FrameSaver® DSL 9783

USER'S GUIDE

Document No. 9783-A2-GB20-00

July 2000

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

4 Configuration Options

5 Security and Logins

6 Operation and Maintenance

7 FTP Operation

8 Troubleshooting

9 Setting Up OpenLane for FrameSaver Devices

10 Setting Up Network Health for FrameSaver Devices

A Menu Hierarchy

B SNMP MIBs and Traps, and RMON Alarm Defaults

About This Guide

Purpose and Intended Audience

This document contains information that applies to the FrameSaver DSL 9783. It is intended for system designers, engineers, administrators, and operators who are familiar with the functional operation of digital data communications equipment and frame relay networks.

Document Organization

Section	Description
Chapter 1	*About the FrameSaver DSL Unit.* Identifies how the FrameSaver DSL 9783 fits into Paradyne's Service Level Management (SLM) solution, and describes the unit's basic features and, if ordered, its advanced Service Level Verification and Management (SLV and SLM) features.
Chapter 2	*User Interface and Basic Operation.* Shows how to navigate the user interface.
Chapter 3	*Configuration Procedures.* Shows how to access and save configuration options.
Chapter 4	*Configuration Options.* Describes the configuration options available on the FrameSaver DSL 9783.
Chapter 5	*Security and Logins.* Provides procedures for controlling access to the unit and setting up logins.
Chapter 6	*Operation and Maintenance.* Provides procedures to display unit identification information and perform file transfers, as well as how to display and interpret status and statistical information.
Chapter 7	*FTP Operation.* Shows how to use File Transfer Protocol to upgrade system software and transfer collected data.

Section	Description
Chapter 8	*Troubleshooting.* Provides device problem resolution, alarm, and other information, as well as troubleshooting and test procedures.
Chapter 9	*Setting Up OpenLane for FrameSaver Devices.* Identifies where installation and setup information is located and how FrameSaver units are supported.
Chapter 10	*Setting Up Network Health for FrameSaver Devices.* Describes setup of Concord's Network Health application so reports can be created for FrameSaver units, and identifies those reports that apply to FrameSaver units.
Appendix A	*Menu Hierarchy.* Contains a graphical representation of how the user interface screens are organized.
Appendix B	*SNMP MIBs and Traps, and RMON Alarm Defaults.* Identifies the MIBs supported and how they can be downloaded, describes the unit's compliance with SNMP format standards and with its special operational trap features, and describes the RMON-specific user history groups, and alarm and event defaults.
Appendix C	*Connectors, Cables, and Pin Assignments.* Shows the rear panel, tells what cables are needed, and provides pin assignments for interfaces and cables.
Appendix D	*Technical Specifications.*
Appendix E	*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*
9783-A2-GN10	*FrameSaver DSL 9783 Installation Instructions*
9783-A2-GL10	*FrameSaver DSL 9783 Quick Reference*
Paradyne Hotwire Documentation:	
8335-A2-GB20	*Hotwire ATM Line Cards, Models 8335 and 8365, User's Guide*
8820-A2-GN20	*Hotwire 8820 GranDSLAM Installation Guide*
Paradyne OpenLane NMS Documentation:	
7800-A2-GZ41	*OpenLane 5.x Service Level Management for UNIX Quick Start Installation Instructions*
7800-A2-GZ42	*OpenLane 5.x Service Level Management for Windows NT Quick Start Installation 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 Used	When Used
Italic	To indicate variable information (e.g., DLCI *nnnn*).
Menu selection sequence	To provide an abbreviated method for indicating the selections to be made from a menu or selections from within a menu before performing a procedural step. For example, *Main Menu* → *Status* → *System and Test Status* indicates that you should select Status from the Main Menu, then select System and Test Status from the Status menu).
(Path:)	To provide a check point that coincides with the menu path shown at the top of the screen. Always shown within parentheses so you can verify that you are referencing the correct table (e.g., Path: main/config/alarm).
Brackets [ ]	To indicate multiple selection choices when multiple options can be displayed (e.g., Clear [*Network/Port-1*] Statistics).
Text highlighted in red	To indicate a hyperlink to additional information when viewing this manual online. Click on the highlighted text.

About the FrameSaver DSL Unit

1

This chapter includes the following:

System Overview

Our system solution consists of:

- FrameSaver® DSL (Digital Subscriber Line) unit
- Hotwire® ATM Line Card in the Hotwire 8820 GranDSLAM
- OpenLane™ SLM (Service Level Management) system

This solution provides increased manageability, monitoring, and diagnostics so customers can identify problems more efficiently, troubleshoot those problems faster, and maximize their network to control costs. It is also compatible with Concord Communication's Network Health software.

FrameSaver DSL Features and Benefits

Large-scale deployment of frame relay services over DSL-based access networks is possible with the innovative FrameSaver DSL, which provides important advantages for frame relay service providers.

- Remote diagnostic and service level management (SLM) functionality allows service providers to install the unit and verify operation quickly and reliably.
- Superior fault isolation and test capabilities allow both the Competitive Local Exchange Carrier (CLEC) and the Frame Relay Network Service Provider (FR NSP) to resolve problems quickly and efficiently.
- End-to-end service level reporting capabilities make this the ideal platform to support managed frame relay services with service level guarantees.
- Reduces operations cost by allowing Network Operations Center (NOC) center personnel to remotely troubleshoot and diagnose problems.
- Optional SLV key turns on historical reporting of service level metrics, allowing this device to be deployed as part of a fully managed service with SLA reporting.
- High-speed and lower access cost of DSL functionality provides service providers critical capabilities necessary to target markets currently served by dial or VSAT services.
- Use of ATM as a transport protocol ensures the required quality of service for each application across the access network.

Features

Specific FrameSaver DSL features include:

- Basic DSU/CSU functionality
- Two feature sets:
  - — Frame aware diagnostic feature set
  - — Advanced SLM and reporting feature set
- Frame aware diagnostic feature set includes:
  - — Nondisruptive PVC diagnostics
  - — Basic frame relay statistics
  - — PVC burst table
  - — Real-time connectivity test and latency snapshots
  - — RMON2 event log
  - — RMON2 user history statistics
  - — Multiplexed management PVCs

- Advanced SLM and reporting feature set includes all of the diagnostic feature set, plus:
  - — CIR relationship statistics
  - — FDR/DDR (Trueput) reporting
  - — Continuous real-time latency report
  - — RMON2 alarms and proactive thresholds
  - — FTP user history poller for graphical and historical reporting
- Performs FRF.8 (transparent mode) for frame to ATM conversion
- ATM OA&M loopbacks
- LMI Trace & Display
- Routing Table Display
- Router independent operation
- Ethernet port for local management
- Intelligent data delivery, latency and burst analyzer features
- Performance monitoring and data collection
- Integrated SNMP agent, TELNET, and ASCII terminal management interfaces with multilevel password protection
- Dual Flash Storage areas and in-band FTP software download
- OpenLane PVC/VC Provisioning Application
- Interoperates with the Hotwire ATM Line Card, supporting rates from 144 to 2320 kbps at distances of up to 20,000 feet (6.1 km)
- Automatically selects the optimal rate using the Conexant AutoBaud algorithm
- Monitors and makes available DSL performance information:

  Through asynchronous terminal interface screens:
  - — Noise margin
  - — Receiver attenuation
  - — Loss of Signal (LOS)
  - — Net margin threshold exceeded
  - — Current SDSL rate

  As SNMP traps and RMON2 Event Log objects:
  - — Loss of Signal
  - — Net margin threshold exceeded
  - — Rate change

An advanced SLM and reporting feature set can be activated on command with the SLV key. In the base configuration, comprehensive Layer 1 and 2 instrumentation allows service providers to isolate, diagnose, and correct problems remotely from their NOC. FR NSPs can expect fewer truck rolls and faster service turn-up times. FrameSaver DSL carries forward the end-to-end, nondisruptive loopback capabilities found in all FrameSaver products, allowing quick verification of circuit operation from customer premises to customer premises. Continuity and latency can be verified prior to cutover or any time thereafter.

When the SLV key is remotely activated, additional historical reporting capabilities are activated. Service level performance reporting in compliance with FRF.13 is possible.

Since FrameSaver DSL operates with other members of the FrameSaver product family, DSL, DDS, T1, E1, NxT1 or T3/E3 circuits can be mixed on the same customer network. This hybrid circuit approach meets the practical needs of the service providers in advance of 100 percent DSL geographic coverage, and allows FR NSPs to partner with the most cost efficient access providers for any location.

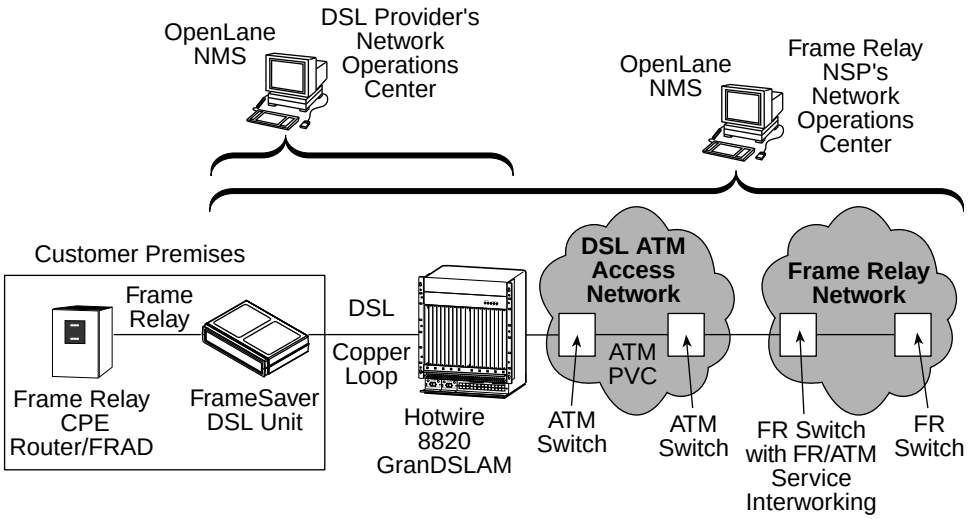
Working in concert with the Hotwire GranDSLAM and the Hotwire ATM SDSL card, quality of service control spans the entire network eliminating the uncertainty of best effort network designs. CBR, VBR-rt, VBR-nrt, and UBR are supported.

Benefits

FrameSaver DSL provides all the benefits of world-class diagnostics and SLM with the cost advantages of DSL access:

- ATM Transport with QoS to insure necessary Quality of Service across the entire network
- Base configuration provides comprehensive diagnostics and reporting capabilities
- Command activated SLV key provides additional service level management and historical reporting capabilities
- Reduces operational costs through proactive and historical diagnostics
- Nondisruptive, end-to-end diagnostics allow accurate fault isolation and speedy trouble-ticket closure without customer disruption or LEC coordination.
- Software downloadability and adherence to standards protects investments and reduces life-cycle costs
- Provides conversion between ATM F4/F5 OA&M and Frame Relay LMI

The following diagram shows the FrameSaver DSL unit in a frame relay network.



FrameSaver DSL Feature Sets

Depending upon the model ordered, the FrameSaver DSL unit has the basic FrameSaver frame relay and diagnostic capability, or it is enhanced with additional SLV (Service Level Verification) reporting capability. These are referred to as feature sets, which provide different levels of intelligence for monitoring, managing, and reporting performance of the unit.

The two feature sets include:

- **Basic Feature Set.** Models with this feature set provide basic capability, which includes the following:
  - Device Health and Status
  - Layer 1 (Physical) and Layer 2 (Frame Relay) performance statistics
  - Nondisruptive Permanent Virtual Circuit (PVC) diagnostics
  - A troubleshooting virtual circuit for DSL access provider use and remote management
  - Limited RMON (Remote Monitoring) functionality
  - Multiplexed management PVCs for use by the frame relay network service provider or customer

  See *Basic Features* for other features and additional information.

- **Advanced SLV Feature Set.** Models with this feature set (sometimes referred to as Feature Set or Group 2) provide all the basic capability, plus advanced SLV (Service Level Verification) features. When additional SLV data is collected and the unit is accessed from an OpenLane SLM system, Web access to the following information is available:
  - TruePut™ Technology using Frame and Data Delivery Ratios
  - Web browser access to all diagnostic and reporting functions
  - Historical SLA (Service Level Agreement) verification and trend reports
  - Real-time RMON (remote monitoring) alarms and configurable alarm thresholds
  - Real-time and historical network performance graphs
  - Multiplexed customer PVCs

  See *Advanced SLV Features* for other features and more information about the additional SLV capability.

You can activate the additional SLV features at any time by ordering a FrameSaver SLV Activation Certificate. You must have the OpenLane SLM system to activate the additional SLV features in the unit.

To obtain an activation certificate, provide the model number (9783), your OpenLane system license key number, and the number of FrameSaver units whose SLV capability is to be activated. When you receive your certificate, it will include an Activation Certificate number, the Feature Group Number for the additional SLV features (Feature Group 2), your OpenLane license key number, and the number of device activations (license keys) ordered.

When ready to activate SLV capability in the unit(s), run the OpenLane SLM application. It will prompt you for the serial numbers of the units to be activated, their IP addresses, and whether the activations will be immediate or scheduled. OpenLane then activates SLV capability in the designated units and the units are reset. A report summary will be available that provides information about the activation certificate, the activated units, and the number of license keys remaining.

The following table summarizes the features that are included in the two feature sets. See *Basic Features* and *Advanced SLV Features* for additional information.

	Feature Set	
Feature	**Basic**	**Advanced SLV**
Frame relay performance statistics	Yes	Yes
SLV performance statistics (e.g., FDR/DDR, latency, CIR/EIR relationships)	No	Yes
Trap Log	Yes	Yes
Multiplexed user data DLCIs	No	Yes
Troubleshooting DLCI for remote management	Yes	Yes
Layer 2 (data link) diagnostics (nondisruptive DLCI loopbacks)	Yes	Yes
PVC Burst Table	Yes	Yes
User history available via SNMP RMON2 polling	Yes	Yes
User history available via FTP	No	Yes
RMON alarms and proactive alarm thresholds	No	Yes
OpenLane SLM system real-time applications	Limited (no SLM)	Yes
OpenLane SLM system historical reports and graphs	No	Yes
NetScout Manager Plus support	Alarms and history	Alarms and history

Basic Features

The FrameSaver DSL unit provides the following features:

- **Easy Installation.** When AutoBaud is used, no configuration is required. SNMP options may be modified if desired to provide security and enable traps.
- **Frame Relay Aware Management.** Supports diagnostic and network management features over the frame relay network. The unit's frame relay capability also supports:
  - — Inband management channels over the frame relay network using dedicated PVCs.
  - — Unique nondisruptive diagnostics.
  - — 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.** Unique diagnostics, performance monitoring, PVC-based in-band network management, and SNMP connectivity is not dependent upon external routers, cables, or LAN adapters.
- **Inverse ARP and Standard RIP Support.** Provides Inverse ARP (Address Resolution Protocol) support so the frame relay router at one end of a management PVC can acquire the IP address of a FrameSaver unit at the other end of the PVC. Standard RIP (Routing Information Protocol) allows the router to automatically learn the routes to all FrameSaver units connected to that FrameSaver unit.
- **Security.** Provides multiple levels of security to prevent unauthorized access to the unit.
- **Auto-Configuration**. Provides the following automatic configuration features:
  - — CIR Determination – For automatic recalculation of 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 you to control 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 so the data can be transferred as a background task using the standard File Transfer Protocol (FTP) over extended periods of time using low bandwidth.

- **Dual Flash Memory.** Allows software upgrades while the unit is up and running. Two software loads can be stored and implemented at the user's discretion.
- **Multiplexed Management 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.**

Feature	Models	
	9783-A1-211 9783-A1-221	9783-A1-213 9783-A1-223
Through Connections (PVCs)	8	64
Dedicated Management PVCs	2	2

- **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. This occurs when the FrameSaver unit is operating in frame relay mode.
- **Frame Relay Traffic Policing.** Ensures proper alignment and correlation of CIR (Committed Information Rate) values between the FrameSaver unit and the frame relay interworking function on the network switch. When this feature is enabled, the unit can enforce CIR and EIR (Excess Information Rate), marking frames that exceed CIR as DE (Discard Eligible) using the same method used by the switch, and discarding frames whose transmission would cause committed burst size (B_c) and excess burst size (B_e) to be exceeded.
- **RMON User History Performance Statistics via SNMP Polling.** Provides access to ESF line, physical interface, and basic frame relay performance statistics by polling the FrameSaver unit using SNMP (Simple Network Management Protocol). These statistics are available real-time via the Enterprise MIB and historically as an RMON2 User History object.
- **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.
- **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 unit's menu-driven user interface or the OpenLane system.

  These tests include V.54 or FT1-ANSI data channel loopback support so the frame relay network service provider can perform a physical loopback from its own switch without having to contact the local service provider for loopback activation.

- **LMI Packet Capture.** Provides a way of uploading data that has been captured 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.

Advanced SLV Features

The following additional features are provided with the advanced SLV feature set:

- **TruePut™ Technology.** Using Frame Delivery Ratios (FDR) and Data Delivery Ratios (DDR), throughput (within and above CIR, as well as between CIR and EIR, and above EIR) can be measured precisely, eliminating inaccuracies due to averaging.
- **Intelligent Service Level Verification.** 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.** Provides the ability to change SLA parameter and RMON alarm thresholds via the OpenLane system to correct them in real-time, before the SLA is violated.
- **Multiplexed Customer PVCs.** Provides a method of multiplexing customer management data and user data with network management data transparently over a single PVC (Permanent Virtual Circuit) when FrameSaver devices are at each end of the circuit.
- **FTP User History Poller.** Provides a bulk collector using FTP through the OpenLane system that generates a file for data at the time that data is uploaded using FTP.
- **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 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.
- **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.

See *OpenLane SLM System* for additional information.

OpenLane SLM System

Being standards-based, the OpenLane SLM (Service Level Management) system can be used with other management applications like HP OpenView or IBM's NetView. OpenLane includes HP OpenView adapters for integrating OpenLane features with the OpenView Web interface.

Being Web-based, the OpenLane system provides Web access to the data contained in the database to provide anytime, anywhere access to this information via a Web browser.

Some of the OpenLane system's features include:

- Real-time performance graphs provide exact performance measurement details (not averages, which can skew performance results) of service level agreement (SLA) parameters.
- Historical SLV graphs provide service level management historical reports so frame relay SLAs can be verified.
- Diagnostic troubleshooting provides an easy-to-use tool for performing tests, which include end-to-end, PVC loopback, connectivity, and physical interface tests.
- Basic configuration allows you to configure FrameSaver devices, and set RMON alarms and thresholds. Network DLCI Circuit IDs can also be assigned.
- Automatic SLV device and PVC discovery allows all SLV devices with their SLV Delivery Ratio configuration option enabled to be discovered automatically, along with their PVCs.
- A FrameSaver unit can be reset from the OpenLane system.
- Firmware downloading provides an easy-to-use tool for downloading to an entire network or a portion of the network.
- On-demand polling of FrameSaver devices, and SNMP polling and reporting are available.
- Configuration of circuits across the Hotwire GranDSLAM and endpoint for easy provisioning by the DSL router.

