FrameSaver® SLV

MODELS 9820, 9820-2M, 9820-8M, and 9820-45M

USER'S GUIDE

Document No. 9820-A2-GB20-20

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

Contents

About This Guide

- Purpose and Intended Audience ix
- Document Organization ix
- Product-Related Documents xi
- Conventions Used xii

1 About FrameSaver SLV In-Line Monitors

- SLM Overview 1-1
- FrameSaver SLV In-Line Monitor Features 1-3

2 User Interface and Basic Operation

- Logging On 2-2
- Main Menu 2-4
- Screen Work Areas 2-5
- Navigating the Screens 2-6
  - Keyboard Keys 2-6
  - Function Keys 2-7
  - Selecting from a Menu 2-8
  - Switching Between Screen Areas 2-8
  - Selecting a Field 2-9
  - Entering Information 2-9

3 Configuration Procedures

- Basic Configuration 3-2
  - Configuration Option Areas 3-3
  - Accessing and Displaying Configuration Options 3-4
  - Changing Configuration Options 3-5
  - Saving Configuration Options 3-6
  - Minimal Configuration Before Deploying Remote Units 3-6

4 Configuration Options

- Configuring Using the Easy Install Screen (Model 9820-45M) 4-3
- Entering System Information and Setting the System Clock 4-4
- Setting Up for Trap Dial-Out (Models 9820, 9820-2M, 9820-8M) 4-5
  - Setting Up an External Modem for Trap Dial-Out 4-5
  - Setting Up Call Directories for Trap Dial-Out 4-5
- Setting Up Auto-Configuration 4-6
  - Selecting a Frame Relay Discovery Mode 4-7
  - Automatically Removing a Circuit 4-9
- Setting Up Management 4-10
  - Setting Up Local Management at the Central Site 4-10
  - Setting Up So the Router Can Receive RIP 4-11
  - Setting Up Service Provider Connectivity at the Central Site 4-11
- Setting Up Back-to-Back Operation 4-12
  - Changing Operating Mode 4-12
- Configuration Option Tables 4-13
- Configuring the Overall System 4-13
  - Configuring Frame Relay and LMI for the System 4-14
  - Configuring Service Level Verification Options 4-16
  - Configuring General System Options 4-18
- Configuring the Physical Interfaces 4-19
  - Configuring the Network Data Port 4-19
  - Configuring the User Data Port 4-21
- Configuring Frame Relay for an Interface 4-23
- Manually Configuring DLCI Records 4-26
- Configuring PVC Connections 4-29
- Setting Up Management and Communication Options 4-32
  - Configuring Node IP Information 4-32
  - Configuring Management PVCs 4-36
  - Configuring General SNMP Management 4-40
  - Configuring Telnet and/or FTP Session Support 4-41
  - Configuring SNMP NMS Security 4-44
  - Configuring SNMP Traps and Trap Dial-Out 4-45
  - Configuring the Ethernet Port (Model 9820-45M) 4-50
  - Configuring the Communication Port 4-52
  - Configuring the COM Port to Support an External Modem (Models 9820, 9820-2M, 9820-8M) 4-57
  - Configuring the Modem Port (Model 9820-45M) 4-59

5 Security and Logins

- Limiting Access 5-2
- Controlling Asynchronous Terminal Access 5-3
- Controlling External COM Port Device Access (Models 9820, 9820-2M, 9820-8M) 5-4
- Controlling Modem Port Device Access (Model 9820-45M) 5-4
- Controlling Telnet or FTP Access 5-5
  - Limiting Telnet Access 5-5
  - Limiting FTP Access 5-6
  - Limiting Telnet or FTP Access Over the TS Management Link 5-7
- Controlling SNMP Access 5-8
  - Disabling SNMP Access 5-8
  - Assigning SNMP Community Names and Access Levels 5-9
  - Limiting SNMP Access Through IP Addresses 5-10
- Creating a Login 5-11
- Modifying a Login 5-12
- Deleting a Login 5-12

6 Monitoring

- Displaying System Information 6-2
- Front Panel LEDs 6-3
  - Front Panel Status LEDs 6-4
- Displaying LEDs and Control Leads 6-6
  - Display LEDs and Control Leads Screen (Models 9820, 9820-2M, 9820-8M) 6-6
  - Display LEDs and Control Leads Screen (Model 9820-45M) 6-8
- Power Module LEDs (Model 9820-45M) 6-10
- Device Messages 6-11
- Status Information 6-16
- System and Test Status Messages 6-17
- Network LMI-Reported DLCIs Status 6-21
- PVC Connection Status 6-23
- Network Interface Status 6-25
- IP Routing Table (Model 9820-45M) 6-26
- Performance Statistics 6-28
  - Clearing Performance Statistics 6-29
  - Service Level Verification Performance Statistics 6-30
  - DLCI Performance Statistics 6-32
  - Frame Relay Performance Statistics 6-34
  - Ethernet Performance Statistics (Model 9820-45M) 6-37
- Trap Event Log (Model 9820-45M) 6-38

