Commands, Codes, and Designations.*

Show Command Summary

Table D-1, Show Commands, lists all of the show, or display, commands for the CLI.

Table D-1. Show Commands

Command	Function
show **a**rp	Displays all the devices in the router's ARP table.
show **b**ridge	Displays the router's bridge forwarding database entries.
show **c**onfiguration	Displays the router's current configuration.
show **c**onfiguration {**s**aved|**u**nsaved}	Shows the current configuration, either saved in memory or entered during the current session.
show **f**rame-relay **m**ap	Shows the status of all frame relay DLCIs on the router's frame relay interface.
show **in**terface [*intf-type intf-num* [*.sub-intf-num*]]	Shows the status of the specified interface, sub-interface, or all interfaces and sub-interfaces for the router.
show **ip** **d**hcp **b**inding [*ip-address*]	Shows the address bindings associated with the DHCP server. ■ If an IP address is specified, only bindings for that client will be displayed. ■ If no IP address is specified, all DHCP server bindings are displayed.
show **ip** **n**at **t**ranslations	Displays all the address bindings associated with the DHCP server.
show **ip** **r**oute [*ip-address*]	Shows the Routing Table entry for the device with the specified IP address, or all Routing Table entries if no IP address is specified.
show **ip** **t**raffic	Shows IP statistics for the router.
show **s**panning-tree	Displays the router's spanning-tree topology.

Access Control and System Level Command Summary

Table D-2, Access Control and System Level Commands, lists of all of the access control and system level commands for the CLI.

Table D-2. Access Control and System Level Commands

Command	Function
?	Displays all valid commands for the current access level.
!	Used to enter comments. Comments following the ! are ignored by the CLI.
configure {**t**erminal|**f**actory)	Enters configuration mode so configuration options can be edited.
disable	Exits Administrator access level.
enable	Enters/enables the Administrator access level.
enable **p**assword *password* **no en**able **p**assword [*password*]	Sets or disables the password level. Default is None.
end	Leaves configuration mode to return to standard operating mode.
exit	Leaves the current configuration level or terminates the session. It may be necessary to enter the exit command several times when leaving configuration mode.
help	Displays a summary of help options.
[**n**o] **pa**ger	Enables/Outputs up to 23 lines.
reload	Resets the router and reloads its configuration.
save	Saves changes to the router's configuration.

CLI Command Summary

Table D-3, CLI Commands lists of all of the system-level commands for the CLI. For the default settings, see *CLI Command Default Settings* on page D-6.

Table D-3. CLI Commands (1 of 2)

Command
access-list *access-list-num* [{permit | deny} { {*source-ip* [*src-wildcard*] | any | host *source-host-ip*} | {*protocol* {*source-ip source-wildcard* | any | host *source-host-ip*} [*src-operator src-port* [*src-end-port*]] {*dest-ip dest-wildcard* | any | host *dest-host-ip*} [[*icmp-msg-type* [*icmp-msg-code*]] | [*dest-operator dest-port* [*dest-end-port*]]] } | {*type-code* [**r**ange *end-type-code*] } } **no ac**cess-list *access-list-num* [{permit | deny} { {*src-ip* [*src-wildcard*] | any | host *src-host-ip*} | {*protocol* {*src-ip src-wildcard* | any | host *src-host-ip*} [*src-operator src-port* [*src-end-port*]] {*dest-ip dest-wildcard* | any | host *dest-host-ip*} [[*icmp-msg-type* [*icmp-msg-code*]] | [*dest-operator dest-port* [*dest-end-port*]]] } | {*type-code* [**r**ange *end-type-code*] }]
arp *ip-address mac-address arp-type* **n**o **ar**p *ip-address* [*mac-address arp-type*]
arp **t**imeout *time* **n**o **ar**p **t**imeout [*time*]
bridge {**c**rb | *bridge-group* {**ac**quire | **ag**ing-time *aging-time* | **pro**tocol *span-tree-protocol* | **pri**ority *span-tree-priority* | **r**oute *route-protocol*} } **n**o bridge {**c**rb | *bridge-group* {**ac**quire | **ag**ing-time [*aging-time*] | **pri**ority [*span-tree-priority*] | **r**oute [*route-protocol*] } }
[**n**o] **b**ridge-group *bridge-group*
[**n**o] **b**ridge-group *bridge-group* {**i**nput-type-list *in-access-list-200num* | **o**utput-type-list *out-access-list-200num*}
clear **a**rp-cache
clear **c**ounters [*intf-type intf-num* [*.sub-intf-num*]]
clear **i**p **n**at **t**ranslations *
default-router *ip-address* **n**o **d**efault-router [*ip-address*]
dns-server *ip-address* **n**o **dn**s-server [*ip-address*]
domain-name *domain-name* **n**o **do**main-name [*domain-name*]

Table D-3. CLI Commands (2 of 2)