User Interface and Basic Operation

2

This chapter explains how to access, use, and navigate the menu-driven user interface. It includes the following:

What appears on the 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 unit and the router.
  - — A LAN port.
- Dial-in connection using an external modem.
- Direct terminal connection over the COM port.

When logging on, the User Interface Idle screen appears.

- If no security was set up or security was disabled, the Main Menu screen appears (see *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.

When the user interface has been idle, a session is automatically ended and the screen goes blank when the unit times out. 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.

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 SNMP trap is generated. ■ Access is denied. See your system administrator to verify your login (Login ID/Password combination).

FrameSaver units 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 client 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 redisplayed. 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.

▶ 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 the Configuration branch, see *Saving Configuration Options* in Chapter 3, *Configuration Procedures*.

Main Menu

Entry to all of the FrameSaver unit's tasks begins at the Main Menu, which has six menus or branches. The Access Level at the top of the screen only appears when security has been set up.

```
main                              Access Level: 1                          9783
Device Name: Node A                                                05/13/2000 02:01

                                    MAIN MENU

                                   Status
                                   Test
                                   Configuration
                                   Auto-Configuration
                                   Control
                                   Easy Install

--------------------------------------------------------------------------------
Ctrl-a to access these functions                                           Exit
```

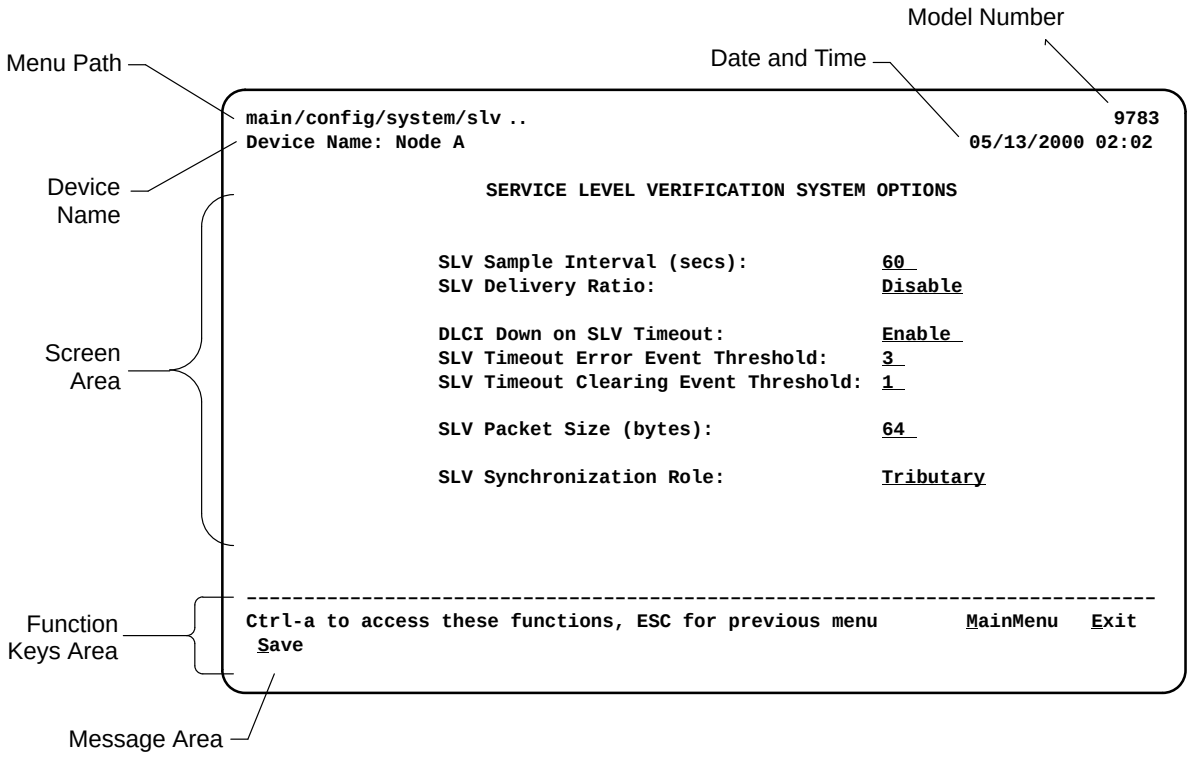
Select . . .	To . . .
Status	View diagnostic tests, interfaces, PVC connections, and statistics. You can also display LEDs and FrameSaver unit identity information.
Test	Select and cancel tests for the FrameSaver unit's interfaces.
Configuration	Display and edit the configuration options.
Auto-Configuration	Configure basic access unit setup automatically based upon a selected application. You can also automatically populate network and data port DLCI configuration options with numeric settings.
Control	Control the menu-driven user interface, device naming, login administration, and selecting software releases. You can also initiate a power-on reset of the FrameSaver unit.
Easy Install	Select Leased Line or Frame Relay mode for minimal configuration and a quick installation.

See Appendix A, *Menu Hierarchy*, for a pictorial view of the menu hierarchy, which represents the organization of the FrameSaver unit's menus and screens.

Screen Work Areas

There are two user work areas:

- **Screen area** – Where you input information into fields.
- **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 identification of the FrameSaver unit.
9783 9783-C 9783-SLV 9783-C-SLV	FrameSaver unit's model number. ■ This is a remote-site unit that supports 8 PVCs. ■ This is a central-site unit that supports 64 PVCs. ■ This is a remote-site unit that supports 8 PVCs and has the advanced SLV feature set installed. ■ This is a central-site unit that supports 64 PVCs and has the advanced SLV feature set installed.
Screen Area	Selection, display, and input fields for monitoring and maintaining the FrameSaver unit.
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 the Screens

You can navigate the screens by:

- Using keyboard keys.
- Switching between the two screen work areas using function keys.

Keyboard Keys

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

Press . . .	**To . . .**
Ctrl-a	Move cursor between the screen area and the screen function keys area.
Esc	Return to the previous screen.
Right Arrow (on same screen row), or Tab (on any screen row)	Move cursor to the next field.
Left Arrow (on same screen row), or Ctrl-k	Move cursor to the previous field.
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.
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.
Left Arrow or Ctrl-b	Move cursor one character to the left if in edit mode.
Ctrl-l	Redraw the screen display, clearing information typed in but not yet entered.
Enter (Return)	Accept entry or, when pressed before entering data or after entering invalid 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.

These keys use the following conventions:

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	Modify 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. Variations include: ■ ClrSLV&DLCIStats for clearing SLV and DLCI statistics. ■ ClrLinkStats for clearing frame relay link 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.

▶ Procedure

To return to a previous screen, press the Escape (Esc) 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:

1. Press Ctrl-a to switch from the screen area to the function keys area.
2. Select either the function's designated (underlined) character or Tab to the desired function key.
3. Press Enter. The function is performed.

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

Selecting a Field

Once you reach the desired menu or screen, select a field to view or change, or issue a command.

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.

Entering Information

You can enter information in one of three ways. Select the field, then:

- Manually type in (enter) the field value or command.

  Example:
  Entering **bjk** as a user's Login ID on the Administer Logins screen (from the Control menu/branch).

- Type in (enter) the first letter(s) of a field value or command, using the unit's character-matching feature.

  Example:
  When configuring a port's physical characteristics with the Port (DTE) Initiated Loopbacks configuration option/field selected (possible settings include Disable, Local, DTPLB, DCLB, and Both), entering **d** or **D** displays the first value starting with d – Disable. In this example, entering **dt** or **DT** would display DTPLB as the selection.

- Switch to the function keys area and select or enter a designated function key.

  Example:
  To save a configuration option change, select Save. S or s is the designated function key.

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.

Configuration Procedures

3

This chapter includes the following:

Basic Configuration

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

The Configuration Edit/Display menu of the FrameSaver DSL Unit is shown below.

Configuration Menu

```
main/config                                                          9783
Device Name: Node A                                    05/13/2000 03:01

                          CONFIGURATION EDIT/DISPLAY

                            System
                            Network
                            Data Ports
                            PVC Connections
                            Management and Communication









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

Configuration Option Areas

The FrameSaver unit 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:

- *FrameSaver DSL 9783 Quick Reference*
- *Configuration Option Tables* in Chapter 4, *Configuration Options*

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.
Customer Configuration 2	Another alternate set of configuration options that the customer can set up and store for future use.
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 only save those changes to the Current, Customer 1, or Customer 2 configuration option areas. The Current, Customer 1, and Customer 2 configuration option areas are identical to the Default Factory Configuration until modified by the customer.

Accessing and Displaying Configuration Options

To access and display configuration options, load (copy) the applicable 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 so 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 Configuration 1 or 2 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 and press Enter (Current Configuration, Customer Configuration 1, Customer Configuration 2, or Default Factory Configuration).

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

This sequence of steps would be shown as the menu selection sequence:

Main Menu → Configuration

Changing Configuration Options

▶ 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. Select the configuration options that are applicable to your network, and make appropriate changes to the setting(s). See Chapter 2, *User Interface and Basic Operation*, for additional information.

   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.

NOTE:

- Only Security Access Level 1 users can change configuration options.
- Security Access Level 2 users can only view configuration options and run tests.
- Security Access Level 3 users can only view configuration options; they cannot change configuration options or run tests.

Saving Configuration Options

When changes to the configuration options are complete, use the Save function key to save your changes to either the Current, Customer 1, or Customer 2 configuration areas.

NOTE:

When changing settings, you must Save for changes to take effect.

▶ Procedure

To save the 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 (usually the Current Configuration) and press Enter.

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

   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

Overview

A variety of configuration options are provided, but not ordinarily required. The recommended configuration tool for the FrameSaver DSL unit is the OpenLane Service Level Management system.

This chapter includes the following:

- *Setting Up Management and Communication Options*
  - *Configuring Node IP Information*
  - *Configuring Management PVCs*
  - *Configuring General SNMP Management*
  - *Configuring Telnet and/or FTP Session Support*
  - *Configuring SNMP NMS Security*
  - *Configuring SNMP Traps*
  - *Configuring the Ethernet Port*
  - *Configuring the Communication Port*
  - *Configuring the COM Port to Support an External Modem*

Using the Easy Install Feature

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

The Easy Install feature allows minimal configuration of the FrameSaver DSL Unit. Once the unit is installed and minimal configuration is completed using Easy Install, the NOC (Network Operation Center) can complete configuration of the unit and verify the setup.

Main Menu → Easy Install

Easy Install Screen Example

```
main/easy_install                                                    9783
Device Name: Node A                                    05/13/2000 04:01
                                EASY INSTALL



          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 Port Options Screen

          Network 1 DSL Line Rate (Kbps)    AutoRate




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

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

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

Node IP Address
Possible Settings: **001.000.000.000 – 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. **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 subnet mask needed to access the node. Since the subnet mask is not bound to a particular port, it can be used 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 class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.
TS Access (Type)
Possible Settings: **None, VPI,VCI, DLCI_on_VPI,VCI** Default Setting: **VPI,VCI**
Specifies whether a DLCI or Virtual Circuit (VC) is defined for troubleshooting by the service provider. **None** – No troubleshooting link is defined. **VPI,VCI** – A troubleshooting VC is defined. Its identifiers must be entered in the next field. **DLCI_on_VPI,VCI** – A DLCI is defined on a specified VC. The identifiers must be entered in the following fields.
TS Access (DLCI)
Possible Settings: **16–1007** Default Setting: blank
Specifies the DLCI on the network interface to be used for troubleshooting by the service provider. *Display Conditions* – This option only appears when TS Access type is DLCI_on_VPI,VCI. **16 – 1007** – Specifies the DLCI.
TS Access (VPI)
Possible Settings: **0–15** Default Setting: **0**
Specifies the VPI on the network interface to be used for troubleshooting by the service provider. VPI 0, VCI 35 is the default management path between the FrameSaver DSL unit and the Hotwire GranDSLAM. **0 – 15** – Specifies the VPI.

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

TS Access (VCI)
Possible Settings: **32–255** Default Setting: **0**
Specifies the VCI on the network interface to be used for troubleshooting by the service provider. VPI 0, VCI 35 is the default management path between the FrameSaver DSL unit and the Hotwire GranDSLAM. **32 – 255** – Specifies the VCI.
Create a Dedicated Network Management Link
With the cursor on the Create a Dedicated Network Management Link field, press Enter. When prompted, enter a DLCI for the link from 16 to 1007. The management link DLCI is added or modified.
Ethernet Port Options Screen
With the cursor on the Ethernet Port Options Screen field, press Enter. The Ethernet Port Options screen appears. See *Configuring the Ethernet Port* on page 4-40. After configuring the Ethernet port configuration options, save your changes. Then press the Esc key to return to the Easy Install screen.
Network 1 DSL Line Rate (Kbps)
Possible Settings: **AutoRate, 144, 192, 272, 384, 400, 528, 768, 1168, 1552, 2320** Default Setting: **AutoRate**
Determines whether the rate on the DSL interface is automatically detected using the Conexant AutoBaud algorithm, or set to a specific value. **144 – 2320** – The DSL line rate is set to the specified value. **AutoRate** – The DSL line rate is automatically detected from the DSL interface.

Setting Up So the Router Can Receive RIP

Using the system's standard Routing Information Protocol (RIP) feature, routing information is passed to the router over the management PVC, so the router can learn routes to FrameSaver devices. The Node IP address must be set (see *Configuring Node IP Information*).

▶ Procedure

1. Configure the router to receive RIP.

   For example, if using a Cisco router, configure **`config-t`**, **`router RIP`**, **`int serialx`**, **`IP RIP Receive version 1`**, then **`ctl-z WR`**.

2. Create a Standard DLCI for the user data port.

   Configuration → Data Ports → DLCI Records

3. Create a Management PVC using the user data port DLCI just configured.

   Configuration → Management and Communication → Management PVCs

4. Set Primary Link RIP to Standard_Out, and Save the configuration.

Refer to Table 4-9, DLCI Record Options, and Table 4-12, Management PVC Options for configuration information.

Entering System Information and Setting the System Clock

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

Main Menu → Control → System Information

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

If the selection is . . .	Enter the . . .
Device Name	Unique name for device identification of up to 20 characters.
System Name	SNMP system name; can be up to 255 characters.
System Location	System's physical location; can be up to 255 characters.
System Contact	Name and how to contact the system person; can be up to 255 characters.
Date	Current date in the month/day/year format (mm/dd/yyyy).
Time	Current time in the hours:minutes format (hh:mm).

NOTE:

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

See Chapter 5, *Security and Logins*, to set up and administer logins.

Configuration Option Tables

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

The following configuration option tables are included:

- Table 4-2. System Frame Relay and LMI Options
- Table 4-3. Service Level Verification Options
- Table 4-4. General System Options
- Table 4-5. Network Physical Interface Options
- Table 4-6. Data Port Physical Interface Options
- Table 4-7. Data Port Frame Relay Options
- Table 4-8. Network ATM Options
- Table 4-9. DLCI Record Options
- Table 4-10. PVC Connection Options
- Table 4-11. Node IP Options
- Table 4-12. Management PVC Options
- Table 4-13. General SNMP Management Options
- Table 4-14. Telnet and FTP Session Options
- Table 4-15. SNMP NMS Security Options
- Table 4-16. SNMP Traps Options
- Table 4-17. Ethernet Port Options
- Table 4-18. Communication Port Options
- Table 4-19. External Modem (COM Port) Options

Configuring the Overall System

The System menu includes the following:

- Frame Relay and LMI
- Service Level Verification
- General

Configuring Frame Relay and LMI for the System

Select Frame Relay and LMI from the System menu to display or change the Frame Relay and LMI options for the entire system (see Table 4-2).

Main Menu → Configuration → System → Frame Relay and LMI

Table 4-2. System Frame Relay and LMI Options (1 of 2)

LMI Behavior
Possible Settings: **Independent, Port-1_Follows_Net1-FR1, Net1-FR1_Follows_Port-1, Port-1_Codependent_with_Net1-FR1** Default Setting: **Port-1_Codependent_with_Net1-FR1**
Configures the device to allow the state of the LMI on Port-1 or ILMI on the network interface to be passed from one interface to another, determining how the unit will handle a change in the LMI or ILMI state. Sometimes referred to as LMI pass-through. **Independent** – Handles the state of each interface separately so that the LMI state of Port-1 has no effect on the ILMI state of the network interface, and vice versa. **Net1-FR1_Follows_Port-1** – Brings VCs cross-connected to Port-1 down on the network interface when LMI on Port-1 goes down. When LMI on Port-1 comes back up, the network VCs are reenabled. Used at central sites, this setting is useful 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 LMI down on Port-1 upon a physical failure or ATM failure. When the alarm on the network interface is cleared, Port-1 is reenabled 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** – Brings VCs cross-connected to Port-1 down on the network interface when LMI on Port-1 goes down (or LMI down on Port-1 when a physical failure or ATM failure occurs on the network interface), and brings VCs cross-connected to Port-1 up on the network interface when LMI on Port-1 comes up (or LMI up on Port-1 when a physical failure or ATM failure is cleared on the network interface). 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.
Traffic Policing
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether or not CIR (Committed Information Rate) and EIR (Excess Information Rate) will be enforced by the unit on frames being sent on network frame relay links. **Enable** – CIR and EIR are enforced. – Frames that exceed CIR will be marked Discard Eligible (DE). These frames are counted in the **`Above CIR but within EIR`** category until this category is full. Once full, additional frames are counted as being in the **`Within CIR`** category. – Frames in excess of EIR will be discarded. **Disable** – CIR and EIR are not enforced.

Table 4-2. System Frame Relay and LMI Options (2 of 2)

LMI Error Event (N2)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 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.
LMI Clearing Event (N3)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 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 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.
LMI Status Enquiry (N1)
Possible Settings: **1, 2, 3, 4, . . . 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, which sets the number of seconds between the initiation of status enquiry 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 enquiry messages in increments of 5.
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. **5 – 30** – Specifies the number of seconds between the receipt of status enquiry messages in increments of 5.
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. **5 – 30** – Specifies the interval of time in increments of 5.

Configuring Service Level Verification Options

SLV options are selected from the System menu (see Table 4-3).