7 FTP Operation

- FTP File Transfer 7-2
  - Upgrading System Software 7-4
  - Determining Whether a Download Is Completed 7-5
  - Changing Software 7-5
  - Transferring Collected Data 7-6

8 Troubleshooting

- Problem Indicators 8-2
- Resetting the Unit and Restoring Communication 8-3
  - Resetting the Unit from the Control Menu 8-3
  - Resetting the Unit By Cycling the Power 8-3
  - Restoring Communication with an Improperly Configured Unit 8-4
- Troubleshooting Management Link Feature 8-5
- LMI Packet Capture Utility Feature 8-5
  - Viewing Captured Packets from the Menu-Driven User Interface . . . 8-6
- Alarms 8-7
- Troubleshooting Tables 8-11
  - Device Problems 8-11
  - Frame Relay PVC Problems 8-13
- Tests Available 8-14
  - Test Timeout Feature 8-14
- Starting and Stopping a Test 8-15
  - Aborting All Tests 8-16
- PVC Tests 8-17
  - Network or Port (Internal) PVC Loopback 8-18
  - Send Pattern 8-18
  - Monitor Pattern 8-19
  - Connectivity 8-19
- Physical Tests 8-20
  - DTE Loopback 8-20
- IP Ping Test 8-21
- Lamp Test 8-22

9 Setting Up OpenLane for FrameSaver Devices

- OpenLane Support of FrameSaver Devices 9-1
- Setting Up the OpenLane SLM System 9-2
- Setting Up FrameSaver SLV Support 9-2

10 Setting Up NetScout Manager Plus for FrameSaver Devices

- Getting Started 10-2
- Configuring NetScout Manager Plus 10-3
  - Adding FrameSaver SLV Units to the NetScout Manager Plus Network 10-4
  - Verifying Domains and Groups (Models 9820 and 9820-2M) 10-5
  - Correcting Domains and Groups (Models 9820 and 9820-2M) 10-6
  - Adding SLV Alarms Using a Template 10-8
  - Editing Alarms 10-9
  - Adding SLV Alarms Manually 10-11
  - Creating History Files 10-13
  - Installing the User-Defined History Files 10-15
- Monitoring a DLCI's History Data 10-16
- Monitoring the Agent Using NetScout Manager Plus (Models 9820 and 9820-2M) 10-19
- Statistical Windows Supported (Models 9820 and 9820-2M) 10-20

11 Setting Up Network Health for FrameSaver Devices

- Installation and Setup of Network Health 11-2
- Discovering FrameSaver Elements 11-3
- Configuring the Discovered Elements 11-4
- Grouping Elements for Reports 11-5
- Generating Reports for a Group 11-6
  - About Service Level Reports 11-6
  - About At-a-Glance Reports 11-6
  - About Trend Reports 11-7
  - Printed Reports 11-7
- Reports Applicable to SLV Devices 11-7

12 Hardware Maintenance (9820-45M)

- Overview 12-1
- Cleaning the Front Panel Assembly 12-2
- Replacing the Front Panel Assembly 12-3
- Replacing a Power Module 12-4

A Menu Hierarchy

- Menus A-1

B SNMP MIBs and Traps, and RMON Alarm Defaults

- MIB Support B-2
- Downloading MIBs and SNMP Traps B-2
- System Group (mib-2) B-3
  - FrameSaver Unit's sysDescr (system 1) B-3
  - FrameSaver Unit's sysObjectID (system 2) B-3
- Interfaces Group (mib-2) B-4
  - Paradyne Indexes to the Interface Table (ifTable) B-4
  - NetScout Indexes to the Interface Table (ifTable) B-5
- Standards Compliance for SNMP Traps B-6
  - Trap: warmStart B-7
  - Trap: authenticationFailure B-7
  - Traps: linkUp and linkDown B-8
  - Traps: enterprise-Specific B-12
  - Traps: RMON-Specific B-14
- RMON Alarm and Event Defaults B-15
  - Network Synchronous Port Physical Interface Alarm Defaults B-16
  - Frame Relay Link Alarm Defaults B-17
  - DLCI Alarm Defaults – Paradyne Area B-19
  - DLCI Alarm Defaults B-21
- Object ID Cross-References (Numeric Order) B-23