Command
encapsulation *encapsulation-type encapsulation-protocol*
[**n**o] **f**rame-relay **i**nterface-dlci *dlci-num*
interface *intf-type intf-num* [.*sub-intf-num* [**p**oint-to-point]] **n**o **in**terface *intf-type intf-num.sub-intf-num* [**p**oint-to-point]
ip address *ip-addr subnet-mask* **n**o **ip ad**dress [*ip-addr subnet-mask*]
[**n**o] **ip ac**cess-group *access-list-1-199num* [**i**n | **o**ut]
[**n**o] **ip dhcp p**ool *pool-name*
ip dhcp relay **m**ax-clients *max-dhcp-clients* **n**o **ip dhcp r**elay **m**ax-clients [*max-dhcp-clients*]
[**n**o] **ip dhcp-s**erver *ip-address*
[**n**o] **ip m**ulticast-routing
[**n**o] **ip n**at {**i**nside | **o**utside}
[**n**o] **ip n**at **i**nside **s**ource {**l**ist *access-list-1–99num* **p**ool *pool-nam*e [**o**verload] | **l**ist *access-list-1–99num* **i**nterface *intf-type intf-num* [.*sub-intf-num*] **o**verload | **s**tatic {*static-ip-addr1 static-ip-addr2* | *protocol static-ip-addr1 static-port-num static-ip-addr2*} }
[**n**o] **ip n**at **p**ool *pool-name start-ip-addr end-ip-addr* {**n**etmask *netmask* | {**p**refix-length | / } *prefix-length*}
ip nat **t**ranslation **t**imeout *time* **n**o **ip n**at **t**ranslation **t**imeout [*time*]
ip route *dest-ip dest-mask* {*next-hop-ip* | *intf-type intf-num* [.*sub-intf-num*] } **n**o **ip route** *dest-ip dest-mask* [*next-hop-ip* | *intf-type intf-num* [.*sub-intf-num*]]
[**n**o] **ip routi**ng
[**n**o] **ip un**numbered [**n**ull **0**]
lease {*days* [*hours*] [*minutes*] | **i**nfinite} **n**o lease [*days* [*hours*] [*minutes*] | **i**nfinite]
network *network-num* [[**n**etmask] *netmask* | {**p**refix-length | / } *prefix-length*] **n**o **ne**twork [*network-num* [[**n**etmask] *netmask* | {**p**refix-length | / } *prefix-length*]]
ping [*protocol*] *dest-ip* [**s**ource *source-ip*] [**l**ength *bytes*] [**t**imeout *time*] [**i**nterface *intf-type intf-num* [.*sub-intf-num*]]
[**n**o] **se**rvice dhcp
traceroute [*protocol*] *dest-ip* [**s**ource *source-ip*] [**l**ength *bytes*] [**t**imeout *time*] [**h**ops *hops*] [**i**nterface *intf-type intf-num* [.*sub-intf-num*]]

CLI Command Default Settings

The following list shows the default settings:

```
!software version d1.06.04
!
no enable password
ip routing
no ip multicast-routing
service dhcp
ip nat translation timeout 86400
ip dhcp relay max-clients 256
bridge 1 acquire
bridge 1 aging-time 300
bridge 1 protocol ieee
bridge 1 priority 32768

interface Ethernet 0
 bridge-group 1
 arp timeout 14400
!
interface Serial 0
 Encapsulation frame-relay ietf
 bridge-group 1
!
end
```

Connectors, Cables, and Pin Assignments

E

This appendix shows the rear panels of the FrameSaver DSL CSU/DSUs and routers, and the pin assignments for the connectors and cables:

In addition, this appendix contains the procedure for *Configuring an External Modem*, using a:

Rear Panels

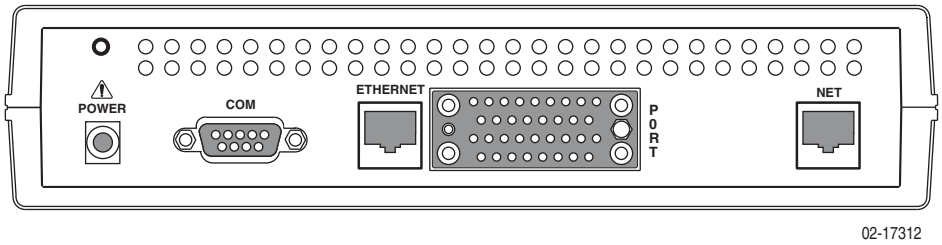


Figure E-1. Model 9720 CSU/DSU Rear Panel

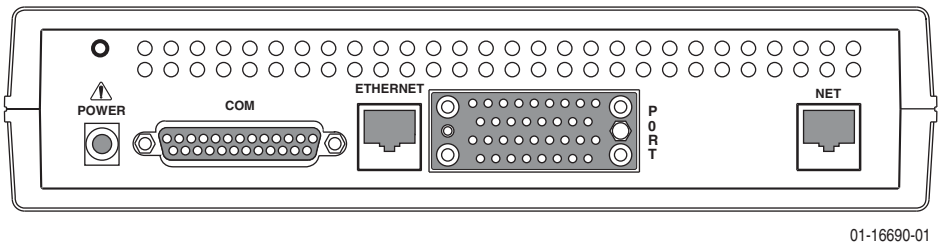


Figure E-2. Model 9783 CSU/DSU Rear Panel

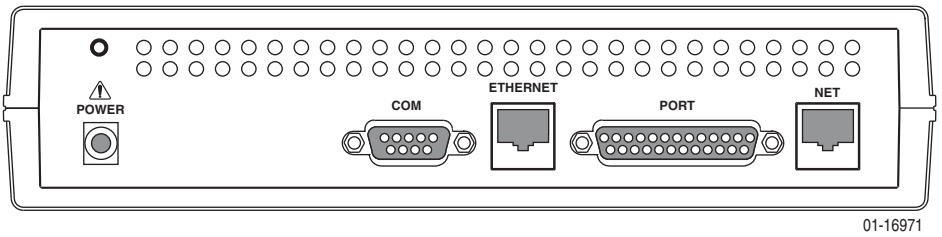


Figure E-3. Model 9788 CSU/DSU Rear Panel

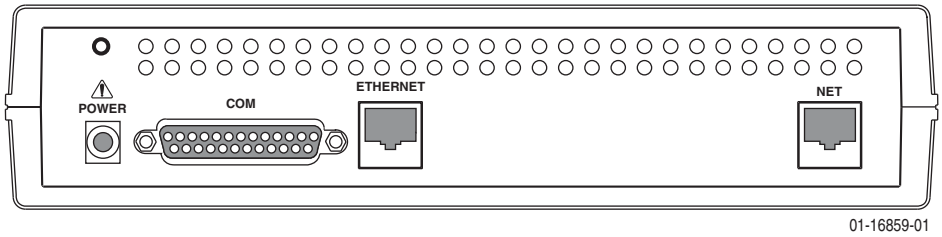


Figure E-4. Model 9783 Router Rear Panel

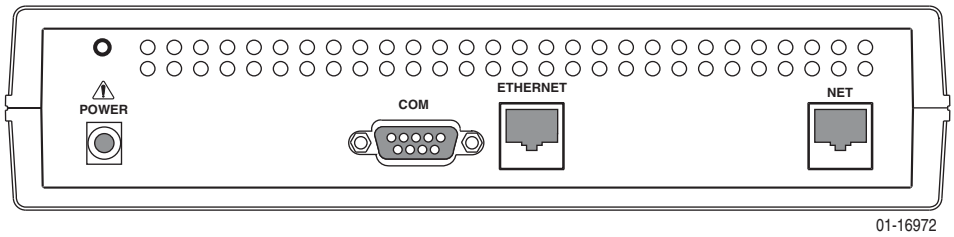


Figure E-5. Model 9788 Router Rear Panel

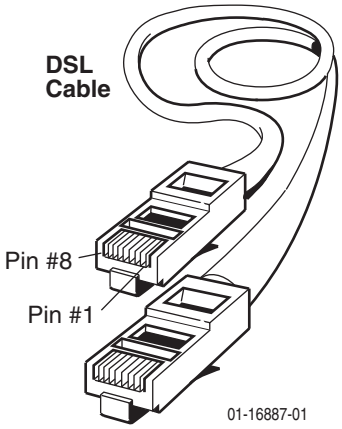
The sections that follow provide pin assignments for each interface and some cables.

DSL Network Interface and Cable

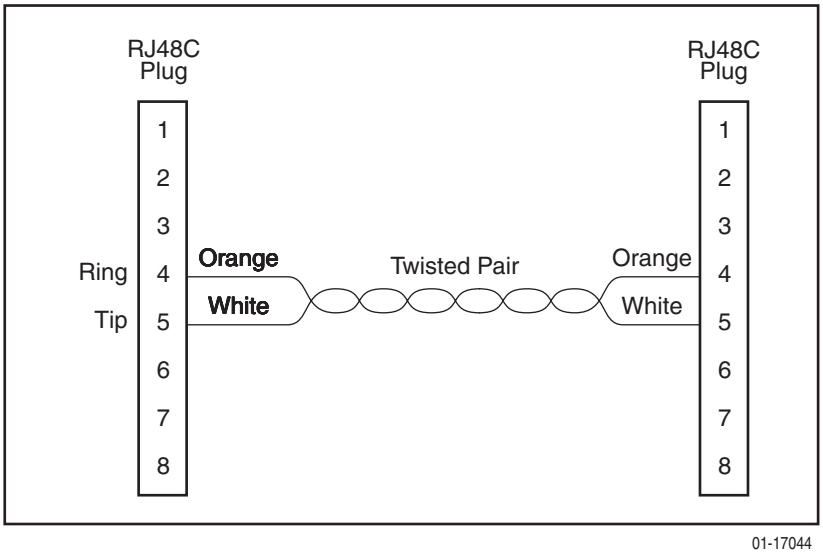
The DSL network interface connector is an 8-position unkeyed RJ48C-type modular jack. Table E-1, DSL Network Interface Connector, shows the pin assignments for the interface. The network cable is orderable by Feature No. 3100-F1-500.

Table E-1. DSL Network Interface Connector

Pin #	Signal
1–3	Unused
4	Ring
5	Tip
6–8	Unused



The following shows the cable's pin assignments and the purpose of each.



Model 9783 COM Port Connector

Table E-2, Model 9783 COM Port Connector, provides the pin assignments for the FrameSaver Model 9783 CSU/DSU's and router's 25-position EIA-232-E communication port connector.

Table E-2. Model 9783 COM Port Connector

Pin #	Signal	Direction
1	Shield (GND)	—
2	DCE Transmit Data (TXD)	From DTE (In)
3	DCE Receive Data (RXD)	To DTE (Out)
4	DCE Request To Send (RTS)	From DTE (In)
5 *	DCE Clear To Send (CTS)	To DTE (Out)
6 *	DCE Data Set Ready (DSR)	To DTE (Out)
7	Signal Ground (GND)	—
8 *	DCE Carrier Detect (CD)	To DTE (Out)
9–19	Unused	—
20	DCE Data Terminal Ready (DTR)	From DTE (In)
21–25	Unused	—

*Pins 5, 6, and 8 are tied together.