Main Menu → Configuration → System → Service Level Verification

Table 4-3. Service Level Verification Options (1 of 2)

SLV Sample Interval (secs)
Possible Settings: **10 – 3600** Default Setting: **60**
Sets the inband communications interval between FrameSaver 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 Delivery Ratio
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether communication of Frame and Data Delivery Ratios (FDR/DDR) between FrameSaver devices is enabled. To use this capability, both ends of all PVCs must be FrameSaver devices. If some of the units are FrameSaver 9124s or 9624s, they must be running software version 1.2 or higher. **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 missed SLV packets will be monitored along with the LMI status to determine the status of PVC connections to remote FrameSaver units. 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, causing the DLCI's status to turn Inactive, an alarm and SNMP trap are generated, and a Health and Status message created. **Disable** – Missed SLV packets are monitored, but the DLCI is not declared down.
SLV Timeout Error Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **3**
Specifies the number of consecutive missed SLV communications that must be detected before a DLCI Inactive status is declared. **1– 20** – Sets the limit for these error events.

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

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 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.
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 FrameSaver 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.

Configuring General System Options

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

Main Menu → *Configuration* → *System*→ *General*

Table 4-4. General System Options

Test Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether or not loopback and pattern tests have a duration after which they are terminated automatically. This setting does not effect DTE-commanded tests or the LMI Packet Capture Utility feature. **Enable** – All Loopback and Pattern tests have a timeout. This setting is recommended when the FrameSaver unit is managed remotely through an in-band data stream. If the FrameSaver unit is accidently commanded to execute a disruptive test on the interface providing the management access, control can be regained after the timeout expires, terminating the test. **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 only appears when Test Timeout is set to Enable. **1 – 120** – Sets the Test Timeout period in minutes (inclusive).

Configuring the Physical Interfaces

Characteristics for the following physical interfaces can be configured:

- Network Interface
- User Data Port

Configuring the Network Interface

When configuring the physical characteristics for the network interface, select Physical from the Network menu (see Table 4-5).

Main Menu → Configuration → Network → Physical

Table 4-5. Network Physical Interface Options

Network 1 DSL Line Rate (Kbps)
Possible Settings: **AutoRate, 144, 272, 384, 400, 528, 768, 1168, 1552, 2320** Default Setting: **AutoRate**
Determines whether the rate on the DSL interface is automatically detected using the Conexant AutoBaud algorithm, or set to a specific value. **144 – 2320** – The DSL line rate is set to the specified value. **AutoRate** – The DSL line rate is automatically detected from the DSL interface.
SNR Margin 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 at which a Signal to Noise Ratio margin threshold condition is declared. **–5 – 10** – Specifies the threshold level.

Configuring the User Data Port

Select Physical from the Data Ports menu to configure the physical characteristics for the user data port (see Table 4-6).

Main Menu → Configuration → Data Ports → Physical

Table 4-6. Data Port Physical Interface Options (1 of 2)

Invert Transmit Clock
Possible Settings: **Auto, Enable, Disable** Default Setting: **Auto**
Determines whether the clock supplied by the FrameSaver unit 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.
Transmit Clock Source
Possible Settings: **Internal, External** Default Setting: **Internal**
Determines whether the DTE's transmitted data is clocked into the FrameSaver unit by its internal transmit clock or by the external clock provided by the DTE. NOTE: Changing settings for this configuration option causes the FrameSaver unit to abort any physical port tests, including any DTE-initiated loopback tests. **Internal** – The FrameSaver unit uses 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 whether the state of the Request To Send (RTS) circuits on the user data port will be used to determine when valid data communication is possible with the DTE. 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 data communication is possible with the DTE. **Disable** – RTS is not monitored. RTS is assumed to be asserted and data is being transmitted, regardless of the state of the lead.

Table 4-6. Data Port Physical Interface Options (2 of 2)

Monitor DTR
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the DTE Ready (DTR) circuit on the user data port will be 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 data terminal equipment using the port's 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 for the Data Port

Select Frame Relay from the Data Ports menu to display or change the Frame Relay options (see Table 4-7).

Main Menu → Configuration → Data Ports → Frame Relay

Table 4-7. Data Port Frame Relay Options (1 of 2)

LMI Protocol
Possible Settings: **Initialize_From_Net1FR1**, **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 protocol will *not* be updated after being initially discovered. The frame relay link discovers the LMI protocol from an attached device via LMI status polls. **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 whenever 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 (see Table 4-2, System Frame Relay and LMI Options). **Custom** – Use the following options in this table to configure LMI parameters.
LMI Error Event (N2)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 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.

Table 4-7. Data Port Frame Relay Options (2 of 2)

LMI Clearing Event (N3)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 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 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.
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. **5 – 30** – Specifies the number of seconds between the receipt of status enquiry messages in increments of 5.
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. **5 – 30** – Specifies the interval of time in increments of 5.

Configuring ATM for the Network Interface

Select ATM from the Network menu to display or change the ATM options (see Table 4-8).

Main Menu → *Configuration* → *Network* → *ATM*

Table 4-8. Network ATM Options

Cell Delineation Error Event Threshold
Possible Settings: **1–1000** Default Setting: **10**
Specifies the number of Out of Cell Delineation (OCD) events that must occur in a one minute interval for a Loss of Cell Delineation (LCD) alarm to be declared. **1 – 1000** – Specifies the LCD threshold.

Configuring Circuit and DLCI Records

Circuit and DLCI records can be created and modified, and PVCs created based on existing DLCIs, using the Network Circuit Records screen and the Data Ports DLCI Records screen:

Main Menu → Configuration → Network → Circuit Records

Main Menu → Configuration → Data Port → DLCI Records

Table 4-9. DLCI Record Options (1 of 3)

DLCI Number
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
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 to 1023. However, the numbers 0 to15 and 1008 to 1023 are 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 settings for this configuration option causes the FrameSaver unit to abort any active frame relay tests. **16 – 1007** – Specifies the DLCI number (inclusive).
VPI,VCI Number (VPI)
Possible Settings: **0 – 15** Default Setting: Initially blank; no default.
Specifies the VPI. Entry of an invalid number results in the error message **`Value Out of Range (0 – 15)`**. The VPI/VCI must be unique on the ATM link. *Display Conditions* – This option does not appear for the user data port. **0 – 15** – Specifies the VPI.
VPI,VCI Number (VCI)
Possible Settings: **32 – 255** Default Setting: Initially blank; no default.
Specifies the VCI. Entry of an invalid number results in the error message **`Value Out of Range (32 – 255)`**. The VPI/VCI must be unique on the ATM link. *Display Conditions* – This option does not appear for the user data port. **32 – 255** – Specifies the VCI.

Table 4-9. DLCI Record Options (2 of 3)

DLCI Type
Possible Settings: **Standard, Multiplexed** 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. *Display Conditions* – This option does not appear for the user data port, and it 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.
CIR (bps)
Possible Settings: **0 – 2320000** Default Setting: **64000**
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* = the maximum line rate available on the port. **0 – 2320000** – 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. This value is calculated based upon the settings for the Committed Burst Size Bc (Bits) and CIR (bps) options.
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: **0 – 2320000** Default Setting: **64000**
Allows you to display or change the DLCI's committed burst size. *Display Conditions* – This option only appears when Committed Burst Size is set to Other. **0 – 2320000** – Specifies the DLCI's committed burst size.

Table 4-9. DLCI Record Options (3 of 3)

Excess Burst Size (Bits)
Specifies the maximum amount of data in bits that the network may accept beyond the CIR without discarding frames.
Be
Possible Settings: **0 – 2320000** Default Setting: **2256000**
Allows you to display or change the DLCI's excess burst size. **0 – 2320000** – 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 *quality of service*). 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 management PVCs on this DLCI to the network. *Display Conditions* – This option is not available on a user data port. **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

The Auto-Configuration feature automatically configures PVC connections and their DLCI Records. PVC connections can also be created manually (see Table 4-10).

Main Menu → Configuration → PVC Connections

From this screen, you can go directly to the Management PVC screen by selecting the MgmtPVCs function key for easy movement between screens. See *Configuring Management PVCs* on page 4-28 for management PVC configuration options.

Quick removal of unused DLCIs included in an existing PVC Connection, except for HQ_Site, is also available when the Delete function key is selected and you respond Yes to the **`Remove otherwise unused components associated with the deleted PVC?`** prompt.

Table 4-10. PVC Connection Options (1 of 2)

Source Link
Possible Settings: **Port-1, Net1-FR1** Default Setting: Initially blank; no default.
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** – 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; no default.
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; no default.
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 only appears when Source DLCI contains a multiplexed DLCI record number. **0 – 62** – Specifies the EDLCI number.

Table 4-10. PVC Connection Options (2 of 2)

Destination Link
Possible Settings: **Net1-FR1** Default Setting: Initially blank; no default.
Specifies the frame relay interface used as the destination link; the **to** 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 which are not part of a PVC connection or management link. For example, if the network interface has no DLCIs defined, Net1-FR1 would not appear as a valid setting. **Net1-FR1** – Specifies the Network interface as the destination link.
Destination DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
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 basic 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; no default.
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 only appears when the Primary Destination DLCI contains a multiplexed DLCI record number. **0 – 62** – Specifies the EDLCI number.

Setting Up Management and Communication Options

The following options can be selected from the Management and Communication menu:

- Node IP Options
- Management PVC Options
- General SNMP Management Options
- Telnet and FTP Sessions Options
- SNMP NMS Security Options
- SNMP Traps Options
- Ethernet Port Options
- Communication Port Options
- External Modem (COM Port) Options

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 4-11). When deploying units to remote sites, minimally configure the Node IP Address and Subnet Mask.

Main Menu → Configuration → Management and Communication → Node IP

This set of configuration options includes a Troubleshooting (TS) Management Link feature 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.

TS_Management_Link is initially disabled in most models, but the link can be enabled at any time. Any valid network Management PVC created on a standard DLCI can be used. When enabled, a troubleshooting link can be accessed any time the service provider requests access. An assigned security level can also control access.

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

NOTE:

The unit may come from the factory with a TS Management PVC already set up (e.g., 980).

Table 4-11. Node IP Options (1 of 3)

Node IP Address
Possible Settings: **001.000.000.000 – 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. **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 subnet mask associated with the IP address that is needed to access the node. Since the subnet mask is not bound to a particular port, it can be used 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 class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.

Table 4-11. Node IP Options (2 of 3)

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. Examples: ■ If the default IP network is connected to the communications port, select COM. ■ If the default IP network is connected to a far-end device over the management PVC named London for the remote device located in the London office, select the PVC name London (as defined by the Name configuration option, Table 4-12, Management PVCs Options). NOTE: If the link to the IP destination selected as the default route becomes disabled or down, the unrouteable data will be discarded. Make sure that the link selected is operational, and if that link goes down, change the default destination. 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 times the retry count. **None** – No default network destination is specified. Unrouteable data will be discarded. This is the recommended setting. **COM** – Specifies that the default destination is connected to the COM port. Only appears when Port Use is set to Net Link (see Table 4-18, Communication Port Options). **Ethernet** – Specifies that the default destination is connected to the Ethernet port. Only appears when the Ethernet port's Interface Status option is enabled. When selected, the Default Gateway Address must also be configured (see Table 4-17, Ethernet Port Options). ***PVCname*** – Specifies a name for the management PVC. Only appears 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 PVC name, which is the link between the local FrameSaver unit and the one located in London. London would appear as one of the available selections.

Table 4-11. Node IP Options (3 of 3)

TS Access Management Link
Available Settings: **None, *PVCname***   Default Setting: **None**
Specifies a troubleshooting management link for the special needs of network service providers. 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 and the option is set to None, and the link and its DLCI and/or VPI,VCI will be deleted. **None** – Disables or does not specify a TS Access Management Link. ***PVCname*** – Specifies the name of the TS Management PVC. *Display Conditions* – This selection only appears when a dedicated management PVC has been defined on the network frame relay or ATM link.
TS Management Link Access Level
Available 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 when the service provider is using the TS Access Management Link. *Display Conditions* – This option only appears when 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 4-14, 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, change configuration options, and run tests. 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 view unit information and run tests only; they cannot change configuration options. **Level-3** – Allows Telnet access by network service providers with the capability to view unit information only; they cannot change configuration options or run tests.

Configuring Management PVCs

Select Management PVCs to define inband management links by adding or changing Management PVCs (see Table 4-12). First, DLCI records must have been configured for the interface where the Management PVC will reside. See *Configuring Circuit and DLCI Records* for additional information.

Main Menu → Configuration → Management and Communication → Management PVCs

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* for additional information).

From this screen, you can go directly to the PVC Connections screen by selecting the PVCConn function key for easy movement between screens.

Select the Delete function key, a Management PVC ID#, and respond Yes to the **`Remove otherwise unused components associated with the deleted PVC?`** prompt for quick removal of unused DLCIs. If the Management PVC selected is defined as a trap Initial Route Destination, a Default IP Destination, or a TS Access Management Link, an ... **`Are You Sure?`** prompt appears to warn you.

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

Table 4-12. Management PVC Options (1 of 3)

Name
Possible Settings: ***ASCII Text Entry*** Default Setting: Initially blank; no default.
Specifies a unique name for the management PVC as referenced on screens (e.g., Tampa for the Tampa, Florida office). ***ASCII Text Entry*** – Enter a unique name for the management PVC (maximum length 8 characters).
Intf IP Address
Possible Settings: **Node-IP-Address, Special** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-IP-Address**
Specifies the IP address needed to access the unit via this management PVC, providing connectivity to an external IP network through the frame relay network. **Node-IP-Address** – Uses the IP address contained in the Node IP Address (see Table 4-11, 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.

Table 4-12. Management PVC Options (2 of 3)

Intf Subnet Mask
Possible Settings: **Node-Subnet-Mask, Calculate, Special** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-Subnet-Mask**
Specifies the subnet mask associated with the IP address that is needed to access the unit when the management PVC is providing connectivity to an external IP network (through frame relay) that requires a specific subnet mask for the interface. **Node-Subnet-Mask** – Uses the *Interface* IP Subnet contained in the Node-Subnet Mask configuration option (see Table 4-11, 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. A text field displays where you can enter the subnet mask for this unit's management PVC.
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. This bit is used by the network to prioritize which frames to discard first during periods of network congestion. This allows management traffic to be viewed as lower priority than customer data. **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, Clear** Default Setting: Initially blank; no default.
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. **Net1-FR1** – Specifies that the network interface be used in the connection. **Port-1** – Specifies that the frame relay link on the user data port be used in the connection. **Clear** – Clears the link and the DLCI field, and suppresses the EDLCI field if the DLCI was multiplexed.

Table 4-12. Management PVC Options (3 of 3)

Primary DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
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., has a DLCI record), and it 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 (inclusive).
Primary EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the EDLCI number used for a management PVC when a multiplexed DLCI is selected. EDLCIs identify individual connections within multiplexed DLCIs that are unique to those DLCIs. Use a unique EDLCI to identify an individual connection within a multiplexed DLCI. 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. NOTE: Clearing the DLCI or changing it to a standard DLCI suppresses EDLCI field. **0 – 62** – Specifies the EDLCI number (inclusive).
Primary Link RIP
Possible Settings: **None, Proprietary, 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. **None** – Does not use a routing protocol. **Proprietary** – Uses a proprietary variant of RIP version 1 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 4-9, DLCI Record Options). **Standard_out** – The device will send 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 port connected to the FrameSaver unit for the management interface (e.g., Cisco: **`config-t, router RIP, int serial`*x*`, IP RIP Receive version 1, ctl-z WR`**). See *Setting Up So the Router Can Receive RIP*.

Configuring General SNMP Management

Select General SNMP Management to add, change, or delete the information needed to allow the FrameSaver unit to be managed as an SNMP agent by the NMS supporting the SNMP protocols (see Table 4-13).

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

You must have Level-1 access to display or configure these options.

Table 4-13. 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 nor send SNMP traps.
Community Name 1
Possible Settings: ***ASCII text entry*, Clear** Default Setting: **Public** in ASCII text field
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 an object in the MIB. ***ASCII text entry*** – Adds to or changes Community Name 1 (maximum 255 characters). **Clear** – Clears Community Name 1.
Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read/Write**
Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 1. **Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP **get** and **set** commands).
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 an object in the MIB. ***ASCII text entry*** – Adds to or changes Community Name 2 (maximum 255 characters). **Clear** – Clears Community Name 2.

Table 4-13. General SNMP Management Options (2 of 2)

Name 2 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 2. **Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP **get** and **set** commands).

Configuring Telnet and/or FTP Session Support

Telnet and FTP options control whether a Telnet or FTP (File Transport Protocol) session is allowed through an interconnected IP network and the access security applicable to the session. Two Telnet sessions can be active at a time (see Table 4-14).

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

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

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

Table 4-14. 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 a Telnet client on an interconnected IP network. **Enable** – Allows Telnet sessions between the FrameSaver unit and Telnet client. **Disable** – Does not allow Telnet sessions.
Telnet Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether a user ID and password (referred to as the login) are required to access the menu-driven user interface via a Telnet session. If required, the login used is the same login used for an 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 4-14. 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 one 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 by users with Login ID access levels of 1, 2, and 3, with the capability 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. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. A reset is required if the Communication Port's Port Use option is set to Net Link (see Table 4-4, General System Options). **Level-2** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information and run tests only; they cannot change configuration options. **Level-3** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information only; they 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.

Table 4-14. Telnet and FTP Session Options (3 of 3)

FTP Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the system responds as a server when an FTP (file transfer protocol) client on an interconnected IP network requests an FTP session. This option must be enabled when downloading files. **Enable** – Allows an FTP session between the system and an FTP client. **Disable** – Does not allow FTP sessions.
FTP Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether 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: **1 – 2320** Default Setting: **2320**
Sets the maximum receive rate of file transfer to the system via management PVCs. This option allows new software and configuration files to be downloaded using selected bandwidth without interfering with normal operation. Using this option, new software and configuration files can be downloaded quickly using the default settings, or at a slower rate over an extended period of time by selecting a slower speed. Based upon TCP flow control, the FTP server in the system throttles bandwidth to match this setting. **1 – 2320** – Sets the download line speed from 1 kilobits per second to the maximum management speed.

Configuring SNMP NMS Security

Select SNMP NMS Security from the Management and Communication menu to display, add, or change SNMP security configuration options for the FrameSaver unit to set up trap managers (see Table 4-15).

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

A table is displayed consisting of the network management systems identified by IP address that are allowed to access the FrameSaver unit by SNMP.

Table 4-15. SNMP NMS Security Options

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 – 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 to or changes the NMS IP address. **Clear** – Fills the NMS IP address with zeros.
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 access (SNMP Get command) to the MIB objects. This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP Get and Set commands) to the MIB objects. 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 4-16).

Main Menu → Configuration → Management and Communication → SNMP Traps

See Appendix B, *SNMP MIBs and 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 4-16. SNMP Traps Options (1 of 3)

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. An NMS IP Address must be configured in the NMS *n* IP Address configuration option for each trap manager to receive trap messages. **1 – 6** – Specifies the number of trap managers (inclusive).
NMS *n* IP Address
Possible Settings: **001.000.000.000 – 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. **Clear** – Fills the NMS IP address with zeros.