C Connectors, Cables, and Pin Assignments

- Rear Panels C-2
- COM (Terminal) Port Connector C-3
  - LAN Adapter Converter and Cable (Models 9820, 9820-2M, 9820-8M) C-3
  - Standard EIA-232 Crossover Cable (Models 9820, 9820-2M, 9820-8M) C-4
- User and Network Data Port Connectors (Models 9820, 9820-2M, 9820-8M) C-6
  - X.21 Network Cable (Models 9820, 9820-2M, 9820-8M) C-7
  - X.21 DTE Adapter Cable (Models 9820, 9820-2M, 9820-8M) C-8
  - V.35 Network Cable (Models 9820, 9820-2M, 9820-8M) C-9
  - V.35 DTE Adapter (Models 9820, 9820-2M, 9820-8M) C-11
  - EIA-530-A Straight-through Cable (Models 9820, 9820-2M, 9820-8M) C-13
- EIA-612/613 HSSI Connectors (Model 9820-45M) C-15
- LAN Connector (Model 9820-45M) C-16
- Modem Connector (Model 9820-45M) C-16

D Technical Specifications

E Equipment List

- Equipment E-1
- Cables E-3

About This Guide

Purpose and Intended Audience

This document contains information needed to properly set up, configure, and verify operation of FrameSaver SLV in-line monitors. It is intended for system designers, engineers, administrators, and operators.

Document Organization

Section	Description
Chapter 1	*About FrameSaver SLV In-Line Monitors.* Identifies how FrameSaver SLV in-line monitors fit into Paradyne's SLM solution, and describes the features of these units.
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 units.
Chapter 5	*Security and Logins.* Shows how to control access to the FrameSaver SLV and setting up logins.
Chapter 6	*Monitoring.* Shows how 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.
Chapter 8	*Troubleshooting.* Provides device problem resolution, alarm, and other information, as well as troubleshooting and test procedures.

Section	Description
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 NetScout Manager Plus for FrameSaver Devices.* Describes setup of the NetScout Manager Plus application so it supports FrameSaver units.
Chapter 11	*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.
Chapter 12	*Hardware Maintenance (9820-45M).* Describes maintenance of the 9820-45M, including replacement of the front panel assembly and power modules.
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:	
9820-A2-GL10	*FrameSaver SLV, Models 9820, 9820-2M, 9820-8M, and 9820-45M, Quick Reference*
9820-A2-GN10	*FrameSaver SLV, Models 9820, 9820-2M, and 9820-8M, Installation Instructions*
9820-A2-GN11	*FrameSaver SLV, Model 9820-45M, Installation Instructions*
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*

Contact your sales or service representative to order product documentation.

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.
(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 FrameSaver SLV In-Line Monitors

1

This chapter includes the following:

- *SLM Overview*
- *FrameSaver SLV In-Line Monitor Features*

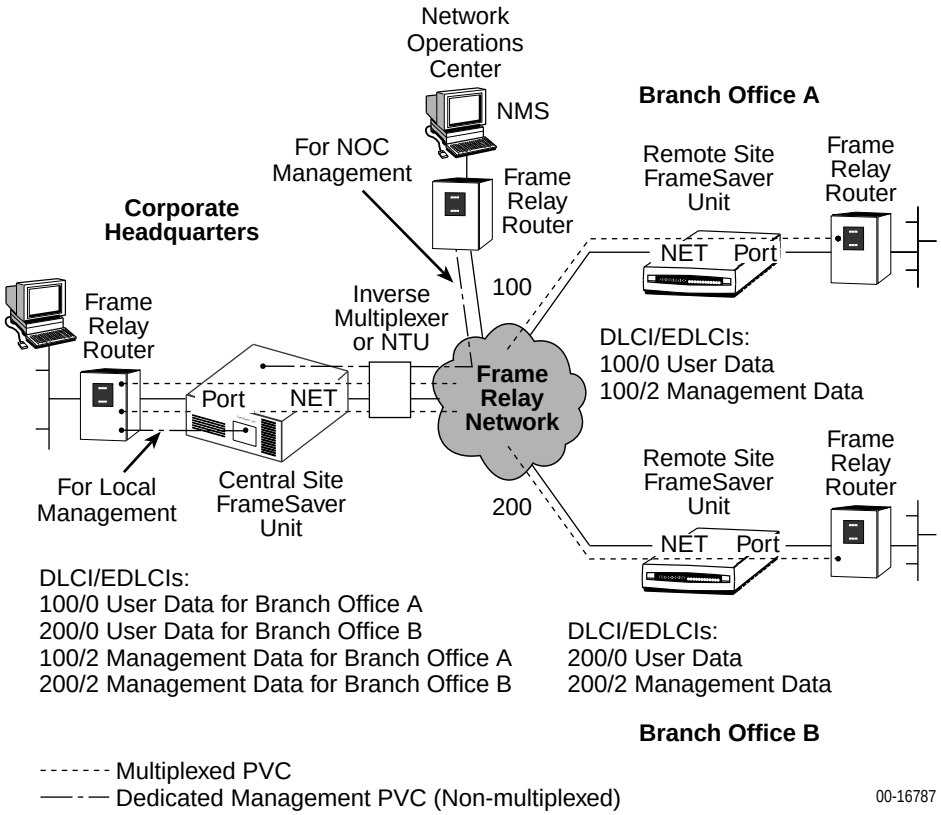
SLM Overview

The Service Level Management (SLM) Solution consists of:

- FrameSaver® SLV units
- OpenLane™ SLM system
- Standalone NetScout Probes and NetScout Manager Plus application (optional)

FrameSaver SLV (Service Level Verifier) in-line monitors add superior diagnostic capability, end-to-end visibility, accurate network performance reporting, and SLM intelligence to any frame relay network connection, regardless of the access device being used. FrameSaver SLV in-line monitors provide a global, multinational SLM solution that can be installed between a DTE (such as a router) and any type of network access device, such as a network termination unit (NTU), a T1/E1 inverse multiplexer, any DSU/CSU, a Digital Subscriber Line (DSL) endpoint, or an ATM IMA device or ATM Integrated Access Device with frame relay interworking.

The following illustration shows a network that includes FrameSaver units at the central site and remote sites. User data PVCs provide LAN-to-LAN connectivity between the central site and the remote sites.



The central site FrameSaver unit ordinarily is configured for management from a Network Management System (NMS), through either the attached router, as shown in the above figure, or through the Network Operations Center (NOC) router (for management by the Network Service Provider). Multiple management PVCs then connect the central site unit to the remote site units using Paradyne's proprietary PVC multiplexing method (embedded DLCIs).

FrameSaver SLV In-Line Monitor Features

The FrameSaver SLV in-line monitor provides the following features:

- **Intelligent Service Level Verification.** Provides accurate throughput, latency, and availability measurements to determine network performance and whether service level agreements (SLAs) are being met, along with SLA reporting. SLA parameter thresholds can be configured to provide proactive notification of a developing network problem.
- **Security.** Provides multiple levels of security to prevent unauthorized access to the unit.
- **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. These ratios are available through OpenLane SLV reports.
- **Frame Relay Aware Management.** Supports diagnostic and network management features over the frame relay network using the Annex-A, Annex-D, and Standard UNI (User Network Interface) LMI management protocol. 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.
- **Auto-Configuration**. Provides the following automatic configuration features:
  - — Frame Relay Discovery – For automatic discovery of network DLCIs and configuration of a user data port DLCI, the PVC connection, and a management PVC, which is multiplexed with user data DLCIs.
  - — LMI Protocol Discovery – For automatic configuration of the protocol being used by the network.
  - — DLCI Deletion – For automatic removal of configuration of unused DLCIs from the unit's configuration and statistical databases.
  - — CIR Determination – For automatic recalculation of the committed rate measurement interval (Tc) and excess burst size (Be) when a DLCI's CIR changes.

    Excess burst size (Be) and committed burst size (Bc) are recalculated when Committed Burst Size Bc (Bits) is set to CIR. The committed rate measurement interval (Tc) is recalculated when Committed Burst Size Bc (Bits) is set to Other.

- **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.

  In addition, port bursting statistics are kept for all frame relay links. These statistics are available real-time via the Enterprise MIB and historically as an RMON2 User History object. In future releases of the OpenLane SLM system, this will enable even more accurate calculations of utilization.

- **Network User History Synchronization.** Allows correlation of RMON2 User History statistics among all SLV devices in a network for more accurate OpenLane SLV reports. 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.

- **Extensive Testing Capability.** Provides a variety of tests to identify and diagnose device, network, and other problems. These tests can be commanded from the unit's menu-driven user interface or the OpenLane system (using its easy-to-use Diagnostic Troubleshooting feature).

- **Dedicated Troubleshooting PVC.** Provides a troubleshooting management link that helps service providers isolate problems within their network. This feature can be configured from the menu-driven user interface.

- **Maximum Number of PVCs and Management PVCs Supported.**

Feature	FrameSaver SLV 9820	FrameSaver SLV 9820-2M	FrameSaver SLV 9820-8M	FrameSaver SLV 9820-45M
Through Connections (PVCs)	16	120	250	512
Dedicated Management PVCs	2	2	2	2

- **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.

- **LMI Packet Capture.** Provides a way to upload 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. The 12 most recent LMI messages can be displayed from the menu-driven user interface.

- **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 or Channel Identifier (VPI/VCI) in the far-end ATM-access endpoint where the local DLCI is mapped so they can be correlated for OpenLane SLV reports.
- **Back-to-Back Operation.** Allows two FrameSaver devices to be connected via a leased-line network or simulation so a point-to-point configuration can be implemented.
- **Configuration Upload/Download and Software Download Capability.** Provides quick transfer of configuration options to and from nodes and software downloads while the unit is running using the standard File Transfer Protocol (FTP). Two software images can be stored.
- **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.
- **OpenLane Service Level Management Solution.** Provides an advanced, standards-based performance monitoring and management application.

  Being standards-based, the OpenLane SLM system can also 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 SLM 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.