Model 9720 and 9788 COM Port Connector

Table E-3, Model 9720 and 9788 COM Port Connector, provides the pin assignments for the FrameSaver Model 9788 CSU/DSU's and router's 9-position EIA-232-E communication port connector.

Table E-3. Model 9720 and 9788 COM Port Connector

Pin #	Signal	Direction
1*	Data Carrier Detect (DCD)	To DTE (Out)
2	Receive Data (RD)	To DTE (Out)
3	Transmit Data (TD)	From DTE (In)
4	Data Terminal Ready (DTR)	From DTE (In)
5	Signal Ground (GND)	—
6*	Data Set Ready (DSR)	To DTE (Out)
7	Not used	—
8*	Clear To Send (CTS)	To DTE (Out)
9	Not used	—

*Pins 1, 6, and 8 are tied together.

Ethernet Port Connector

Table E-4, Ethernet Port Connector, provides the pin assignments for the FrameSaver CSU/DSU's and router's Ethernet interface 8-position unkeyed modular jack, which is similar to an RJ45 jack.

Table E-4. Ethernet Port Connector

Pin #	10/100BaseT Signal	Direction
1	Transmit Data (TD +)	To LAN Interface (Out)
2	Transmit Data (TD –)	To LAN Interface (Out)
3	Receive Data (RD +)	From LAN Interface (In)
4–5	Unused	—
6	Receive Data (RD –)	From LAN Interface (In)
7–8	Unused	—

Model 9720 and 9783 CSU/DSU Data Port Connector

Table E-5, Model 9720 and 9783 CSU/DSU Data Port Connector, provides the pin assignments for the 34-position V.35 connector to the DTE.

This does not apply to the router.

Table E-5. Model 9720 and 9783 CSU/DSU Data Port Connector

Signal	ITU-T Number	Direction	Pin
Shield	101	—	A
Signal Ground/Common	102	—	B
Request to Send (RTS)	105	To DSU (In)	C
Clear to Send (CTS)	106	From DSU (Out)	D
Data Set Ready (DSR)	107	From DSU (Out)	E
Receive Line Signal Detector (RLSD or LSD)	109	From DSU (Out)	F
Data Terminal Ready (DTR)	108/1, /2	To DSU (In)	H
Local Loopback (LL)	141	To DSU (In)	L
Transmit Data (TXD)	103	To DSU (In)	P (A) S (B)
Receive Data (RXD)	104	From DSU (Out)	R (A) T (B)
Transmit Signal Element Timing – DTE Source (XTXC or TT)	113	To DSU (In)	U (A) W (B)
Receive Signal Element Timing – DCE Source (RXC)	115	From DSU (Out)	V (A) X (B)
Transmit Signal Element Timing – DCE Source (TXC)	114	From DSU (Out)	Y (A) AA (B)
Test Mode Indicator (TM)	142	From DSU (Out)	NN

Standard V.35 Straight-through Cable

A standard V.35 straight-through cable can be used to connect a DTE port to a DTE, where a 34-pin plug-type connector is needed for the data port and a 34-position socket-type connector is needed for the DTE. No special-order cables are required.

Model 9788 CSU/DSU Data Port Connector

Table E-6, Model 9788 CSU/DSU Data Port Connector, provides the pin assignments for the 25-position EIA-530-A connector to the DTE.

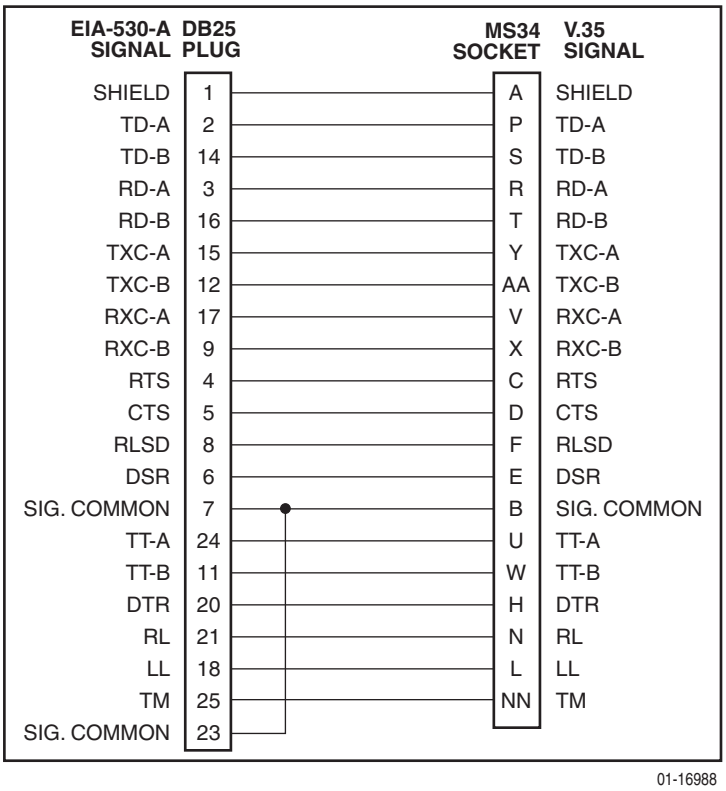
This does not apply to the router.