Table 4-16. SNMP Traps Options (2 of 3)

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 4-11, Node IP Options). **Ethernet** – Uses the Ethernet port. Only appears when the Ethernet port's Interface Status option is enabled (see Table 4-17, Ethernet Port Options). **COM** – Uses the COM port. Only available when Port Use is set to Net Link (see Table 4-18, Communication Port Options). ***PVCname*** – Uses the defined management *linkname* (the name given the Management PVC). Only appears 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 4-16. SNMP Traps Options (3 of 3)

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 these trap messages on the network interface only. **Ports** – Generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on the user data port only. **All** – Generates these 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
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 these trap messages on DLCIs for the network interface only. **Ports** – Generates these trap messages for DLCIs on a user data port only. **All** – Generates these trap messages on all frame relay interfaces. **None** – No DLCI trap messages are generated.
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 as a result of the Alarms and Events Groups of RMON1 when a selected variable's configured threshold is exceeded. *Display Conditions* – This option only appears for units with the SLV feature set. **Enable** – Sends RMON trap messages when set thresholds are exceeded. **Disable** – Does not send RMON trap messages.

Configuring the Ethernet Port

Select Ethernet Port from the Management and Communication menu to configure the Ethernet port (see Table 4-17).

Main Menu → Configuration → Management and Communication → Ethernet Port

Table 4-17. Ethernet Port Options (1 of 2)

Interface Status
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the Ethernet port is being used and can be configured. **Enable** – The port is active. It can receive Version 2 or IEEE 802.3 MAC frames, or transmit Version 2 MAC frames only. **Disable** – The port is not active. When the port is disabled, the following will occur: ■ No alarms or traps configured for the port will be generated. ■ All port uses that refer to the Ethernet port, like the Default IP Destination and Initial Route Destination, will be reset to their default values (see Table 4-11, Node IP Options, and Table 4-16, SNMP Trap Options).
IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the Ethernet port. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the port, which can be viewed or edited. **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 subnet mask associated with the IP address that is needed to access the Ethernet port. **000.000.000.000 – 255.255.255.255** – Set the Ethernet port's subnet mask. The range for each byte is 000 to 255. **Clear** – Fills the subnet mask associated with the IP address with zeros.
Default Gateway Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address for the port's default gateway. It is used for packets that do not have a route. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the port, which can be viewed or edited (i.e., a router on the LAN). **Clear** – Fills the default gateway's IP address with zeros.

Table 4-17. Ethernet Port Options (2 of 2)

Proxy ARP
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the port can be used to supply the MAC (Media Access Control) address of a FrameSaver unit at the other end of a PVC using ARP (Address Resolution Protocol). This technique is used for communication between devices on different networks but on the same subnet. Using this technique, the Default Gateway Address is provided when there is an ARP request, and when data is sent to the gateway, the gateway forwards the data to the appropriate device. The gateway acts as an agent for the destination device. **Enable** – Proxy ARP is enabled on the port. **Disable** – The port cannot be used to acquire the IP address of a FrameSaver unit at the other 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 4-18).

Main Menu → Configuration → Management and Communication → Communication Port

Table 4-18. Communication Port Options (1 of 4)

Port Use
Possible Settings: **Terminal, Net Link** Default Setting: **Terminal**
Assigns a specific use to the COM port. NOTE: If the Default IP Destination is set to COM (see Table 4-11, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. **Terminal** – The COM port is used for the asynchronous terminal connection. **Net Link** – The COM port is the network communications link to the IP network or IP device port.
Data Rate (Kbps)
Possible Settings: **9.6, 14.4, 19.2, 28.8, 38.4, 57.6, 115.2** Default Setting: **19.2**
Specifies the rate for the COM port in kilobits per second. **9.6 – 115.2 kbps** – Sets the communication port speed.
Character Length
Possible Settings: **7, 8** Default Setting: **8**
Specifies the number of bits needed to represent one character. NOTE: Character length defaults to 8 and cannot be changed if Port Use is set to Net Link. **7** – Sets the character length to seven bits. **8** – Sets the character length to eight bits. Use this setting if using the COM port as the network communication 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 character of transmitted data is approved as error-free if the “1” bits add up to an odd or even number as specified by this configuration option. **None** – Provides no parity. **Even** – Makes the sum of all 1 bits and its corresponding parity bit always even. **Odd** – Makes the sum of all 1 bits and its corresponding parity bit always odd.

Table 4-18. Communication Port Options (2 of 4)

Stop Bits
Possible Settings: **1, 2** Default Setting: **1**
Determines the number of stop bits used for the COM port. **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. **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 (referred to as the login) is required in order to log on to the asynchronous terminal connected to the COM port. *Display Conditions* – This option only appears 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 asynchronous terminal connected to the COM port. If a login is required for the 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. 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 will be permitted for the port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **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 3, make sure that the Telnet Session Access Level is set top 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** – Allows limited access and control of the device. The user can monitor and perform diagnostics, display status and configuration option information. **Level-3** – Allows limited access with monitoring control only. The user can monitor and display status and configuration screens only.

Table 4-18. 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 only appears when Port Use is set to Terminal. **Enable** – Disconnects user session after the specified time of inactivity. **Disable** – Does not disconnect user session.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Specifies the number of minutes of inactivity that can elapse before the session is disconnected. *Display Conditions* – This option only appears when Port Use is set to Terminal. **1 – 60** – Sets the time from 1 to 60 minutes (inclusive).
IP Address
Possible Settings: **001.000.000.000 – 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. 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 only appears 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. **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 only appears when Port Use is set to Net Link. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the COM port, 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 class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.

Table 4-18. 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 only appears 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 (e.g., Cisco: **`config-t, router RIP, int serialx, IP RIP Receive version 1, ctl-z WR`**). To create this management interface, make sure that Node or COM port IP Information has been set up (*Configuring Node IP Information*).

Configuring the COM Port to Support an External Modem

Select External Modem (Com Port) to display or change the configuration options that control call processing for an external device attached to the COM port (see Table 4-19).

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 *Standard EIA-232-D Crossover Cable* in Appendix C, *Connectors, Cables, and Pin Assignments*, for cable pin assignments.

Table 4-19. 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. **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). CAUTION: Do *not* use this setting if you have an asynchronous terminal connected to the COM port.
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.

Security and Logins

5

This chapter includes the following:

Limiting Access

The FrameSaver unit provides access security on the following interfaces:

- Asynchronous (async) terminal
- Telnet
- FTP
- SNMP

Up to two direct or Telnet sessions can be active at any given time; that is, you can have two simultaneous Telnet sessions, or one Telnet session and one active asynchronous terminal session, or two simultaneous asynchronous terminal sessions.

Controlling Asynchronous Terminal Access

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

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

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

▶ Procedure

To limit asynchronous terminal access to the menu-driven user interface:

1. Select the Communication Port options.

   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*.
Limit the effective access level to Level-3 or Level-2	Port Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the port (e.g., if a user has a Level-1 login and Level-2 port access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow Level-1 users to configure the unit, keep the access at Level-1.

NOTE:

See *Resetting the Unit and Restoring Communication* in Chapter 8, *Troubleshooting*, should you be locked out inadvertently.

3. Save your changes.

Controlling External COM Port Device Access

Dial-in access can be controlled when an external device (modem) is connected to the unit's communication (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 only appears when the External Device Commands option is set to AT.

3. Save your change.

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 or FTP Access

The FrameSaver unit provides several methods for limiting access via a Telnet or FTP session. Telnet or FTP access can be on a standard management link or on a service provider's troubleshooting (TS) management link.

Limiting Telnet Access

Telnet access can be limited by:

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

▶ Procedure

To limit Telnet 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 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*.
Assign an access level	Session Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the Telnet session (e.g., if a user has a Level-1 login and Level-2 telnet access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow users to configure the unit, keep the access at Level-1.

3. Save your changes.

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

Limiting FTP Access

FTP access can be limited by:

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

▶ 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*. If you want to allow users to configure the unit or perform file transfers, including downloads, keep the access at Level-1. Level-1 access is required to download software to the unit, or to upload or download configuration files. Level-3 is sufficient for NMS access for SLV historical information.
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 Session Support* 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 when the session is **on** the TS Management Link:

1. Select the Telnet and FTP Session 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.
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 Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the session (e.g., if a user has a Level-1 login and Level-2 telnet access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow users to configure the unit, keep the access at Level-1.

5. Save your changes.

See *Configuring Telnet and/or FTP Session Support* 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 IP addresses of those NMSs 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 change.

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 Management Information Base (MIB).
- Specifying the type of access allowed for each SNMP community name.

Whenever an SNMP manager attempts to access an object in the MIB, 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 names	Community Name 1 and Community Name 2 to a community name text, up to 255 characters in length.
Assign the type of access allowed for the SNMP community names	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 IP addresses of NMSs that can access the FrameSaver unit.
- Performing validation checks on the IP address of SNMP management systems attempting to access the FrameSaver unit.
- Specifying the access allowed for the authorized NMS when IP address validation is performed.

The SNMP NMS Security Options screen provides the configuration options that determine whether security checking is performed on the IP address of SNMP management systems attempting to communicate with the unit.

Make sure that SNMP Management is set to Enable.

Menu selection sequence:
Main Menu → *Configuration* → *Management and Communication* → *General SNMP Management* → *SNMP Management: Enable*

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

▶ Procedure

To limit SNMP access through IP addresses:

1. Select the SNMP NMS Security options:

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

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

To . . .	**Set the configuration option . . .**
Enable IP address checking	NMS IP Validation to Enable.
Specify the number (between 1 and 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 IP address.
Specify the access allowed for an authorized NMS when IP address validates 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.

Creating a Login

A login is required if security is enabled. (Security is enabled by the configuration options Login Required for the communication port, modem port, and Telnet Login Required or FTP Login Required for a Telnet or FTP Session.) Up to six login ID/password combinations can be created using ASCII text, and each login must have a specified access level. Logins must be unique and they are case-sensitive.

▶ 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 the . . .
Login ID	ID of 1 to 10 characters.
Password	Password from 1 to 10 characters.
Re-enter password	Password again to verify that you entered the correct password into the device.
Access Level	Access level: 1, 2, or 3. ■ Level-1 – User can add, change, and display configuration options, save, and perform device testing. ■ Level-2 – User can monitor and perform diagnostics, display status and configuration option information. ■ Level-3 – User can only monitor and display status and configuration screens. **CAUTION:** Make sure at least one login is set up for Level-1 access or you may be inadvertently locked out.

NOTE:

See *Resetting the Unit and Restoring Communication* in Chapter 8, *Troubleshooting*, should you be locked out inadvertently.

3. Save your changes.

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

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

Modifying a Login

Logins are modified by deleting the incorrect 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, and the record before the deleted record reappears.

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

Operation and Maintenance

6

This chapter includes the following information:

Displaying System Information

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

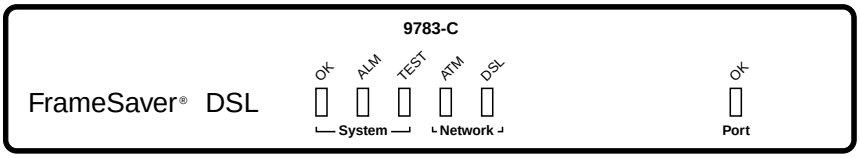
Main Menu → *Status* → *Identity*

View this field . . .	To find the . . .
System Name	Domain name for this SNMP-managed node (up to 255 ASCII characters).
System Contact	Contact person for this SNMP-managed node.
System Location	Physical location for this SNMP-managed node.
NAM	
NAM Type	Type of Network Access Module (NAM) installed (DSL FR-ATM NAM). This card type is supported by the SNMP SysDescr Object.
Serial Number	Unit's 7-character serial number.
Ethernet MAC Address	Media Access Control (MAC) address assigned to the Ethernet port during manufacturing.
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 is the same as for the Current Software Revision. ■ **`In Progress`** indicates that the flash memory is currently being downloaded. ■ **`Invalid`** indicates that no download has occurred or the download was not successful

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.

The central site unit (supporting 64 PVCs) is shown.



00-16769

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.

Main Menu → Status → Display LEDs and Control Leads

Display LEDs & Control Leads Screen

```
main/status/leds                                                    9783-C
Device Name: Node A                                      05/13/2000 06:01

                        DISPLAY LEDS & CONTROL LEADS

                                DSL FR-ATM NAM

              GENERAL        NETWORK1            PORT-1
              OK             Data Mode           OK
              Alarm          LOS                 TXD
              Test           Training            RXD
                             LCD                 DTR
              ATM Mode                           RTS




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

Refresh the screen to view control lead transitions. LED and control lead descriptions are in the sections that follow.

LED Descriptions

The following table identifies the alarms that cause the Alarm LED to light. See Table 6-2 and Table 6-3 for network and user data port interface LED information.

Table 6-1. General Status LEDs (1 of 1)

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

Table 6-2. Network Interface LEDs

Label	Indication	Color	What It Means
ATM	ATM Link Status	Multi-colored	Yellow – The ATM link is down. Green – The ATM link is up. OFF – The FrameSaver unit is in leased line mode.
DSL	DSL Status	Green	ON – The DSL link is in data mode and functioning normally. OFF – The DSL link is down. Flashing – The DSL link is training.

Table 6-3. User Data Port LED

Label	Indication	Color	What It Means
OK	Operational Status	Green	ON – The interchange circuits for the port are in the correct state to transmit and receive data. OFF – The port is idle. Occurs if the port is disabled, or if the port is configured to monitor DTR and/or RTS and the lead(s) is not asserted.

Control Lead Descriptions

In addition to the LEDs, certain control leads can be monitored through the Display LEDs and Control Leads screen. They are described in Table 6-4.

Table 6-4. Additional Control Leads

Label	Indication	What It Means
Network Interface		
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	A Loss Of Signal condition has been detected on the network.
Training	Training in Progress	The unit is training. The front panel DSL LED is flashing.
LCD	Loss of Cell Delineation	A Loss of Cell Delineation alarm condition has been detected. The front panel ATM LED is yellow.
User Data Port		
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 Data Terminal Equipment (DTE) is not ready to operate.
RTS	Request to Send	The DTE has indicated that it is ready to transmit data.

Device Messages

These messages appear in the messages area at the bottom of the screens. All device messages are listed in alphabetical order.

Table 6-5. 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 the Management PVCs Options screen, 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 access.	Set up at least one login with Access Level-1 so the unit can be configured.
Command Complete	Configuration has been 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 has already been created so is not unique.	Enter another DLCI number.
DLCI Number Reserved	User tried to designate a special troubleshooting DLCI.	No action is needed.

Table 6-5. Device Messages (2 of 5)

Message	What It Indicates	What To Do
Duplicate DLCI Number	DLCI number entered is not unique for the frame relay link.	No action is needed; previous contents of the DLCI number field is restored.
File Transfer Complete (Seen at an FTP terminal.)	A file transfer was performed successfully.	Switch to the newly downloaded software. See *Changing Software* in Chapter 7, *FTP Operation*.
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 *Changing Software* in Chapter 7, *FTP Operation*.
Invalid Character (*x*)	A non-valid printable ASCII character has been entered.	Reenter information using valid characters.
Invalid date: must be mm/dd/yyyy	A non-valid date was entered on the System Information screen.	Reenter the date in the month/day/4-digit year format.
Invalid date and/or time	A non-valid date or time was entered on the System Information screen. The date does not exist (e.g., February 30th).	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	A non-valid system time was entered on the System Information screen.	Reenter the time in the hour:minutes:seconds format.
Invalid – Already Active	A test was already in progress when it was selected.	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	A conflicting loopback or pattern test was in progress when Start was selected to start another test, or was active on the same or another interface when Start was selected.	■ 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.

Table 6-5. Device Messages (3 of 5)

Message	What It Indicates	What To Do
Limit of six Login IDs reached	An attempt to enter a new login ID was made, and the limit of six login/password combinations has been reached.	■ Delete another login/password combination. ■ Reenter the new login ID.
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	New was selected from the PVC Connection Table and the maximum number of PVCs has already been created.	■ 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 previously.	Enter another 4-character name for the logical/management link.
No Destination Link DLCIs Available	New 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 PVC Destination.	Configure additional DLCIs for the network link and try again.
No DLCIs available for connection	New was selected from the PVC Connection Table, but all configured DLCIs have been connected.	No action needed, or configure more DLCIs and try again.
No DLCIs available for connection	New was selected from the Management PVCs option screen, but all Link/DLCI pairs have been connected.	Configure more network and/or Port-1 Links/DLCIs pairs and try again.
No DLCIs Available for Mgmt PVC	New was selected from the Management PVCs option screen, but all configured DLCIs have been connected.	Configure more network and/or Port-1 DLCIs and try again.
No DLCIs Defined	DLCI Records was selected from an interface's Configuration Edit/Display menu, and no DLCI Records have been created for this interface.	Select New and create a DLCI record.

Table 6-5. Device Messages (4 of 5)

Message	What It Indicates	What To Do
No more DLCIs allowed	New or CopyFrom was selected from an interface's DLCI Records configuration screen, and the maximum number of DLCI Records had already been reached.	Delete a DLCI, then create the new DLCI Record.
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 Login screen, and no security records had been defined.	■ 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* in Chapter 7, *FTP Operation*.
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Port Inactive	The port is disabled, or it supports synchronous data and is configured for leased line mode when a DTE Loopback was started.	No action is needed.

Table 6-5. Device Messages (5 of 5)

Message	What It Indicates	What To Do
Resetting Device, Please Wait ...	Yes (or y) was entered in the **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 when it came to saving the changes, 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 already in use 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 also provided.	■ Wait and try again. ■ Contact one of the IP address user and request that they log off.
User Interface Idle	Previously active session is now closed/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).

Status Information

Status information is useful when monitoring the FrameSaver unit. The following illustration shows the Status menu for the FrameSaver DSL unit.

Status Menu

```
main/status                                                          9783
Device Name: Node A                                   05/13/2000 06:02

                                  STATUS

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




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

NOTE:

Status messages in the following sections are in alphabetical order.

System and Test Status Messages

System and test status information is selected from the Status menu.

Main Menu → Status → System and Test Status

The following information is included on this screen:

- *Self-Test Results Messages*
- *Last System Reset Date and Time*
- *Health and Status Messages*
- *Test Status Messages*

Self-Test Results Messages

One of these self-test result messages appear in the Self-Test Results field at the top of the System and Test Status screen.

Table 6-6. 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. Contact your service representative.
Passed	No problems were found during power-on or reset.	No action needed.

Last System Reset Date and Time

This field indicates the last time the FrameSaver unit was reset. It appears after the Self-Test Results field at the top of the System and Test Status screen.

- Date is in mm/dd/yyyy format (month/day/year).
- Time is in mm:ss format (minutes:seconds).

Health and Status Messages

The following table provides Health and Status messages that apply to the FrameSaver DSL unit.