- **NetScout Manager Plus and NetScout Probe Support.** Provides complete LAN and WAN traffic analysis and monitoring functions for FrameSaver SLV devices. The following features are supported using this application:

  — Thresholds for RMON 1 (Remote Monitoring, Version 1) alarms and events can be configured.

  — (Models 9820 and 9820-2M.) Performance monitoring can be performed using collected RMON 2 (Version 2) data. NetScout Manager Plus's Protocol Directory and Distribution functionality allows FrameSaver SLV 9820 and 9820-2M units to measure up to eleven network-layer protocols and report the amount of traffic generated by each. Its IP Top Talkers and Listeners reporting identifies the devices using network bandwidth for traffic and protocol analysis, identifying the network's top six users. In addition, it collects performance statistics from FrameSaver devices. Up to 900 samples can be stored in 15-minute buckets, with 96 buckets in a 24-hour period, for up to five days worth of data.

  — Optional standalone NetScout Probes can be used with FrameSaver devices at sites where full 7-layer monitoring, an unlimited number of protocols, and advanced frame capture and decode capabilities are desired.

	OSI Layers Monitored			
Using:	**9820**	**9820-2M**	**9820-8M**	**9820-45M**
FrameSaver SLV	1–3	1–3	1–2	1–2
Netscout Probe	3–7	3–7	3–7	3–7

- **Hardware Bypass Feature.** In the event of catastrophic system failure or power loss, data traffic is routed through hardware directly between the network port and the user data port.

User Interface and Basic Operation

2

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

- *Logging On*
- *Main Menu*
- *Screen Work Areas*
- *Navigating the Screens*
  - *Keyboard Keys*
  - *Function Keys*
  - *Selecting from a Menu*
  - *Switching Between Screen Areas*
  - *Selecting a Field*
  - *Entering Information*

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.
  - — A local in-band management channel configured on the DTE port between the FrameSaver unit and the router.
- Dial-in connection using the internal modem (Model 9820-45M).
- Direct terminal connection over the COM port (Terminal port on the Model 9820-45M).

When logging on, the User Interface Idle screen appears.

- If no security was set up or security was disabled, the Main Menu screen (see *Main Menu* on page 2-4) appears. 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.
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. – An external modem is disconnected. – An SNMP trap is generated. Access is denied. See your system administrator to verify your login (Login ID/Password combination).

If two sessions are already active, wait and try again.

- If attempting to access the unit through Telnet, the local Telnet client process returns a **`Connection refused:`** message.
- If attempting to access the unit over the COM (or Terminal) port or Modem port, not via Telnet, the User Interface Already In Use screen is redisplayed.