Table E-6. Model 9788 CSU/DSU Data Port Connector

Signal	Circuit Mnemonic	ITU-T Number	Direction	Pin
Shield	—	—	—	1
Signal Common	AB	102A	—	7
Signal Common	AC	102B	—	23
Transmitted Data	BA	103	To CSU/DSU	2 (A) 14 (B)
Received Data	BB	104	From CSU/DSU	3 (A) 16 (B)
Request to Send	CA	105	To CSU/DSU	4 (A) 19 (B)
Clear to Send	CB	106	From CSU/DSU	5 (A) 13 (B)
Received Line Signal Detector	CF	109	From CSU/DSU	8 (A) 10 (B)
DCE Ready	CC	107	From CSU/DSU	6
DTE Ready	CD	108/1, /2	To CSU/DSU	20
Transmit Signal Element Timing (DTE Source)	DA	113	To CSU/DSU	11 (B) 24 (A)
Transmit Signal Element Timing (DCE Source)	DB	114	From CSU/DSU	12 (B) 15 (A)
Receiver Signal Element Timing (DCE Source)	DD	115	From CSU/DSU	17 (A) 9 (B)
Local Loopback	LL	141	To CSU/DSU	18
Remote Loopback	RL	140	To CSU/DSU	21
Test Mode	TM	142	From CSU/DSU	25

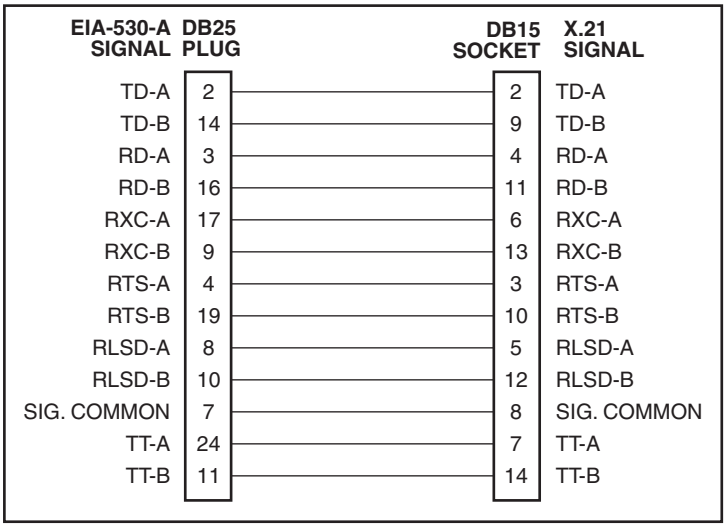
EIA-530-A-to-V.35 Adapter

An EIA-530-A-to-V.35 adapter for the Model 9788 CSU/DSU user data port must have the following connections. An appropriate adapter is available from Paradyne (Feature No. 3100-F1-572).



EIA-530-A-to-X.21 Adapter

An EIA-530-A-to-X.21 adapter for the Model 9788 CSU/DSU user data port must have the following connections. An appropriate adapter is available from Paradyne (Feature No. 3100-F1-571).



Configuring an External Modem

▶ Procedure

To configure an external modem:

1. Disconnect the asynchronous terminal from the standard cable.
2. Reconnect the crossover cable to the external modem. See *DB25-to-DB25 Crossover Cable* on page E-12 or *DB9-to-DB25 Crossover Cable* on page E-13 for a drawing of the cable.
3. Enable auto-answer on your modem, and configure it to use the following LSD, DSR, CTS, RTS, and DTR control leads.

   See the table below for AT D0 command strings. Use the following command string:

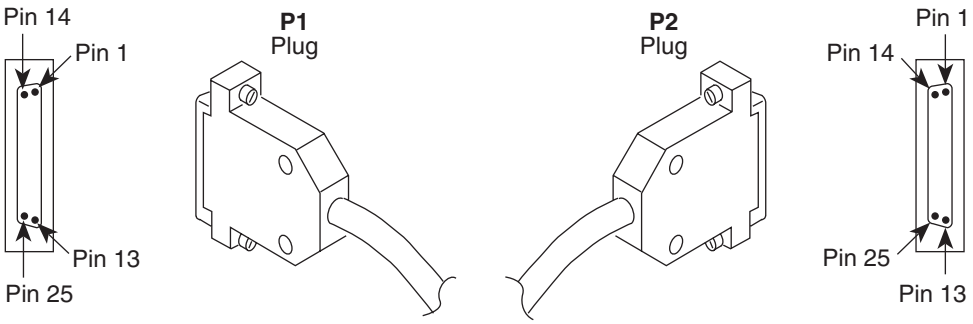
   AT &C0 &D2 &S0 &R1 \D0 S0=1

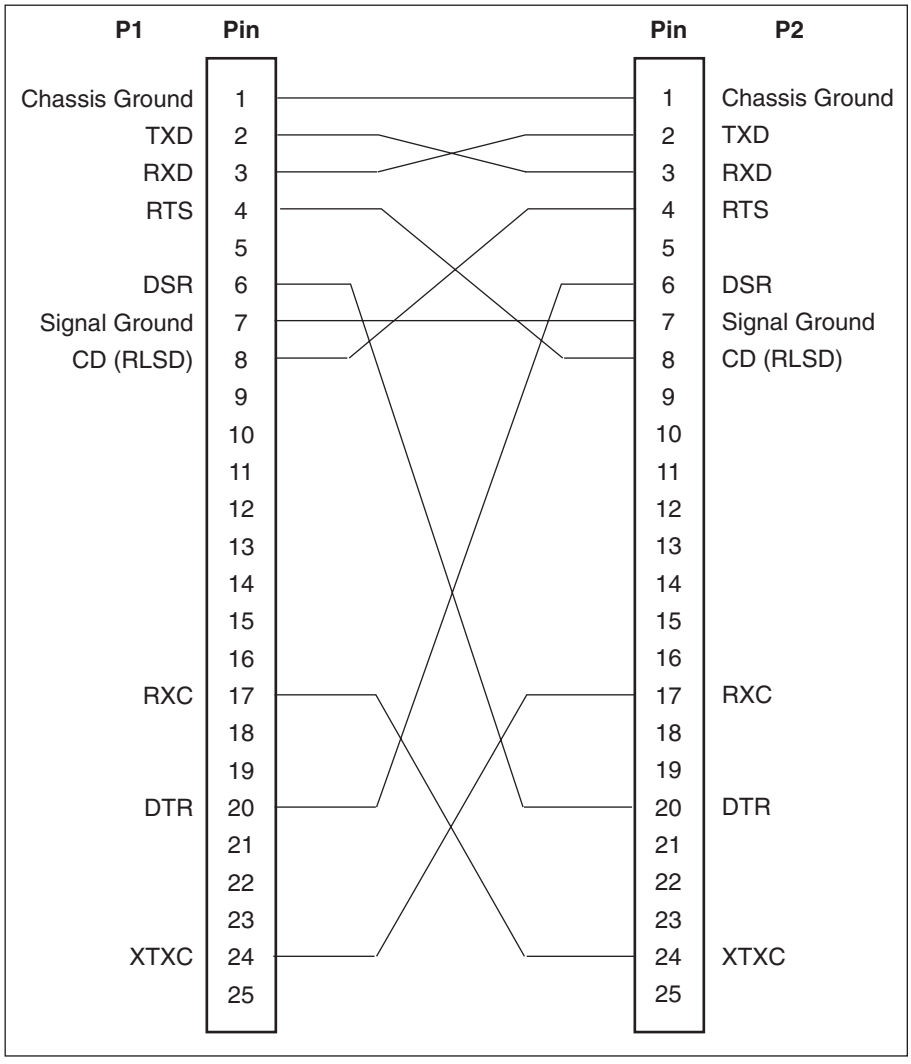
Enter AT Command . . .	To configure the modem to . . .
&C0	Force LSD on
&D2	Drop the connection when the unit drops DTR
&S0	Force DSR on
&R1	Ignore RTS
\D0	Force CTS on
S0=1	Automatically answer incoming calls

DB25-to-DB25 Crossover Cable

A standard crossover cable can be used to connect the Model 9783 COM port to an external modem. The external modem must be configured so it is compatible with the FrameSaver CSU/DSU. See *Ethernet Port Connector* on page E-6 to configure an external modem.

This does not apply to the router.