Table 6-7. Health and Status Messages (1 of 3)

Message	What It Indicates
AIS at Network 1	An Alarm Indication Signal (AIS) is received by the network interface. AIS is an unframed, all ones signal. Possible reasons include: ■ Upstream FrameSaver unit is transmitting AIS (keep-alive signal). ■ The network is transmitting an AIS.
Auto-Configuration Active	Auto-Configuration feature is active, which allows automatic configuration and cross-connection of DLCIs as they are reported by the network LMI.
Back-to-Back Mode Active	The operating mode 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.
CTS down to Port-1 Device	The user data port CTS control lead on the FrameSaver unit is off.
DLCI *nnnn* Down, *frame relay link* [1,2]	The DLCI for the specified frame relay link is down.
DTR Down from Port-1 Device	The DTR control lead from the device connected to the user data port is deasserted.
EER at Network 1	The error rate of the received network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.

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

[2] *frame relay link* is one of the following:

– Net1-FR1. The frame relay link specified for the network interface, Network 1.

– Port-1. The frame relay link associated with the user data port.

Table 6-7. Health and Status Messages (2 of 3)

Message	What It Indicates
Ethernet Link Down	The Ethernet port is enabled, but communication between the management system and the unit is not currently possible on the port.
Link Down Administratively, *frame relay link* [2]	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.
LMI Down, *frame relay link* [2]	The Local Management Interface(s) has been declared down for the specified frame relay link.
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 Transmission Convergence (TC) layer has been in an 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 communication link for the COM port is down, and the COM port is configured for Net Link.
OOF at Network 1	An Out of Frame (OOF) condition is detected on the network interface. Possible reasons include: ■ Incompatible framing format between the network and the FrameSaver unit. ■ Network cabling problem.
Primary Clock Failed	A failure of the primary clock source configured for the unit is detected and the unit's internal clock is providing the timing. This condition clears when the configured primary clock is restored.

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

[2] *frame relay link* is one of the following:

– Net1-FR1. The frame relay link specified for the network interface, Network 1.

– Port-1. The frame relay link associated with the user data port.

Table 6-7. Health and Status Messages (3 of 3)

Message	What It Indicates
SLV Timeout, DLCI *nnnn*, *frame relay link* [1, 2, 3]	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. 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 while this condition exists.
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.
Time Slot Discovery in Progress, Network 1	Time slot discovery is currently taking place to determine the time slots that will be used for frame relay traffic on the network interface. This message only appears when the Time Slot Discovery option is enabled (*Main Menu* → *Configuration* → *Time Slot Assignment* → *Frame Relay Network Assignments)* and an LMI failure is detected on the network interface's frame relay link.
Yellow at Network 1	A yellow alarm signal is received on the network interface. Possible reasons include: ■ Network cable problem. ■ T1 facility problem.

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

[2] *frame relay link* is one of the following:

– Net1-FR1. The frame relay link specified for the network interface, Network 1.

– Port-1. The frame relay link associated with the user data port.

[3] Does not apply to a TS Management Link DLCI.

Test Status Messages

These test messages appear in the right column of the System and Test Status screen. You have the option of allowing the test to continue or aborting the test. See Chapter 8, *Troubleshooting*, for more information on tests, including how to start and stop them.

Table 6-8. Test Status Messages (1 of 2)

Message	What It Indicates
DCLB Active, [Net1-FR1/Port-1]	A Data Channel V.54 Loopback (DCLB) is active on the T1 network frame relay link, or on the data for the user data port.
DTE External LB Active, Port-1	An external DTE Loopback is running on the user data port.
DTE Init. Ext LB Active, Port-1	The DTE has initiated an external DTE Loopback on the user data port.
DTPLB Active, Port-1	A Data Terminal Payload Loopback (DTPLB) is active for the specified slot and port.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the faceplate to flash on and off.
LLB Active, Network 1	A network Line Loopback (LLB) is active on the specified interface.
Monitor *Pttn* Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	The unit is monitoring a test pattern on the specified DLCI on the specified frame relay link.
Monitor *Pttn* Active, *[Interface]*	A Monitor Pattern test is active on the specified interface. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
No Test Active	No tests are currently running.
PLB Active, Network 1	A Payload Loopback (PLB) is active on the specified interface.
PVC Loopback Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	A PVC Loopback is active on the specified DLCI on the frame relay link.
RLB Active, Network 1	A network Repeater Loopback (RLB) is active on the specified interface.

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

[2] *frame relay link* is one of the following:

– Net1-FR1. The frame relay link specified for the network interface, Network 1.

– Port-1. The frame relay link associated with the user data port.

Table 6-8. Test Status Messages (2 of 2)

Message	What It Indicates
Send *Pttn* Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	The unit is monitoring the selected test pattern on the specified DLCI for the interface.
Send *Pttn* Active, *[Interface]*	A Send Pattern test is active on the specified interface. This test cannot be activated on user data ports that have Port Use set to Frame Relay.

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

[2] *frame relay link* is one of the following:

– Net1-FR1. The frame relay link specified for the network interface, Network 1.

– Port-1. The frame relay link associated with the user data port.

PVC Connection Status

PVC connection statuses are selected from the Status menu.

Main Menu → Status → PVC Connection Status

Only PVC connections with Source DLCIs configured to be Active are shown. This screen only appears when Service Type is set to Frame Relay.

PVC Connection Status Screen Example

```
main/status/connections                                              9783
Device Name: Node A                                    05/13/2000 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     0     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
 Mgmt PVC Mgm205  Net1-FR1   (0,35)         Active
 Port-1  206      Net1-FR1   1001           Active
 Port-1  207      Net1-FR1   1001           Active
 Port-1  208      Net1-FR1    500           Active
 Port-1  209      Net1-FR1    502     2     Inactive
 Port-1  210      Net1-FR1    504     2     Inactive

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

If the **`No PVC Connections`** message appears instead of a list of PVC connections, no PVC connections have been configured yet.

Table 6-9. PVC Connection Status (1 of 2)

Field	Status	What It Indicates
Link		Identifies the cross-connection of DLCIs configured for the unit.
	Net1-FR1	■ Source/destination is frame relay link 1 on Network 1
	Port-1	■ User data port – Port-1
	Mgmt PVC *Name*	■ Virtual circuit is a management link that terminates in the unit, where *Name* is the link name
DLCI	*DLCI* (16–1007) *or* (*VPI,VCI*) (0–15,31–255)	Identifies an individual link.

Table 6-9. PVC Connection Status (2 of 2)

Field	Status	What It Indicates
EDLCI	0 to 62	For multiplexed DLCIs only. Identifies an individual link/ connection embedded within a DLCI.
Status		Identifies whether the physical interfaces, LMIs, and DLCIs are all enabled and active for this PVC connection.
	Active [1]	■ The PVC is currently active.
	Inactive	■ The PVC is inactive because: – Alarm conditions and network and SLV communication status indicate that data cannot be successfully passed. – The unit has disabled the interface or frame relay link due to internal operating conventions. – Activation of an alternate virtual circuit is not warranted; that is, no alarm condition on the primary destination link has been detected.
	Disabled	■ The PVC cannot be activated and is essentially disabled as a result of how the unit was configured. Possible causes: – The physical interface at one or both ends of the PVC is/are disabled. – The frame relay link on one or both ends of the PVC is/are disabled.
	Invalid	■ Some portion of the PVC connection is not fully configured.

[1] For the circuit to be active, both Source and Destination Statuses must be Active.

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                                                    9783
Device Name: Node A                                    05/13/2000 06:04

                          NETWORK 1 INTERFACE STATUS

                   Operating Rate(Kbps):        2320
                   Receiver Attenuation(dB):    0
                   SNR Margin(dB):              15.5

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

Table 6-10. Network Interface Status

Field	Status	What It Indicates
Operating Rate	144, 192, 272, 384, 400, 528, 768, 1168, 1552, 2320	The DSL line rate.
	Disconnected	The line is disconnected.
	Auto-rating	The unit is in the process of determining the line rate.
Receiver Attenuation(dB)	–3, 0, +3, +6, +9, +12	The 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)	–64 to +63.5 dB in 0.5 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.

IP Routing Table

Use the IP Routing Table to see all the routes configured in the FrameSaver unit.

Main Menu → Status → IP Routing Table

IP Routing Table Screen Example

```
main/status/ip_rout                                                    9783
Device Name: Node A                                        05/13/2000 06:05

                                                              Page 1 of 2
                              IP ROUTING TABLE

  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       30
135.001.222.113  255.255.255.255  135.026.001.254  1    RIP     PVCMgmt1003    30
135.001.002.111  255.255.255.255  135.026.001.254  1    NMS     PVCMgmt1004     2
135.001.002.111  255.255.255.255  135.026.001.254  1    NMS     PVCMgmt1005    48
135.001.002.111  255.255.255.255  135.026.001.254  1    NMS     PVCMgmt1006    21


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

The table is sorted by the Destination IP address, from the lowest number to the highest. If no routes exist, the **No Routes** message appears instead of routing information.

Table 6-11. IP Routing Table Values

Column	What It Indicates
Destination	The Destination IP Address for the route: 001.000.000.000 – 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 appear as well. It is a reserved number.
Gateway	The Gateway IP Address for the route: 001.000.000.000 – 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. ■ 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. ■ 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 (Simple Network Management Protocol). The route remains until there is a power reset of the unit. ■ Tmp: The route was added as a temporary route in order to respond to an IP packet that was received. The route remains until its TTL expires or there is a power reset.
Interface	Specifies the interface to be used to reach the destination. ■ COM: Communications port ■ Ethernet: Ethernet port ■ PVC*name*: Name of the management PVC (e.g., PVCMgmt1001) ■ Internal: The 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, in seconds: 1 – 999

Performance Statistics

Use the Performance Statistics menu to display statistical information for a selected interface. Statistical information is useful when trying to determine 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 port. The following menu shows the performance statistics that can be selected.

Performance Statistics Menu

```
main/status/performance                                                    9783
Device Name: Node A                                          05/13/2000 06:06

                              PERFORMANCE STATISTICS


                              Service Level Verification
                              DLCI
                              Frame Relay
                              ATM
                              Ethernet
                              Clear All Statistics









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

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. True statistic counts are always maintained so SLAs can be verified, and they can be viewed from an SNMP NMS. However, since statistics can be cleared locally, the statistics viewed via the menu-driven user interface may be different from those viewed from the NMS.

▶ Procedure

To clear all statistics:

Performance Statistics → Clear All Statistics

▶ Procedure

To clear specific sets of statistics:

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

  Performance Statistics → Service Level Verification
  Performance Statistics → DLCI

- Use the ClrLinkStats function key to reset the frame relay link performance statistics.

  Performance Statistics → Frame Relay

- Use the ClrNearStats or ClrFarStats function key to reset all near-end or all far-end Extended SuperFrame (ESF) line performance statistics.

  Performance Statistics → ESF Line

Service Level Verification Performance Statistics

These statistics 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 and only if DLCIs are multiplexed. In addition, this screen only appears for units with the SLV feature set, when Service Type is set to Frame Relay.

Table 6-12. Service Level Verification Performance Statistics (1 of 2)

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.
Inbound Dropped Frames *	Total number of frames 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 4-3, 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.
* Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.	

Table 6-12. Service Level Verification Performance Statistics (2 of 2)

Statistic	What It Indicates
■ 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 4-3, 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 .
■ 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.
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. **Unknown** 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 4-3, Service Level Verification Options) over the previous 15-minute period. If SLV Packet Size is changed, a new average is not available until a new sample has been received. **Unknown** appears if communication with the far-end device over the last 15 minutes has not been successful.
Max RdTrip Latency	Same as average (Avg RdTrip Latency), but storing the maximum value of latency over the previous 15-minute interval. **Unknown** appears if communication with the far-end device over the last 15 minutes has not been successful.
* Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.	

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 (Frame Relay Delivery Ratio/Data Delivery Ratio) performance statistics are collected. If the far-end device is a non-FrameSaver device, or a FrameSaver 9120 or 9620, only frame relay statistics are collected.

DLCI Performance Statistics

These statistics appear when DLCI is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → DLCI

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

Table 6-13. DLCI Performance Statistics (1 of 2)

Statistic	What It Indicates
DLCI Up Since *	Date and time that 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 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 amount of 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 DLCI on the frame relay link.
■ Within CIR **	■ The number of frames and octets sent by the far-end device for on the selected DLCI of the frame relay link that were within the committed information rate.
■ Between CIR&EIR **	■ The number of frames and octets sent by the far-end device on the selected DLCI of the frame relay link that were between the committed information rate and excess information rate.
■ Above EIR **	■ The number of frames and octets sent by the far-end device on the selected DLCI of the frame relay link that were above the excess information rate.
■ With DE Set	■ The number of frames and octets sent on the selected DLCI of the frame relay link with the discard eligible bit set.
* Only appears for the network interface. ** Only appears for units with the SLV feature set.	

Table 6-13. DLCI Performance Statistics (2 of 2)

Statistic	What It Indicates
■ With BECN Set	■ The number of frames and octets sent on the selected DLCI of the frame relay link with backward explicit congestion notifications. BECNs are sent to notify users of data traffic congestion in the opposite direction of the frame carrying the BECN indicator.
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.
■ Within CIR **	■ The number of frames and octets received on the selected DLCI of the frame relay link that were within the committed information rate.
■ Between CIR&EIR **	■ The number of frames and octets received on the selected DLCI of the frame relay link that were between the committed information rate and excess information rate.
■ Above EIR **	■ The number of frames and octets received on the selected DLCI of the frame relay link that were above the excess information rate.
■ With DE Set	■ The number of frames and octets received on the selected DLCI of the frame relay link with the discard eligible bit set.
■ With BECN Set	■ The number of frames and octets received on the selected DLCI of the frame relay link with backward explicit congestion notifications. BECNs are sent to notify users of data traffic congestion in the opposite direction of the frame carrying the BECN indicator.
■ With FECN Set	■ The number of frames and octets received on the selected DLCI of the frame relay link with forward explicit congestion notifications. The network sends FECNs to notify users of data traffic congestion in the same direction of the frame carrying the FECN indicator.
** Only appears for units with the SLV feature set.	

Frame Relay Performance Statistics

The following statistics appear when Frame Relay is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → Frame Relay

All counts continue to increment until the maximum value is reached (2^{32}–2), then the count starts over. The NextLink and PrevLink function keys only appear when multiple frame relay links have been configured.

Table 6-14. Frame Relay Performance Statistics (1 of 2)

Statistic	What It Indicates
Frame Relay Link	
Frames Sent	The number of frames sent over the interface.
Frames Received	The number of frames received over the interface.
Characters Sent	The number of data octets (bytes) sent over the interface.
Characters Received	The number of data octets (bytes) received over the interface.
FECNs Received	The number of foreword explicit congestion notifications received over the interface. The network sends FECNs to notify users of data traffic congestion in the same direction of the frame carrying the FECN indicator.
BECNs Received	The number of backward explicit congestion notifications received over the interface. The network sends BECNs to notify users of data traffic congestion in the opposite direction of the frame carrying the BECN indicator.
Frame Relay Errors	
Total Errors	The number of total frame relay errors, excluding LMI errors. Short frames, long frames, invalid DLCIs, unknown DLCIs, and unknown errors are included in this total. Indicates that 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	The number of invalid frames received over the Network or Port-1 interface. There is a non-frame relay device on the other end of the link.
Long Rx Frames	The number of frames received over the Network or Port-1 interface that were more than 8192-octets in length. The device on the far end of the link may be configured incorrectly.

Table 6-14. Frame Relay Performance Statistics (2 of 2)

Statistic	What It Indicates
Frame Relay Errors *(cont'd)*	
Unknown Error	The number of frames received over the interface that do not fall into one of the other statistic categories. Indicates that the error is not one that the unit can recognize.
Frame Relay LMI	
LMI Protocol	The LMI protocol configured for the frame relay link. Normal condition.
Status Msg Received	The number of LMI status messages received over the interface. Normal condition.
Total LMI Errors	The number of LMI errors. Reliability errors, protocol errors, unknown report types, unknown information elements, and sequence errors are included in this total. Network problems.
Number of Inactives	The number of times the LMI has declared the frame relay link Inactive. Network problems.
Frame Relay HDLC Errors	
Rx Total Errors	The number of receiver errors on the interface. The following are included in this count: ■ 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	The number of receiver discards on the interface. The following are included in this count: ■ Resource errors ■ Rx Overruns ■ Frames received when the link was down ■ Inactive and disconnected DLCIs ■ Inactive destination DLCIs ■ Unknown EDLCIs
Rx CRC Errors	The number of received CRC (cycle redundancy check) errors.
Tx Total Errors	The total number of transmit errors on the interface, including transmits discards and transmit overruns.
Tx Total Discards	The total number of transmit discards on the interface, including underrun flushes.

ATM Performance Statistics

The following statistics appear when Frame Relay is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → ATM

All counts continue to increment until the maximum value is reached (2^{32}–2), then the count starts over.

Table 6-15. ATM Performance Statistics (1 of 2)

Statistic	What It Indicates
AAL5	
Tx PDUs	The number of ATM Adaption Layer (AAL5) Common Part Convergence Sublayer (CPCS) Protocol Data Units (PDUs) passed to the lower layer for transmission.
Rx PDUs	The number of received AAL5 CPCS PDUs passed to a higher layer.
Tx Octets	The number of AAL5 CPCS octets (bytes) passed to the lower layer for transmission.
Rx Octets	The number of received AAL5 CPCS octets (bytes) passed to a higher layer.
Errored Tx PDUs	The number of AAL5 CPCS PDUs that could not be transmitted due to errors.
Errored Rx PDUs	The number of received AAL5 CPCS PDUs that contained errors.
Discarded Tx PDUs	The number of AAL5 CPCS PDUs received for transmission that were discarded.
Discarded Rx PDUs	The number of received AAL5 CPCS PDUs discarded.
TC Sublayer	
Total Tx Cells	The number of cells transmitted.
Total Rx Cells	The number of cells received.
Total Rx Cells Dropped	The number of received cells dropped due to errors.
Rx HEC Errors	The number of cells received whose HEC fields were in error.
Unknown Rx Cells	The number of received cells discarded during cell header validation. These include: ■ Cells with unrecognized VPI/VCI values ■ Cells with invalid cell header patterns ■ Cells with 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 in this field.

Table 6-15. ATM Performance Statistics (2 of 2)

Statistic	What It Indicates
OCD Events	The number of times Out of Cell Delineation (OCD) events have been detected. An OCD event is declared when 7 consecutive cells with HEC violations are detected.
Cell Delineation State	Whether the cell last received was in synchronization. Possible values are: ■ In Sync ■ Out of Sync

Ethernet Performance Statistics

The following statistics appear when Ethernet is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → Ethernet

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

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
Device Name: Node A                                          05/13/2000 06:07
                              TRAP EVENT LOG
                                                    Total Trap Events:    4

 Time Elapsed
 Since Event    Event
   0d 23:59:59  Change in Frames Discarded due to Inbound Resource Errors on Sync
   6d 00:01:02  DLCI 101 of Sync Data Port S01P1 frame relay link “Port-1” up.
  10d 10:21:32  DLCI 101 of Sync Data Port S01P1 frame relay link “Port-1” down.
 364d 11:13:14  Unit reset.









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

Up to 12 trap events can be displayed on a screen, the most current 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 and Traps, and RMON Alarm Defaults*.

FTP Operation

7

This chapter includes the following information:

FTP File Transfers

The FrameSaver unit supports a standard File Transfer Protocol (FTP) server over Transmission Control Protocol (TCP). A complete binary image of the configuration files can be copied to a host to provide a backup. 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 a user data port 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 the user history reports regardless of 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 putting 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*).
- 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.

FrameSaver units 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.

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

NOTE:

Loading a configuration with many DLCIs from a unit's Customer Configuration 1 or 2 option area into its Current Configuration area may take 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 your 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* in Chapter 5, *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
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).
remotehelp [*command*]	Print the meaning of the command. If no argument is given, a list of all known commands is printed.
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**.
send *file1* [*file 2*]	Same as a **put**.
pwd	Print the name of the current directory of the FrameSaver unit node.
bin	Places the FTP session in binary-transfer mode.

Upgrading System Software

If you need to upgrade the FrameSaver unit's program code, you must transfer the upgrade of the **nam.ocd** file in the system memory directory using the **put** command.

NOTE:

Upgrades can be performed through the network using a Management PVC, or through the COM port if Port Use is set to Net Link (see Table 4-18, 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 *Changing Software* to activate the newly downloaded software.

Determining Whether a Download Is Completed

To see whether a download has completed, 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.

Changing Software

Once a software upgrade is downloaded, it needs to be activated. When activated, the unit resets, then executes the downloaded software. 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 select Select Software Release.

   Main Menu → *Control* → *Select Software Release*

   The currently loaded software version and the new release that was just transferred 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* 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 System Information* in Chapter 6, *Operation and Maintenance*, 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 4-14, 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 Captured Packets from the Menu-Driven User Interface* in Chapter 8, *Troubleshooting*, for additional information).

▶ 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.

3. Close the FTP session.

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

Troubleshooting

8

This chapter includes the following:

- *DTE Loopback*
- *IP Ping Test*
- *Lamp Test*

Problem Indicators

The unit provides a number of indicators to alert you to possible problems:

Indicators . . .	**See . . .**
LEDs	*Viewing LEDs and Control Leads* and *LED Descriptions* in Chapter 6, *Operation and Maintenance*, as well as the user interface screen. *Main Menu → Status → Display LEDs and Control LEDs*
Health and status	*Health and Status Messages* in Chapter 6, *Operation and Maintenance*. *Main Menu → Status → System and Test Status* Messages also appear at the bottom of any menu-driven user interface screen.
Performance statistics	*Performance Statistics* in Chapter 6, *Operation and Maintenance*, to help you determine how long a problem has existed.
Alarm conditions that will generate an SNMP trap	*Alarms* on page 8-7.
SNMP traps	Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults*. Traps supported include warm-start, authentication-failure, enterprise-specific (those specific to the unit), link-up, and link-down.

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 (see 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

Improperly configuring the unit 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* 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 and 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

A packet capture utility has been provided to aid with problem isolation when LMI errors are detected. Using this utility, any enabled frame relay link on the user data port or network interface 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.

The LMI Trace Log also provides access to captured packet information. See *Viewing Captured Packets from the Menu-Driven User Interface* 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. Select an enabled frame relay link, or Capture Interface, either Net1-FR1 or 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, *FTP Operation*, for additional information about this feature.

Viewing Captured Packets from the Menu-Driven 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:

LMI Packet Capture Utility → Display LMI Trace Log

LMI Trace Log Example