  The type of connection (Telnet connection, direct COM (or Terminal) port connection, or direct Modem 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 COM (Terminal) port-connected terminal, the session is ended.
   - — For a modem port-connected terminal, 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 five menus or branches. The Access Level at the top of the screen only appears when security has been set up.

```
main                              Access Level: 1                    9820-45M
Device Name: Node A                                              05/13/2000 02:01
Slot: 1  Type: T1 FR NAM

                                    MAIN MENU

                                   Status
                                   Test
                                   Configuration
                                   Auto-Configuration
                                   Control
                                   Easy Install (Model 9820-45M only)









--------------------------------------------------------------------------------
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 test 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 automatically populate network and data port DLCI configuration options with numeric settings.
Control	Control the asynchronous user interface for call directories, device naming, login administration, and selecting software releases. You can also initiate a power-on reset of the FrameSaver unit.

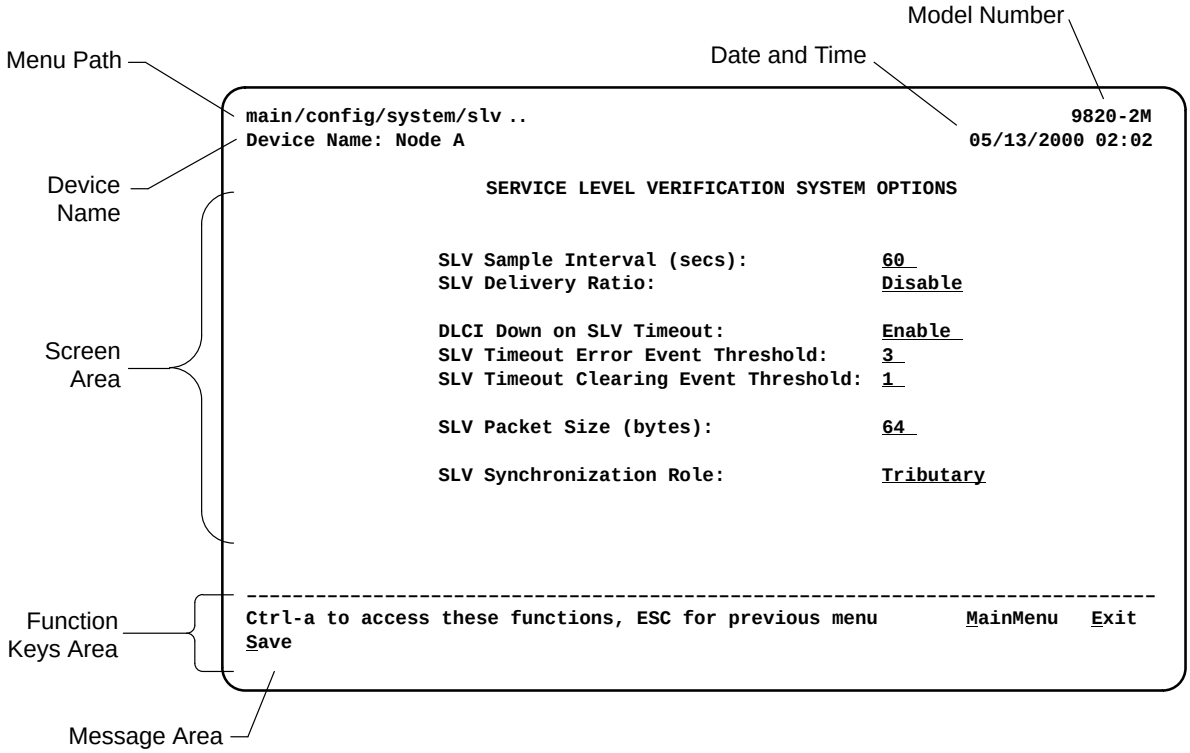
See Appendix A, *Menu Hierarchy*, for a pictorial view of the menu hierarchy, which represents the organization of the FrameSaver unit's menus and screens.

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.

Below is a sample configuration screen showing a 2 Mbps unit.



Screen Format	Description
Menu Path	Menu selections made to reach the current screen.
Device Name	Customer-assigned identification of the FrameSaver unit.
9820	FrameSaver unit's model number: the 128 kbps 9820, 2 Mbps 9820-2M, 8 Mbps 9820-8M, or 45 Mbps 9820-45M.
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) 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 asynchronous terminal 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.

▶ 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 Areas*
  - *Accessing and Displaying Configuration Options*
  - *Changing Configuration Options*
  - *Saving Configuration Options*
  - *Minimal Configuration Before Deploying Remote Units*

Basic Configuration

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

The Configuration Edit/Display menu of a FrameSaver SLV 9820-2M is shown below.

Configuration Menu

```
main/config                                                    9820-2M
Device Name: Node A                                    5/13/2000 23:32