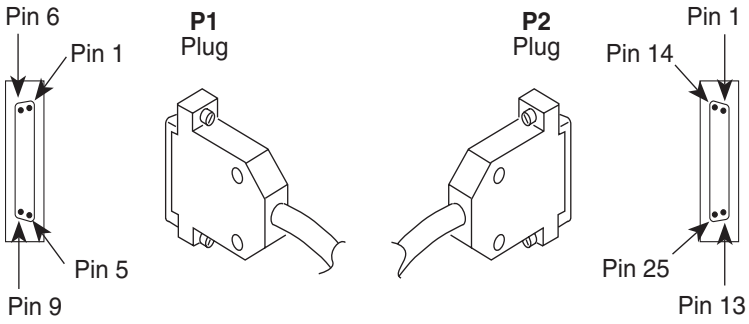


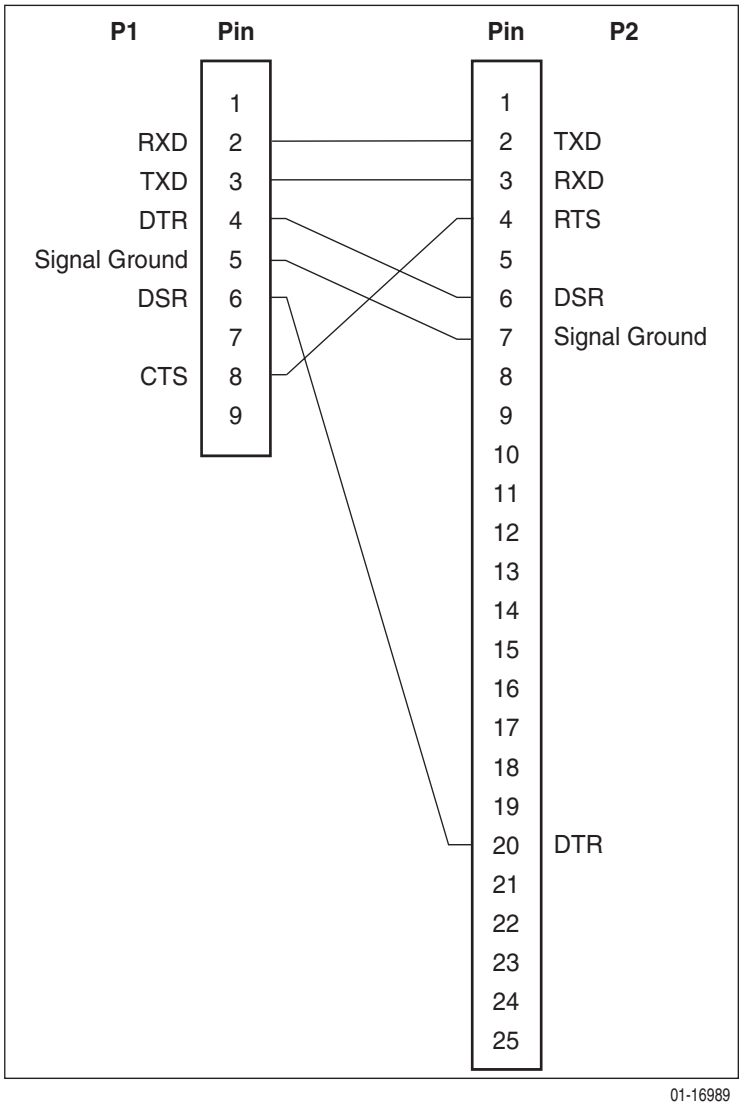
496-15180

DB9-to-DB25 Crossover Cable

A standard crossover cable can be used to connect the Model 9720 or 9788 COM port to an external modem. The external modem must be configured so it is compatible with the FrameSaver CSU/DSU. See *Ethernet Port Connector* on page E-6 to configure an external modem.

This does not apply to the router.





01-16989

Technical Specifications

F

Technical specifications for the FrameSaver DSL CSU/DSUs and routers are the same, except that the routers do not have a data port.

Table F-1. FrameSaver DSL Technical Specifications (1 of 2)

Specification	Criteria
Approvals	
FCC Part 15, ICES-003, CISPR 22	Class A digital device
Safety	Refer to the equipment's label for safety information.
Physical Environment	
Operating temperature	0°C to 50°C (32°F to 122°F)
Storage temperature	–20°C to 70°C (–4°F to 158°F)
Relative humidity	5% to 85% (noncondensing)
Shock and vibration	Withstands normal shipping and handling
Power Consumption and Dissipation (9720)	5.6 watts, 60 Hz ± 3, 69 mA at 120 VAC ± 12 Result: 19.1Btu per hour
Power Consumption and Dissipation (9783)	4.5 watts, 60 Hz ± 3, 135 mA at 120 VAC ± 12 Result: 15.4 Btu per hour
Power Consumption and Dissipation (9788)	7.5 watts, 60 Hz ± 3, 84 mA at 120 VAC ± 12 Result: 25.59 Btu per hour 7.6 watts, 50 Hz, 48 mA at 230 VAC Result: 25.93 Btu per hour
Physical Dimensions	
Height (with feet) Height (without feet)	2.1 inches (5.3 cm) 2.0 inches (5.1 cm)
Width	8.7 inches (22.1 cm)
Depth	6.2 inches (15.7 cm)
Weight (9720)	1.25 lbs (0.57 kg)
Weight (9783)	1.38 lbs (0.62 kg)
Weight (9788)	1.2 lbs (0.55 kg)

Table F-1. FrameSaver DSL Technical Specifications (2 of 2)

Specification	Criteria
COM Port (9783)	25-position (DB25) connector
Standard	EIA-232-E/ITU V.24 (ISO 2110)
Data rates	9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 kbps
COM Port (9720, 9788)	9-position (DB9) connector
Standard	EIA-232-E/ITU V.24 (ISO 2110)
Data rates	9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 kbps
DSL Network Interface (9720)	6-position modular unkeyed RJ11-type jack
Line code	2B1Q
Service supported	IDSL (T1.601-1992)
Data rates	64, 128, 144 kbps
DSL Network Interface (9783)	8-position modular unkeyed RJ45-type jack
Line code	2B1Q
Service supported	SDSL
Data rates	144−2320 kbps
DSL Network Interface (9788)	8-position modular unkeyed RJ45-type jack
Line code	TC PAM
Service supported	SHDSL (G.991.2)
Data rates	200−2312 kbps
Ethernet Port	8-position modular unkeyed RJ45 jack
Standard	ANSI/IEEE Standard 802.3, Ethernet Version 2
Data rates	10/100BaseT (auto-sensing 10 and 100 Mbps Ethernet rates)
Data Port (9720 CSU/DSU, 9783 CSU/DSU)	34-position V.35 connector
Standard	V.35/ITU (ISO 2593)
Data rates	Automatically set to the network rate
Data Port (9788 CSU/DSU)	25-position EIA-530-A connector
Standards	EIA-530-A, V.35/ITU (ISO 2593), X.21
Data rates	Automatically set to match the network payload

Equipment List

G

Equipment

See *Cables* on page G-5 for cables you can order.

Description	Model Number
FrameSaver DSL 9720 CSU/DSUs	
FrameSaver DSL 9720 CSU/DSU with 8 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, V.35 Adapter, and Installation Instructions.*	9720-A1-211
FrameSaver DSL 9720 CSU/DSU with 8 PVCs and Advanced SLM Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, V.35 Adapter, and Installation Instructions.*	9720-A1-221
FrameSaver DSL 9783 CSU/DSUs	
FrameSaver DSL 9783 CSU/DSU with 8 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-211
FrameSaver DSL 9783 CSU/DSU with 64 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-213
FrameSaver DSL 9783 CSU/DSU with 8 PVCs and Advanced SLM Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-221

* For international models, the country code is shown as *-xxx*. Contact your Paradyne sales office for the correct number.