```
main/control/lmi_capture/display_log                                    9783
Device Name: Node A                                          05/13/2000 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:

- 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 seconds (s), which is reset to 1 second when this amount of time is exceeded.

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

- 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. It shows the DLCI number, its active bit status, and if Standard LMI is running, the DLCI's CIR value.

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.

Main Menu → Status → System and Test Status

Table 8-1. Alarm Conditions (1 of 4)

Alarm Condition	What It Indicates	What To Do
CTS down to Port-1 Device	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 from the user data port.
DLCI *nnnn* Down, *frame relay link* [1,2]	The DLCI for the specified frame relay link is down.	Verify that the network LMI is up. If it is, contact your network service provider.
DTR Down from Port-1 Device	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 Link Down	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.
Link Down Administratively, *frame relay link* [2]	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.	Verify that the network LMI is up. If it is, contact your network provider.

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

[2] *frame relay link* is one of the following:

– Net1-FR1. The frame relay link specified for the network interface, Network 1.

– Port-1. The frame relay link associated with the user data port.

Table 8-1. Alarm Conditions (2 of 4)

Alarm Condition	What It Indicates	What To Do
LMI Down, *frame relay link* [2]	The Local Management Interface is down for the specified frame relay link.	For the network interface: ■ If LMI was never up, verify that the LMI Protocol setting reflects the LMI type being used. ■ If LMI was never up: – Verify that the proper time slots have been configured. – Verify that the LMI Protocol setting reflects the LMI type being used. ■ Verify that Frame Relay Performance Statistics show LMI frames being transmitted. If all of the above have been verified and the physical link is not in Alarm, contact your network provider.
LMI Down, *frame relay link* [2]	The Local Management Interface is down for the specified frame relay link.	For user data port: ■ 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.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. Clears when a signal is detected. ■ Network cable problem. ■ No signal is being transmitted at the far-end FrameSaver unit.	■ Check that the network cable is securely attached at both ends. ■ Check far-end FrameSaver unit status.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network port, Network 1.
– Port-1. The frame relay link associated with the user data port.

Table 8-1. Alarm Conditions (3 of 4)

Alarm Condition	What It Indicates	What To Do
Loss of Cell Delineation, *atm link*	The ATM Transmission Convergence (TC) layer has been in an LCD state for one minute, or the number of Out of Cell Delineation (OCD) delineation events has exceeded the user-specified threshold.	Contact your network provider.
Network Com Link Down	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.
OOF at Network 1	An Out of Frame (OOF) condition is detected on the network interface. ■ Incompatible framing format between the network and the FrameSaver unit. ■ Network cabling problem.	■ Check that the framing format for the network interface is correct. ■ Check that the network cable is securely attached at both ends.
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 Timeout, DLCI *nnnn*, *frame relay link* [1,2]	An excessive number of SLV communication responses from the remote system have been missed on the specified multiplexed DLCI and link. If the frame relay link is Net1-FR1, the timeout is on the network FrameRly1 timeslot assignment. 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.

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

[2] *frame relay link* is one of the following:

– Net1-FR1. The frame relay link specified for the network interface, Network 1.

– Port-1. The frame relay link associated with the user data port.

Table 8-1. Alarm Conditions (4 of 4)

Alarm Condition	What It Indicates	What To Do
SNR Margin Threshold Exceed, Network 1	The user-specified SNR margin threshold 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.

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.

See *Trap Event Log* in Chapter 6, *Operation and Maintenance*.

Troubleshooting Tables

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

Device Problems

Table 8-2. Device Problems (1 of 2)

Symptom	Possible Cause	Solutions
No power, or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle to rear panel connection.	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 some equipment that is known to be working. ■ 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).

Table 8-2. Device Problems (2 of 2)

Symptom	Possible Cause	Solutions
Cannot access the unit or the menu-driven user interface.	Login or password is incorrect, COM port is improperly configured, or the unit is otherwise configured so it prevents access.	■ Reset the unit (see *Restoring Communication with an Improperly Configured Unit*.) ■ Contact your service representative.
Failure *xxxxxxxx* appears at the top of the System and Test Status screen, at 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.
An LED appears dysfunctional.	LED is burned out.	Run the Lamp Test. If the LED in question does not flash with the other LEDs, then contact your service representative.
Not receiving data.	Network cable loose or broken.	■ Reconnect or repair the cable. ■ Call the network service provider.
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
OCD events; loss of cell delineation.	Line impairments.	Check Hotwire GranDSLAM statistics. Reduce the link rate.
ATM statistics show VCs receiving no data.	VC improperly configured or not configured in the Hotwire GranDSLAM.	Check Hotwire GranDSLAM statistics. Configure the VC.

Frame Relay PVC Problems

Table 8-4. Frame Relay PVC Problems

Symptom	Possible Cause	Solutions
No receipt or transmission of data	Cross Connection of the DLCIs are configured incorrectly.	Verify the PVC connections and DLCIs by checking the network-discovered DLCIs on the LMI Reported DLCIs screen.
	DLCI is inactive on the frame relay network.	■ Verify that the DLCI(s) is active on the LMI Reported DLCIs screen. If the DLCI(s) is not active, contact the service provider. ■ Verify the LMI Reported DLCI field on the Interface Status screen.
	DTE is configured incorrectly.	Check the DTE's configuration.
	LMI is not configured properly for the DTE or network.	Configure LMI characteristics to match those of the DTE or network.
	LMI link is inactive.	Verify that the LMI link is active on the network; the Status Msg Received counter on the Network Frame Relay Performance Statistics screen increments.
Losing Data	Frame relay network is experiencing problems.	Run PVC Loopback and Pattern tests to isolate the problem, then contact the service provider.
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 – the physical line quality. Contact the service provider.

Tests Available

The following tests are available to a FrameSaver DSL unit.

Test Menu Example

```
main/test                                                          9783
Device Name: Node A                                  05/13/2000 08:02

                                    TEST

                            Network PVC Tests
                            Data Port PVC Tests


                            Data Port 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 menu when no PVCs have been configured on the interface. Check that both ends of the cables are properly seated and secured.

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 unit 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 abort specific tests. To abort all active tests on all interfaces, see *Aborting All Tests*.

When the status of a test is . . .	The only command available is . . .
Inactive	Start
Active	Stop

Start or stop an individual test using the same procedure.

▶ Procedure

To start and stop a loopback or a 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 Port number and press Enter.

4. 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.

5. Highlight the Start command for the test you want to start and press Enter.

   `Stop` now appears and is highlighted, and the status of the test changes to **`Active`**.

6. Press Enter to stop the test.

   `Start` reappears and the status of the test changes back to **`Inactive`**.

7. 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, with exception to DTE-initiated loopbacks. To abort individual tests that are active, see *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. The FrameSaver unit must be operating in frame relay mode.

- 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 example below shows a PVC Test screen for a FrameSaver unit with the multiplexed DLCI 550 selected. If a standard DLCI was selected, (**Disruptive**), rather than (**Non-Disruptive**), would be displayed after Test. Also, the Connectivity test would not appear.

PVC Tests Screen Example

```
main/test/network_pvc                                                    9783
Device Name: Node A                                        05/13/2000 08:03

                                NETWORK 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:

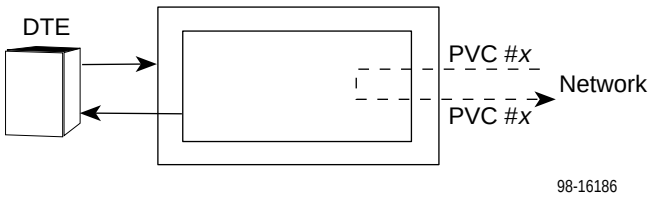
Errors encountered during these tests may be caused by mismatched CIRs in the two FrameSaver units. If errors are detected, verify the CIR configuration and retest.

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.

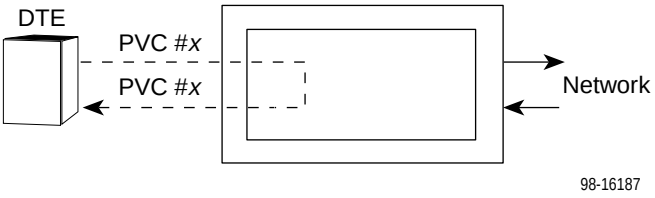
Main Menu → Test → Network PVC Tests

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

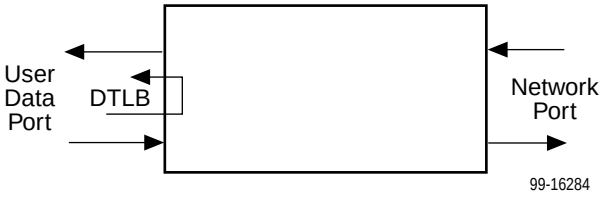
Selecting Connectivity sends a frame to the FrameSaver unit at the other end of the PVC. A **RndTrip Time(ms)** message appears in the Result column when a response is received within 5 seconds, indicating that the FrameSaver unit at the remote end is alive (operational and connected), and the round 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.

DTE Loopback

The local DTE external Loopback (DTLB) test 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.



CAUTION:

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

IP Ping Test

An IP Ping test can be run to test connectivity between 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 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 Procedure 2 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 Procedure 2 to ping the SNMP trap managers.

▶ Procedure 1

To ping any far-end FrameSaver unit:

1. Select the IP Ping test.

   Main Menu → *Test* → *IP Ping*

2. Enter the IP Address of the device the Ping is being sent to, then select Start.

   NOTE:

   If the FrameSaver unit has just initialized, 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.

   If accessing the unit remotely to enter or change frame relay parameters, send the Ping five times in a row, in rapid succession; the unit will be operating in frame relay mode.

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. Latency = `*`nn`*` ms`** should appear as the Status (*nn* being the amount of time the test took in milliseconds).

   If any other message is displayed, additional testing will be required.

▶ Procedure 2

To ping the NMS at the central site:

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, as when using the Auto-Configuration feature.
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. Latency = `*`nn`*** **`ms`** should appear as the Status (*nn* being the amount of time the test took in milliseconds).

   If any other message is displayed, additional testing will be required.

Lamp Test

The FrameSaver unit 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* for additional information.

Setting Up OpenLane for FrameSaver Devices

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 SLV 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 SLV feature set activated
- Automatic device and PVC discovery for SLV devices with their SLV Delivery Ratio configuration option enabled
- Easy firmware downloads to an entire network or parts of the network
- Remote SLV feature activation

- Device reset capability
- HP OpenView adapters for integrating OpenLane with the OpenView Web interface

The advanced SLV feature set may be activated, depending upon the model ordered; or, it can be activated when SLV functionality is needed using the OpenLane SLM system.

To activate SLV functionality at a later time, order an Activation Certificate (Feature No. 9783-C1-220).

Setting Up the OpenLane SLM System

Instructions for installing the OpenLane SLM system are found in the following documents:

- *OpenLane 5.x Service Level Management for UNIX Quick Start Installation Instructions*
- *OpenLane 5.x Service Level Management for Windows NT Quick Start Installation Instructions*

See *Product-Related Documents* in *About This Guide* for document numbers. Select the appropriate document.

In addition to installation instructions, these documents include instructions for:

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

The OpenLane SLM system has an extensive Help system. For additional information refer to the following sources:

- **For UNIX users** – Refer to the readme.txt file for distributed infrastructure details, and the online Help for operational details.
- **For Windows NT users** – Refer to the online Help.

Setting Up FrameSaver and SLV Support

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

▶ Procedure

To set up FrameSaver and SLV support:

1. Start the OpenLane services, then access the application.
2. Enter a Customer ID of **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 units with the SLV feature set activated.

See the Quick Start Installation Instructions to learn how to perform these steps and for additional information.

Setting Up Network Health for FrameSaver Devices

10

FrameSaver units are compatible with Concord Communication's Network Health software.

For FrameSaver units with the SLV and SLM reporting 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 FrameSaver SLV report example on page 10-10). To get 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:

- *Installation and Setup of Network Health* and reports
- *Discovering FrameSaver Elements*
- *Configuring the Discovered Elements*
- *Grouping Elements for Reports*
- *Generating Reports for a Group*
  - *About Service Level Reports*
  - *About At-a-Glance Reports*
  - *About Trend Reports*
  - *Printed Reports*
- *Reports Applicable to FrameSaver SLV Devices*

For additional information about installing, accessing, and managing FrameSaver DSL devices through Concord's Network Health, and for information about applicable reports, refer to:

- *Network Health Installation Guide* to help you install the application.
- *Network Health User Guide* to help you get started using the application.
- *Network Health Reports Guide* to help you understand and use Frame Relay reports.
- *Network Health – Traffic Accountant Reports Guide* to help you understand and use Traffic Accountant reports.

Installation and Setup of Network Health

Refer to the *Network Health Installation Guide* for installation instructions, and follow the instructions applicable to your network platform. Once Network Health is installed, you need to set up the application so it will support FrameSaver units.

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 units and collect data.

To use this application:

1. Discover network elements, units, and interfaces in the network.
2. Configure the Network Health applications, then 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 units in your network and discover their DLCIs. Saving the results of the search creates definitions in the Poller Configuration, which are used to poll the units.

IP addresses and the Community String for the FrameSaver units must be entered for Network Health to find the FrameSaver units 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 elements 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 find 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 units to be located, and the Community String (Community Name in the FrameSaver unit). 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 units 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.

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 unit for the first time. For a FrameSaver DSL unit, the speed set would be the unit's CIR. No additional configuration should be required. However, you should verify that all appropriate information has been retrieved.

NOTE:

If a FrameSaver unit 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.

Additional information that can be edited, as well. See *Discovering Elements* in the *Network Health User Guide* for additional information.

▶ Procedure

To change the CIR for FrameSaver DSL 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 CIR for the unit in the text box.

   Letters **k** and **m** can be used as shortcuts (e.g., enter 56 k for 56 kilobits per second, or 16 m for 16 Mbits per second).

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 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 units 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 all 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. That chapter also tells you how to customize 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 on page 10-10, 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 SLV Devices

The following frame relay reports support FrameSaver units:

- **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.