                          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
```

Changing an Auto-Configuration setting can also change the FrameSaver unit's configuration. See *Setting Up Auto-Configuration* for additional information.

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 SLV, Models 9820, 9820-2M, 9820-8M, and 9820-45M, Quick Reference*
- *Configuration Option Tables*

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.

Minimal Configuration Before Deploying Remote Units

At a minimum, the following configuration options must be set before deploying a a FrameSaver unit to a remote site:

- Node IP Address
- Node Subnet Mask

Configuration Options

4

This chapter includes the following:

- *Configuring Using the Easy Install Screen (Model 9820-45M)*
- *Entering System Information and Setting the System Clock*
- *Setting Up for Trap Dial-Out (Models 9820, 9820-2M, 9820-8M)*
  - *Setting Up an External Modem for Trap Dial-Out*
  - *Setting Up Call Directories for Trap Dial-Out*
- *Setting Up Auto-Configuration*
  - *Selecting a Frame Relay Discovery Mode*
  - *Automatically Removing a Circuit*
- *Setting Up Management*
  - *Setting Up Local Management at the Central Site*
  - *Setting Up So the Router Can Receive RIP*
  - *Setting Up Service Provider Connectivity at the Central Site*
- *Setting Up Back-to-Back Operation*
  - *Changing Operating Mode*
- *Configuration Option Tables*
- *Configuring the Overall System*
  - *Configuring Frame Relay and LMI for the System*
  - *Configuring Service Level Verification Options*
  - *Configuring General System Options*
- *Configuring the Physical Interfaces*
  - *Configuring the Network Data Port*
  - *Configuring the User Data Port*

- *Configuring Frame Relay for an Interface*
- *Manually Configuring DLCI Records*
- *Configuring PVC Connections*
- *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 and Trap Dial-Out*
  - *Configuring the Ethernet Port (Model 9820-45M)*
  - *Configuring the Communication Port*
  - *Configuring the COM Port to Support an External Modem (Models 9820, 9820-2M, 9820-8M)*
  - *Configuring the Modem Port (Model 9820-45M)*

Configuring Using the Easy Install Screen (Model 9820-45M)

The Easy Install screen provides direct access to the configuration options required to establish communication and prepare for Auto-Configuration.

Main Menu → Easy Install

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. This address may be shared only among management PVCs. **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, DLCI** Default Setting: **None**
Specifies whether a DLCI is defined for troubleshooting by the service provider. **None** – A troubleshooting DLCI is not defined. **DLCI** – A troubleshooting DLCI is defined. Its value must be entered in the next field.
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. **16 – 1007** – Specifies the DLCI.
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.

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

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 4-50. After configuring the Ethernet port configuration options, save your changes. Then press ESC to return to the Easy Install screen.

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:ss).

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.

Setting Up for Trap Dial-Out (Models 9820, 9820-2M, 9820-8M)

An external modem can be attached to the COM port for dialing out when an SNMP trap is generated.

To set up an external modem, you need to:

1. Set up SNMP trap managers.
2. Set up an external modem.
3. Set up Modem Directory phone numbers.
4. Configure trap dial-out.

See *Configuring SNMP NMS Security* to set up SNMP trap managers.
See *Setting Up Call Directories for Trap Dial-Out* when trap dial-out is desired.
See *Configuring SNMP Traps and Trap Dial-Out* for trap and alarm information.

Setting Up an External Modem for Trap Dial-Out

(Models 9820, 9820-2M, 9820-8M.) When trap dial-out is desired, the PC or asynchronous terminal must be disconnected from the unit's COM port when setup is complete, and an external modem connected instead. See *Configuring the COM Port to Support an External Modem* for additional information.

Setting Up Call Directories for Trap Dial-Out

(Models 9820, 9820-2M, 9820-8M.) To set up call directories:

▶ Procedure

1. Set up directory phone numbers.
   Main Menu → Control → Modem Call Directories
2. Select Directory Number A (for Alarm).
3. Enter the phone number(s).

Valid characters include . . .	For . . .
ASCII text	Entering the phone number.
Space, underscore (_), and dash (–)	Readability characters.
Comma (,)	Readability character for a 2-second pause.
B	Blind dialing.
P	Pulse dialing, unless B is specified.
T	Tone dialing, unless B is specified.
W	Wait for dial tone.

4. Save the phone number(s).

Setting Up Auto-Configuration

The auto-configuration feature allows you to select a method of automatic configuration and connection of DLCIs within the FrameSaver unit, as well as to automatically remove DLCIs and connections that are no longer supported by the network service provider. Auto-configuration also maintains associated DLCI option settings when Standard LMI is used on the network data port.

Main Menu → Auto-Configuration

Auto-Configuration Screen Example

```
main/auto-configuration                                          9820–2M
Device Name: Node A                                      5/13/2000 23:32

                          AUTO-CONFIGURATION


            Frame Relay Discovery Mode:        1MPort
            Automatic Circuit Removal:         Enable




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

Selecting a Frame Relay Discovery Mode

When a Frame Relay Discovery Mode is active, the FrameSaver unit "discovers" network DLCIs from the network LMI status response message. It configures a network DLCI, a user data port DLCI, and automatically connects them to create a PVC.

Main Menu → Auto-Configuration → Frame Relay Discovery Mode

Automatically configured network DLCIs are multiplexed, and each automatically configured port DLCI carries the same DLCI Number as its corresponding network DLCI. These are the same DLCI numbers that would have been available had the FrameSaver unit not been inserted in the link, between your equipment and the network.

NOTE:

A local Management PVC (e.g., the PVC between the router and the FrameSaver unit's user data port) must be configured manually; it cannot be configured automatically (see *Setting Up Local Management at the Central Site*).

The following will occur when a Frame Relay Discovery Mode is selected:

Discovery Mode	Configuration Description
1MPort *(default)*	■ Auto-configuration is enabled on Port-1. ■ A management DLCI is configured. ■ A multiplexed network DLCI containing two embedded DLCIs (EDLCIs) is configured for Port-1 user data and management data. ■ A PVC connection is configured between the network and port DLCIs.
1Port	■ Auto-configuration is enabled on Port-1. ■ No management DLCI is configured. ■ A multiplexed network DLCI is configured for Port-1 user data. ■ A PVC connection is configured between the network and port DLCIs.
NetOnly	■ Auto-configuration of a network DLCI only; no Port-1 or PVC connections are configured. ■ No Port-1, PVC connection, or management DLCI is configured.
Disable	■ No frame relay discovery or automatic configuration takes place. The FrameSaver unit will be configured manually.

NOTE:

If 1MPort (the default) is not the setting required for your application, change the Frame Relay Discovery Mode **before** connecting the network cable or editing discovered option settings. Otherwise, the FrameSaver unit will start "discovering" DLCIs as soon as it powers up.

To recover from this problem, edit a selected "discovered" DLCI or PVC connection manually if any DLCIs or PVC Connections have been configured manually. If only a local management PVC between the router and the FrameSaver unit has been configured, select the desired Frame Relay Discovery Mode and Save the change.