Description	Model Number
FrameSaver DSL 9783 DSU/CSUs *(continued)*	
FrameSaver DSL 9783 CSU/DSU with 64 PVCs and Advanced SLM Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-223
FrameSaver DSL 9783 CSU/DSU with 8 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 100 or 230 VAC Power Supply, Network Cable, Ferrite Choke, Installation Instructions, and Quick Reference.*	9783-A1-311-*xxx**
FrameSaver DSL 9783 CSU/DSU with 64 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 100 or 230 VAC Power Supply, Network Cable, Ferrite Choke, Installation Instructions, and Quick Reference.*	9783-A1-313-*xxx**
FrameSaver DSL 9783 CSU/DSU with 8 PVCs and Advanced SLM Feature Set. *Includes 1-Slot Housing, 100 or 230 VAC Power Supply, Network Cable, Ferrite Choke, Installation Instructions, and Quick Reference.*	9783-A1-321-*xxx**
FrameSaver DSL 9783 CSU/DSU with 64 PVCs and Advanced SLM Feature Set. *Includes 1-Slot Housing, 100 or 230 VAC Power Supply, Network Cable, Ferrite Choke, Installation Instructions, and Quick Reference.*	9783-A1-323-*xxx**
FrameSaver DSL 9788 CSU/DSUs	
FrameSaver DSL 9788 CSU/DSU with 64 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Ferrite Choke, V.35 Adapter, Installation Instructions, and Quick Reference.*	9788-A1-211
FrameSaver DSL 9788 CSU/DSU with 64 PVCs and Advanced SLM Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Ferrite Choke, V.35 Adapter, Installation Instructions, and Quick Reference.*	9788-A1-221
FrameSaver DSL 9788 CSU/DSU with 64 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 230 VAC Power Supply, Network Cable, Ferrite Choke, Installation Instructions, and Quick Reference.*	9788-A1-311
FrameSaver DSL 9788 CSU/DSU with 64 PVCs and Advanced SLM Feature Set. *Includes 1-Slot Housing, 230 VAC Power Supply, Network Cable, Ferrite Choke, Installation Instructions, and Quick Reference.*	9788-A1-321

***** For international models, the country code is shown as *-xxx*. Contact your Paradyne sales office for the correct number.

Description	Model Number
FrameSaver DSL 9783 Routers	
FrameSaver DSL 9783 Router with 8 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-214
FrameSaver DSL 9783 Router with 8 PVCs and Advanced SLM Feature Sets. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-224
FrameSaver DSL 9783 Router with 8 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 100 or 230 VAC Power Supply, Network Cable, Ferrite Choke, Installation Instructions, and Quick Reference.*	9783-A1-314-*xxx**
FrameSaver DSL 9783 Router with 8 PVCs and Advanced SLM Feature Sets. *Includes 1-Slot Housing, 100 or 230 VAC Power Supply, Network Cable, Ferrite Choke, Installation Instructions, and Quick Reference.*	9783-A1-324-*xxx**
FrameSaver DSL 9788 Routers	
FrameSaver DSL 9788 Router with 8 PVCs and the Diagnostic Feature Set. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9788-A1-214
FrameSaver DSL 9788 Router with 8 PVCs and Advanced SLM Feature Sets. *Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9788-A1-224
FrameSaver SLV Upgrade	
FrameSaver SLV 9720 Activation Certificate	9720-C1-220
FrameSaver SLV 9783 Activation Certificate	9783-C1-220
FrameSaver SLV 9788 Activation Certificate	9788-C1-220
FrameSaver SLV Activation Instructions	9000-A2-GK43
User Manual	
FrameSaver DSL, Models 9720, 9783, and 9788, User's Guide (Paper Manual)	9700-A2-GB20

***** For international models, the country code is shown as *-xxx*. Contact your Paradyne sales office for the correct number.

Description	Model Number
NMS Products	
OpenLane Enterprise	7805-D1-001
OpenLane Workgroup	7805-D1-003
NetScout Manager Plus – For UNIX or Windows NT	9180
NetScout Server – For UNIX or Windows NT	9190
NetScout WebCast – For UNIX or Windows NT	9155
Optional Housing Mounting Kit Features	
Wall Mounting Kit for 1-Slot Housing	9001-F1-891
Shelf Mounting Kit for 1-Slot Housing	9001-F1-894

***** For international models, the country code is shown as *-xxx*. Contact your Paradyne sales office for the correct number.

Cables

This table lists cables you can order.

Description	Part Number	Feature Number
IDSL, SDSL, or SHDSL Network Cable with 8-Pin RJ48C-type Connectors (20 feet / 6.1 meters) *For use in the U.S.*	035-0209-2031	3100-F1-500
For a DB25-to-DB9 connection: ■ DB25-to-8-Pin Modular Adapter ■ 8-Pin Modular-to-DB9 Cable (14 feet / 4.2 meters) *For connection to an external device with a DB9 connector.*	 002-0069-0033 035-0313-1431	 3100-F1-920 3100-F2-550
Standard DB25-to-DB25 EIA-232-D Crossover Cable (15 feet / 4.5 meters) *For connection to an external device.*	035-0222-1531	4951-035F
DB25-to-MS34 EIA-530-A-to-V.35 Cable or DB25-to-MS34 EIA-530-A-to-V.35 Adapter	035-0244-0031 or 002-0095-0131	3100-F1-570 or 3100-F1-572
DB25-to-DB15 EIA-530-A-to-X.21 Adapter	035-0302-0131	3100-F1-571

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X