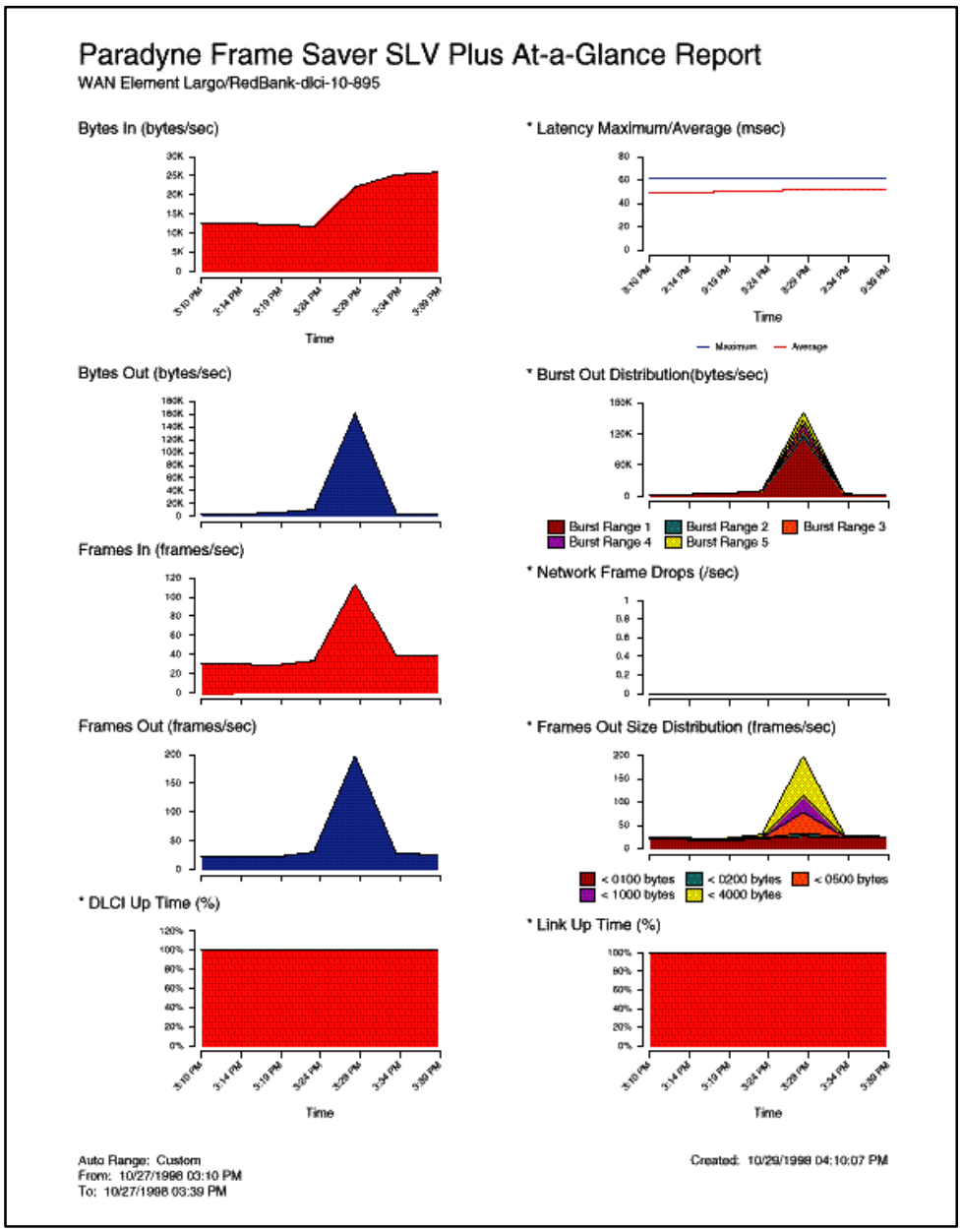
  - — **Customer Service Level Report** – Provides service level information for customers. This report is used to provide service level information to service customers to help them determine optimum service levels needed based upon their own traffic data, as well as provide documented evidence for increasing 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 SLV unit'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.

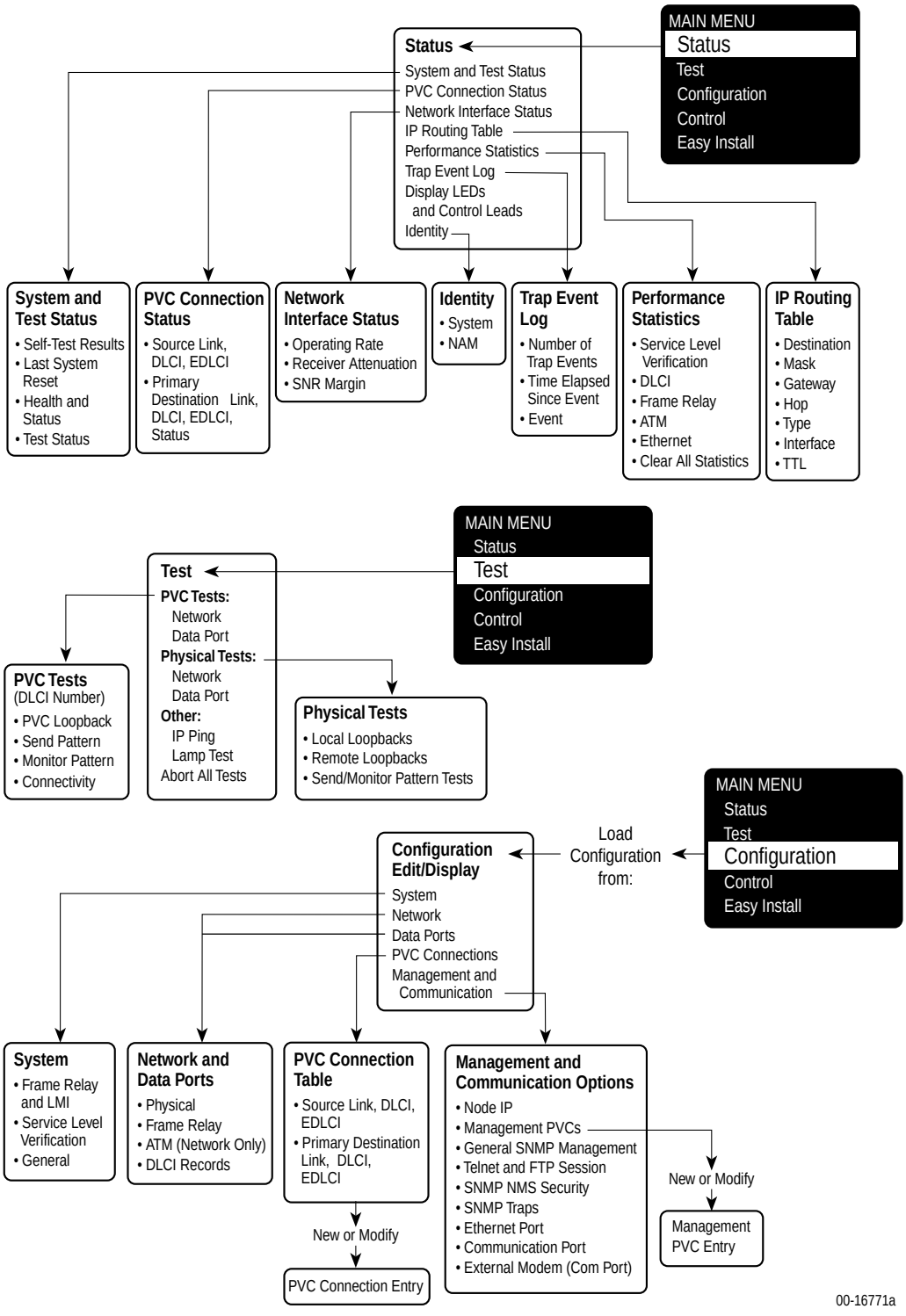
Menu Hierarchy

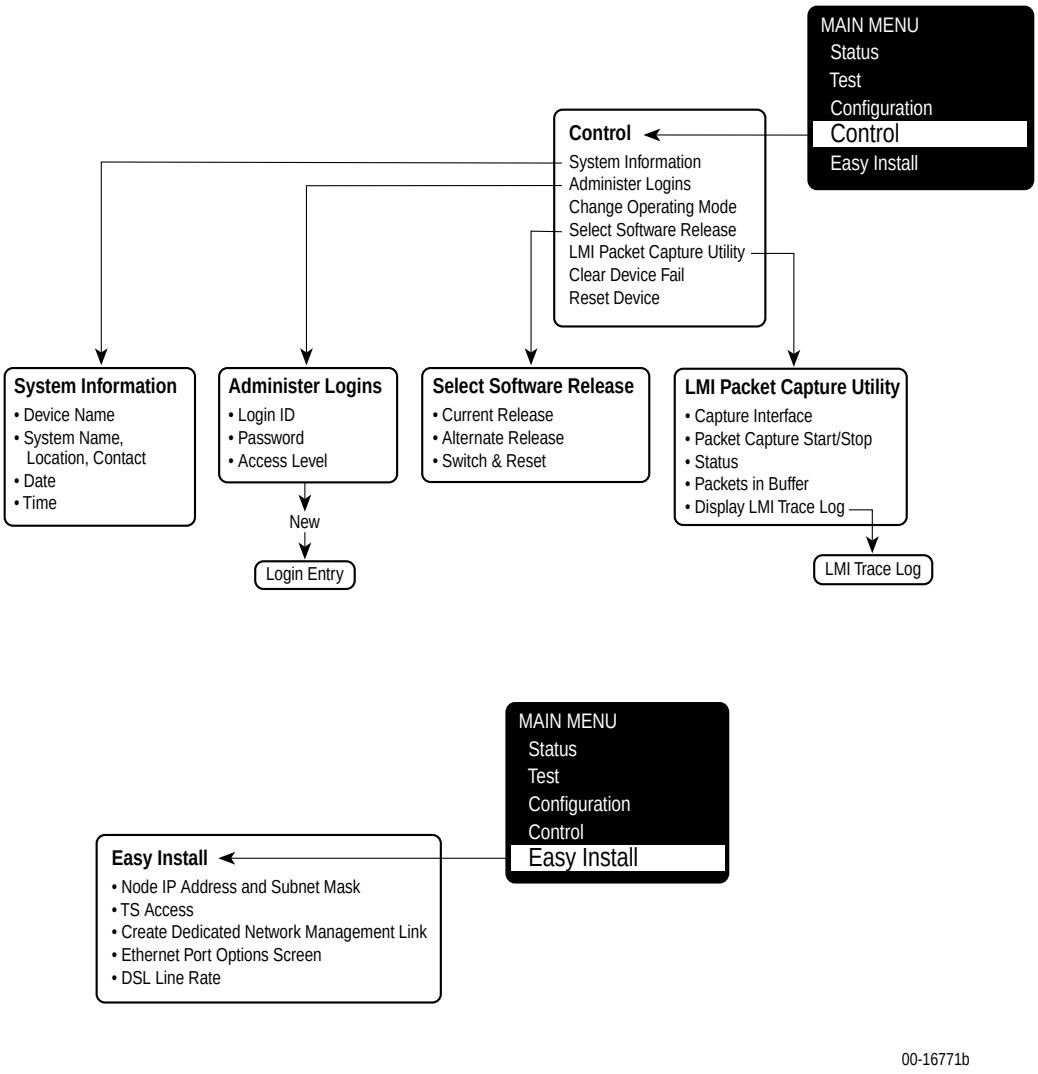
A

Menus

The following menus are a graphical representation of the FrameSaver DSL unit's menu organization.

Menu Hierarchy – Frame Relay Mode





00-16771b

SNMP MIBs and 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)
- Enterprise MIB
- 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.

▶ Procedure

To access Paradyne MIBs:

1. Access the Paradyne World Wide Web site at **www.paradyne.com**.
2. Select Technical Support.
3. Select Management Information Base (MIBs).

The download procedure may vary depending upon your browser or NMS application software. Refer to your browser or NMS manual 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 unit, which is an SNMPv1 MIB.

FrameSaver Unit's sysDescr (system 1)

The following is the system description (sysDescr [system 1]) for the NMS subsystem in the FrameSaver DSL unit:

PARADYNE DSL FrameSaver Flex; Model: *9783*; S/W Release: *(MM.mm.bb [MM=Major.mm=minor.bb=build] format)*; NAM CCA number: *(hardware version in hhhh-hhh format)*; Serial number: *sssssss*

FrameSaver Unit's sysObjectID (system 2)

The following is the system object identifier (sysObjectID [system 2]), or OID, for the NMS subsystem in the FrameSaver DSL unit:

1.3.6.1.4.1.1795.1.14.2.4.9.1.1 for the basic feature set, or
1.3.6.1.4.1.1795.1.14.2.4.9.1.2 for the advanced SLV feature set.

NOTE:

The sysObjectID is 1.3.6.1.4.1.1795.1.14.2.4.9.1.1 (basic) until the advanced SLV feature set is activated using 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)

The following table 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 the 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*	

NetScout Indexes to the Interface Table (ifTable)

For remote monitoring at sites where FrameSaver units are operating with NetScout Probes, use the following ifName, ifDescr, and ifIndex.

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 – 100000000

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:

- warmStart
- authenticationFailure
- linkUp and linkDown
- enterprise-Specific
- 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 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 lost of approved managers. *String:* 'Unauthorized access attempted.'
	Variable-Binding	
	devLastTrapString (devHealthAndStatus.mib)	

Traps: linkUp and linkDown

These traps are supported on the following interfaces:

- Physical sublayer interfaces: network, Ethernet, and synchronous data ports
- Frame relay logical link layer interfaces

Table B-5. linkUp and linkDown Traps

Trap	What It Indicates	Possible Cause
linkDown	A failure in one of the communication interfaces has occurred.	A failure in one of the communication interfaces has occurred.
linkUp	One of the failed communication interfaces is up and operational.	One of the failed communication interfaces is up and operational.

Their linkUp and linkDown variable-bindings are in Table B-6.

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) – Loss of Frame (LOF) – Loss of Link (LOL) – Loss of Signal Quality – LPR Events *Sample strings:* 'Network DSL down due to LOS, LOF, and LOL.' 'Network DSL down due to Loss of Signal Quality.' ■ linkUp – No alarms on the interface. *String:* '$ifString up.'
Synchronous Data Port (Supported by the media-specific RS232-like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the port. Alarm conditions include: – DTR off [1] – RTS off [2] – '' – Not DTR or RTS, but link is down. *String:* '$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.'

[1] The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state.

[2] The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state.

Table B-6. linkUp and linkDown Variable-Bindings (2 of 3)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer *(cont'd)*		
Ethernet Port	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – Communication is not possible over the Ethernet port. *Strings:* '$ifString down.' '$ifString administratively shut down.' (Due to an intentional shutdown.) ■ linkUp – Communication on the port is restored. *String:* '$ifString up.'
Logical Link Sublayer		
Synchronous Data Port Service Side of the Frame Relay UNI (Supported by the media-specific Frame Relay Services MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured,[3] or Frame Relay link is disabled. '$ifString LMI down.' No alarms exist on the link. (e.g., 'Sync Data Port S01P1 frame relay link "Port-1" LMI down.') '$ifString administratively shut down.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$ifString up.'
Network DTE Side of the Frame Relay UNI (Supported by the media-specific Frame Relay DTE's MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured,[3] or Frame Relay link is disabled. *Strings:* '$ifString LMI down.' '$ifString administratively shut down.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$ifString up.'

[3] If the LMI Protocol is not configured, a linkUp/linkDown trap is based solely upon whether the interface is enabled or disabled.

Table B-6. linkUp and linkDown Variable-Bindings (3 of 3)

Interface	Variable-Bindings	Possible Cause
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. Alarm condition: _ Loss of Cell Delineation *String:* '$ifString down.' (The physical link is down.) '$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.'

Traps: enterprise-Specific

These traps indicate that an enterprise-specific event has occurred. Supported enterprise-specific traps are listed 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 $CIR bps.'
enterpriseConfig-Change(6)	■ devLastTrapString (devHealthAndStatus.-mib)	Configuration has been changed via the menu-driven user interface, an SNMP Manager, or auto-configuration after 60 seconds has elapsed without another change. *String:* 'Device configuration change.'
enterpriseDLCI-delete(17)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib.)	The DLCI has been deleted. The network no longer supports the DLCI, and it was removed. *Strings:* '$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.)
enterpriseDLCIUp(12)		DLCI Status is set to Active; DLCI is up again. *String:* '$ifString up.'

Table B-7. enterprise-Specific Traps and Variable-Bindings (2 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseMissedSLV-Down(16)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciMissed-SLVs (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.'
enterpriseMissedSLV-Up(116)		SLV Timeout Error Event has been cleared. *String:* 'SLV up on $ifString because SLV communication was reestablished. Total SLV packets lost is $numLost.'
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 For virtual circuits (DLCIs): ■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib	At least one test has been started on an interface or virtual circuit. *String:* '$testString test started on $ifString.' (e.g., 'DTE Loopback test started on Sync Data Port S01P1.')
enterpriseTest-Stop(105)		All tests have been halted on an interface or virtual circuit. *String:* '$testString test stopped on $ifString.' (e.g., 'Disruptive PVC Loopback test stopped on DLCI 100 of Sync Data Port S01P1 frame relay.')
enterpriseLinkSpeed Change(14)	■ ifIndex (RFC 1573) ■ ifSpeed (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib	The link speed has changed. *String:* 'Speed on $ifName changed to $ifSpeed bps.'

Traps: RMON-Specific

Two traps are defined to support the Alarm and Events Groups of RMON. See *RMON Alarm and Event Defaults* 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 alarm Falling 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 $alarmFallingThreshold by $(alarmValue – AlarmFallingThreshold.'

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. When the threshold set for the monitored variable is exceeded, an SNMP trap or a log event is sent.

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 alarm default tables starting on the next page show how each RMON default alarm is set by the FrameSaver unit, shows the alarm and event types, the interval used when generating alarms, and thresholds.

- *Physical Interface Alarm Defaults*
- *Frame Relay Link Alarm Defaults*
- *DLCI Alarm Defaults – Paradyne Area*
- *DLCI Alarm Defaults – NetScout Area*

See *Standards Compliance for SNMP Traps* for information about how traps work, and *Traps: RMON-Specific* 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.

Physical Interface Alarm Defaults

This alarm only applies to the FrameSaver DSL unit's network interface.

Table B-9. Network Physical Interface Alarm Defaults

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Unavailable Seconds	D	*MIB:* pdn_FrExt.mib (E) *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. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID of 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	Rising Threshold Default	Falling Threshold Default
Invalid Frames	D	*MIB:* pdn_FrExt.mib (E) *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 (E) *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 (E) *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 (E) *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
Tx Discards	D	*MIB:* pdn_FrExt.mib (E) *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 (E) *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

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID of 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	Rising Threshold Default	Falling Threshold Default
Tx Total Errors	D	*MIB:* pdn_FrExt.mib (E) *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 (E) *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 (E) *Tag:* devFrExtLinkTx-Underruns *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 (E) *Tag:* devFrExtLinkRx-NonOctet *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 (E) *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 (E) *Tag:* devFrExtLinkTotal-LMIErrs *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. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.

DLCI Alarm Defaults – Paradyne Area

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 put into the Paradyne alarm area.

Table B-11. DLCI Alarm Defaults – Paradyne Area (1 of 3)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Average Latency	A	*MIB:* pdn_FrExt.mib (E) *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 (E) *Tag:* devFrExtDlciSts-CongestedSecs *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 (E) *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 (E) *Tag:* devFrExtDlciStsInactive-Secs *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 (E) *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:* FR 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

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute. Indicates that the exact value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.
D = DLCI number.

Table B-11. DLCI Alarm Defaults – Paradyne Area (2 of 3)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Frames Sent	D	*MIB:* FR 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
Missing Latency Responses	D	*MIB:* pdn_FrExt.mib (E) *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:* FR 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:* FR 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:* FR 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:* FR 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:* FR 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

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute. Indicates that the exact value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.
D = DLCI number.

Table B-11. DLCI Alarm Defaults – Paradyne Area (3 of 3)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Tx Frames Exceeding CIR	D	*MIB:* pdn_FrExt.mib (E) *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

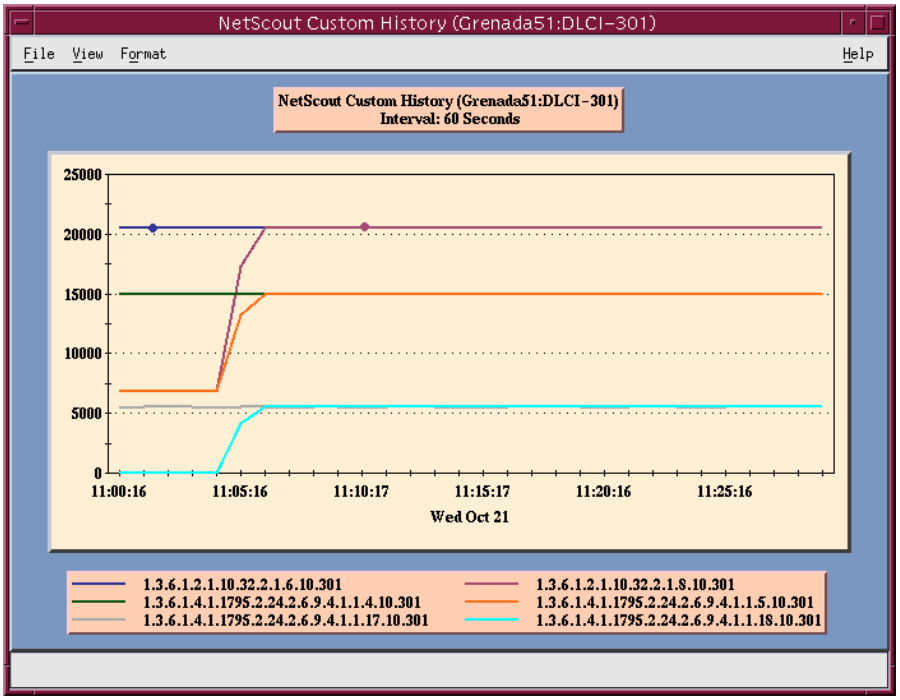
[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute. Indicates that the exact value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.
D = DLCI number.

Object ID Cross-References (Numeric Order)

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.

This table is helpful in identifying alarm conditions being tracked when viewing the NetScout Custom History screen (shown below), which provides the OID instead of the alarm condition.



See Table B-14 for an RMON history OID cross-reference and Table B-15 for an RMON alarm OID cross-reference.

Table B-14. History OID Cross-Reference (1 of 5)

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**	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.**16.I**	All DLCI + LMI Tx Octets	*MIB:* MIB II (RFC 1573) *Tag:* ifOutOctets
.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:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.**5.I**.**D**	Rx BECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.**6.I**.**D**	Tx Frames	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.**7.I**.**D**	Tx Octets	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**8.I**.**D**	Rx Frames	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.**9.I**.**D**	Rx Octets	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets
.1.3.6.1.4.1.1795.2.24.2. . .		
.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 (E) *Tag:* devFrExtLinkRxNonOctet

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-14. History OID Cross-Reference (2 of 5)

Object ID (OID) [1]	Item	MIB/Tag
.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**.1.1.3.I.D**	DLCI CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciFrCIR
.1.3.6.1.4.1.1795.2.24.2.6.9. 4**.1.1.7.I .D**	Tx DEs	*MIB:* pdn_FrExt.mib (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *Tag:*devFrExtDlciDropFrCirToEir

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-14. History OID Cross-Reference (3 of 5)

Object ID (OID) [1]	Item	MIB/Tag
.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.**1.1.57.I** .**D**	Network Frames Dropped Above CIR Within EIR	*MIB:* pdn_FrExt.mib (E) *Tag*:devFrExtDlciRxFrNetDrop-CirToEir
.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 (E) *Tag*:devFrExtDlciOfferedFrOverEir
.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 (E) *Tag*:devFrExtDlciRxFrNetDrop-OverEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.63.I** .**D**	DLCI EIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2**.**1.2.I**.**D**	Inactive Seconds	*MIB:* pdn_FrExt.mib (E) *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 (E) *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 (E) *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 (E) *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**.**N**	Frame Size Upper Limit (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtFrameSzUpLimit
.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 (E) *Tag:* devFrExtFrameSzCount

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-14. History OID Cross-Reference (4 of 5)

Object ID (OID) [1]	Item	MIB/Tag
.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 (E) *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 (E) *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 (E) *Tag:* devFrExtBurstFrames
.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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *Tag:* devFrExtLinkRxDiscards
.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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *Tag:* devFrExtLinkTotLMIErrs

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-14. History OID Cross-Reference (5 of 5)

Object ID (OID) [1]	Item	MIB/Tag
.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 (E) *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 (E) *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 (E) *Tag:* devFrExtLinkUtilTxOctets

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

See Table B-15 for an RMON alarm OID cross-reference.

Table B-15. Alarm OID Cross-Reference (1 of 2)

Object ID (OID)	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:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.**5.I.D**	Rx BECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.**6.I.D**	Frames Sent	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx CIR Utilization	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx DLCI Link Utilization	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**8.I.D**	Frames Received	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.**9.I.D**	Rx DLCI Link Utilization	*MIB:* FR 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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *Tag:* devFrExtLatencyAvg

Table B-15. Alarm OID Cross-Reference (2 of 2)

Object ID (OID)	Item	MIB/Tag
.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.**3.1.7.I.D**	Current Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyLatest
.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 (E) *Tag:* devFrExtFrameSzUpLimit
.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 (E) *Tag:* devFrExtFrameSzCount
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.6.I**	Rx Short Frames	*MIB:* pdn_FrExt.mib (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *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 (E) *Tag:* devFrExtLinkTotalLMIErrs

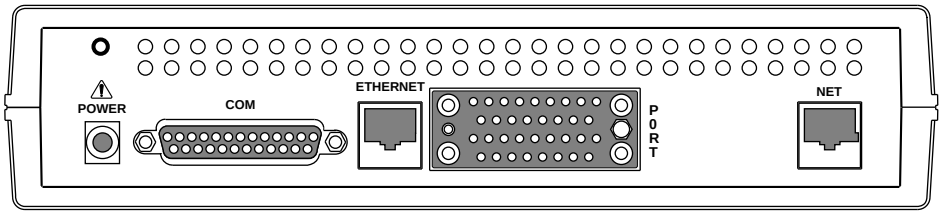
Connectors, Cables, and Pin Assignments

C

This appendix shows the FrameSaver unit's rear panel, and the pin assignments for the connectors/interfaces and cables.

Rear Panel

The following illustration shows the FrameSaver DSL unit's rear panel.



00-16690

The sections that follow provide pin assignments for each interface.

NOTE:

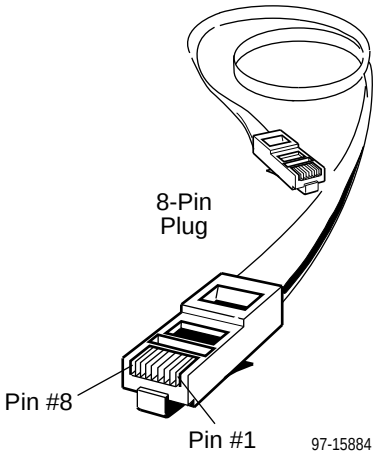
In the pin assignment tables of this appendix, if the pin number is not shown, it is not being used.

DSL Network Interface Cable

The DSL network interface connector is an RJ48C 8-position keyed modular jack.

Table J-1. DSL Network Interface Connector

Pin Number	Signal
1	(Unused)
2	(Unused)
4	Ring
5	Tip



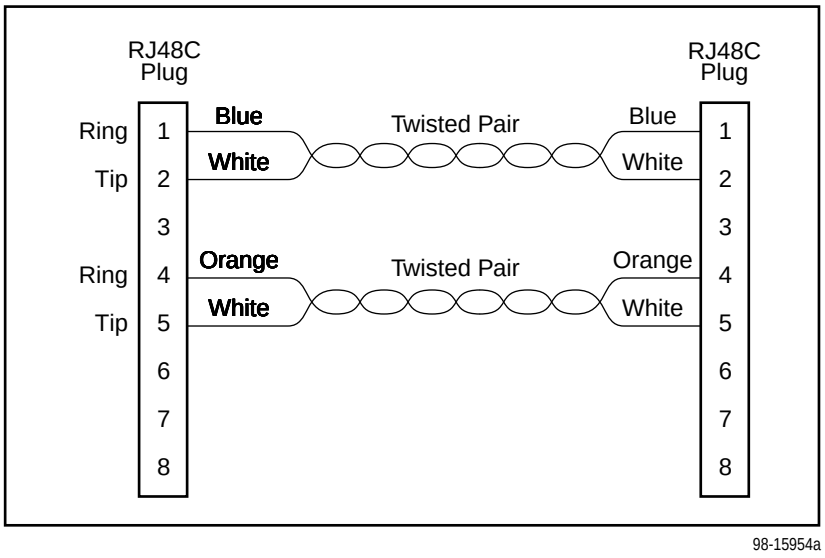


Figure C-1. DSL Network Interface Cable with RJ48C Connector)

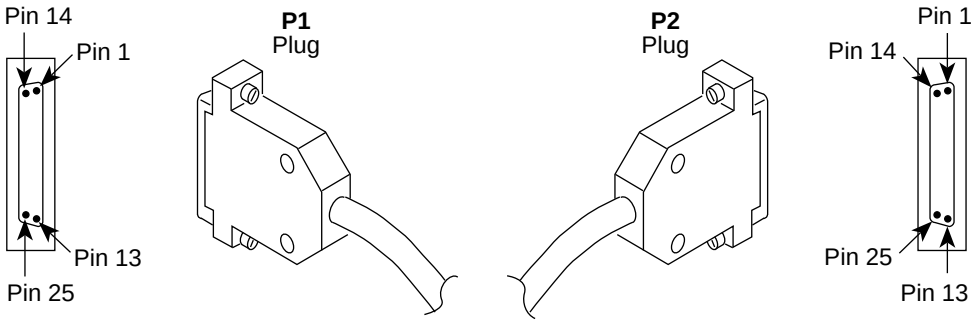
COM Port Connector

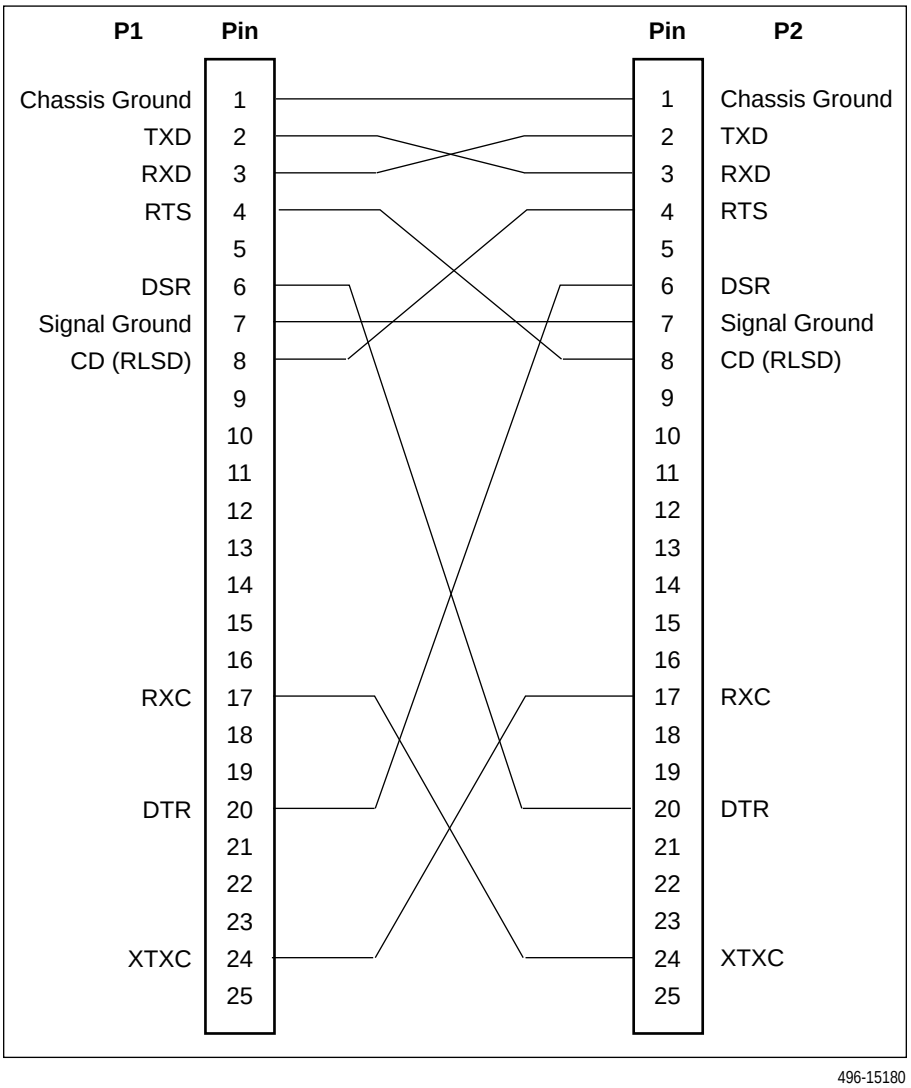
The following table provides the pin assignments for the FrameSaver unit's 25-position EIA-232C communication port connector.

Signal	Direction	Pin #
Shield (GND)	—	1
DCE Transmit Data (TXD)	From DTE (In)	2
DCE Receive Data (RXD)	To DTE (Out)	3
DCE Request To Send (RTS)	From DTE (In)	4
DCE Clear To Send (CTS)	To DTE (Out)	5 *
DCE Data Set Ready (DSR)	From DTE (In)	6 *
Signal Ground (GND)	—	7
DCE Carrier Detect (CD)	To DTE (Out)	8 *
DCE Data Terminal Ready (DTR)	From DTE (In)	20
* Pins 5, 6, and 8 are tied together.		

Standard EIA-232-D Crossover Cable

A standard crossover cable can be used to connect the COM port to an external modem. The external modem must be configured so it is compatible with the FrameSaver unit. See page C-5 to configure an external modem.





496-15180

▶ Procedure

To configure an external modem:

1. Disconnect the asynchronous terminal from the standard cable. See page C-4 for an illustration of the COM Port connection.
2. Reconnect the crossover cable to the external modem.
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

AT Command String	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.

Data Port Connector

The following table provides the pin assignments for the 34-position V.35 connector to the DTE.

Signal	ITU CT#	Direction	34-Pin Socket
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.

Ethernet Port Connector

The following table provides the pin assignments for the FrameSaver unit's 8-position RJ45 Ethernet port unkeyed modular jack.

Signal	Direction	Pin #
10/100BaseT Transmit Data (TD +)	To LAN Interface (Out)	1
10/100BaseT Transmit Data (TD –)	To LAN Interface (Out)	2
10/100BaseT Receive Data (RD +)	From LAN Interface (In)	3
10/100BaseT Receive Data (RD –)	From LAN Interface (In)	6

Technical Specifications

D

Table D-1. FrameSaver DSL Technical Specifications (1 of 2)

Specification	Criteria
Approvals	
FCC Part 15	Class A digital device
Safety	Refer to the equipment's label for safety information.
Physical Environment	
Operating temperature	32°F to 122°F (0°C to 50°C)
Storage temperature	–4°F to 158°F (–20°C to 70°C)
Relative humidity	5% to 85% (noncondensing)
Shock and vibration	Withstands normal shipping and handling
Power Consumption and Dissipation	4.5 watts, 60 Hz ±3, 0.135 A at 120 Vac±12 Result: 15.4 Btu per hour
Physical Dimensions	
Height (with feet) Height (without feet)	2.1 inches (5.3 cm) 2.0 inches (5.1 cm)
Width	6.2 inches (15.7 cm)
Depth	8.7 inches (22.1 cm)
Weight	1.38 lbs (0.62 kg)

Table D-1. FrameSaver DSL Technical Specifications (2 of 2)

Specification	Criteria
COM Port	25-position (DB25) connector
Standard	EIA-232, 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	8-position modular unkeyed USOC RJ48C jack
Line Code	2B1Q
Service	SDSL
Data rates	144-2320 kbps
Ethernet Port	8-position modular unkeyed USOC RJ45 jack
Standard	ANSI/IEEE Standard 802.3, Ethernet Version 2
Data rates	10/100 BaseT (auto-sensing 10 and 100 Mbps Ethernet rates)
Data Port	34-position V.35 connector
Standard	V.35/ITU (ISO 2593)
Data rates	Automatically set to the network rate.

Equipment List

E

Equipment

See page E-2 for cables you can order.

Description	Model/Feature Number
FrameSaver DSL Units	
FrameSaver DSL unit with 8 PVCs and Basic Feature Set. *Includes 1-Slot Housing, 120 Vac Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-211
FrameSaver DSL unit with 8 PVCs and Basic and Advanced SLV Feature Sets. *Includes 1-Slot Housing, 120 Vac Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-221
FrameSaver DSL unit with 64 PVCs and Basic Feature Set. *Includes 1-Slot Housing, 120 Vac Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-213
FrameSaver DSL unit with 64 PVCs and Basic and Advanced SLV Feature Sets. *Includes 1-Slot Housing, 120 Vac Power Supply, Network Cable, Installation Instructions, and Quick Reference.*	9783-A1-223
FrameSaver SLV Upgrade	
FrameSaver DSL SLV Activation Certificate	9783-C1-220
User Manual	
FrameSaver DSL 9783 User's Guide (Paper Manual)	9783-A2-GB20

Description	Model/Feature 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 Features	
Wall Mounting Kit for 1-Slot Housing	9001-F1-891
Shelf Mounting Kit for 1-Slot Housings	9001-F1-894

Cables

This table lists cables you can order.

Description	Part Number	Feature Number
RJ48C DSL Network Cable, RJ48C-to-RJ48C/RJ49C (20 feet – 6.1 meters) – *For use in the U.S.*	035-0209-2031	3100-F1-500
Standard EIA-232 Straight-Through Cable, DB25-to-RJ48 (14 feet – 4.3 meters) – *For connection to an asynchronous terminal or PC with an 8-pin modular interface.*	035-0314-1431	3100-F2-540
Standard EIA-232 Straight-Through Cable, DB25-to-D-Sub9 (14 feet – 4.3 meters) – *For connection to a PC with a D-Sub9 interface.*	035-0313-1431	3100-F2-550
V.35 DTE Adapter, EIA-530A-to-V.35 – *For connection to equipment with V.35, MS34 connectors.*	035-0244-0031	3100-F1-570
Standard EIA-232-D Crossover Cable (14 feet – 4.3 meters) – *For connection to an external device.*	035-0336-1431	9008-F1-550

Index

Numbers

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W