The default discovery mode is 1MPort (management DLCIs multiplexed with data DLCIs on Port-1, which creates two embedded DLCIs [EDLCIs] – one EDLCI for Port-1 user data, and another EDLCI for management data); that is, for each DLCI discovered on the network, a multiplexed network DLCI and a standard data port DLCI will be configured and connected, and a Management PVC will be embedded in the network DLCI. When LMI is active on the network interface and PVC status information (with provisioned DLCI numbers) is next received from the network, the unit automatically saves the settings to the Current Configuration area.

Configuration options set by the selected discovery mode can be manually modified, refined, or deleted at any time using the Configuration menus. No previously discovered and configured DLCIs or cross-connections will be removed unless authorized or Automatic Circuit Removal is enabled (see *Automatically Removing a Circuit*). Additional discovered DLCIs will be configured according to the current Frame Relay Discovery Mode setting. Selecting or changing the setting will not affect IP Addresses or Subnet Masks.

NOTE:

When auto-configuration creates a multiplexed DLCI, but a standard DLCI is needed, change the DLCI to standard from the network DLCI Records screen: *Configuration → Network → DLCI Records*

When a Frame Relay Discovery Mode is changed and saved, the **`Saving will cause Auto-Configuration to update and Restart. Are you sure?`** prompt appears. No is the default for this prompt.

- If Yes (y) is entered, the **`Delete All DLCIs and PVC Connections?`** prompt appears. No is the default for this prompt.
  - — If Yes is entered, all multiplexed DLCIs and PVC Connections are deleted, except for Management PVCs with the user data port as the primary destination and the Management PVC that is designated as TS Management Link.
  - — If No is entered, previously discovered and auto-configured option settings will not be removed, but configuration updates due to LMI response messages are performed according to the just saved mode setting.
- If No (n) is entered, or if you exit the screen without responding to the prompt, no Auto-Configuration updates are performed and updates due to LMI response messages are performed according to the previously saved setting.

Automatically Removing a Circuit

Using the automatic circuit removal feature, which comes enabled, network DLCIs and PVCs can be automatically removed from the unit's configuration when the the network service provider no longer supports them. Automatic deletion is based upon information from a LMI full status response on an active frame relay link.

When this feature is set to:

- **Enable** – The following will be automatically removed from the unit's configuration:
  - — Unsupported network DLCIs and PVC connections that include multiplexed network DLCIs.
  - — Unsupported standard network DLCIs that are not configured as the primary destination in a management PVC.
  - — Non-management PVCs in which unsupported standard network DLCIs are included.
  - — DLCIs not included in three consecutive LMI full status response messages.
  - — LMI status responses that indicate a Deleted status for the DLCI.

  All configured options relating to the deleted circuits are also deleted and they revert to their default settings.

  A DLCI will not be deleted if the physical interface or frame relay link is down, or if the DLCI is used for the TS Management Link.
- **Disable** – Unused network DLCIs, PVC connections, and management PVCs must be manually removed.

Setting Up Management

FrameSaver units are already set up for SNMP management, with Community Name 1 set to Public and Name 1 Access set to Read/Write. For remote sites, other than the IP Address, this is all that is required.

Configuration → Management and Communication → General SNMP Management

See Table 4-12, General SNMP Management Options, for configuration information. For the central site, local management between the unit and the router must be set up, as well (see *Setting Up Local Management at the Central Site*).

Setting Up Local Management at the Central Site

Set up a local management PVC between the central site unit and its router for local management control by the end-user customer.

▶ Procedure

To set up management through the router:

1. Create a DLCI that will be used for management on the user data port.

   Configuration → Data Ports → DLCI Records

2. Create a Management PVC using the user data port DLCI just created.

   Configuration → Management and Communication → Management PVC

   Minimally, enter the following options:

   — Name for the management PVC

   — Interface IP Address and Subnet Mask, if different from the Node's

   — Primary Link for this Management PVC (the user data port)

   — Primary DLCI (i.e., the data port DLCI)

3. Save the configuration.

See Table 4-8, DLCI Record Options, and Table 4-11, Management PVC Options, for configuration information.

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 SLV devices. Node IP information should be set up (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 serial`*`x`***, **`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 4-8, DLCI Record Options, and Table 4-11. Management PVC Options for configuration information.

Setting Up Service Provider Connectivity at the Central Site

When management needs to be set up between a service provider's customer and its network operations center (NOC), a non-multiplexed DLCI must be configured to carry management data between the customer's central site and the NOC console. This requires that a frame relay discovered DLCI needs to be modified. This is because all auto-configured network DLCIs are configured as multiplexed DLCIs.

▶ Procedure

To set up NOC management:

1. Select DLCI Records on the network interface.

   Configuration → *Network* → *DLCI Records*

2. Select Modify. The **`Modify DLCI Record for DLCI Number`** prompt appears.

3. Select the DLCI that will be used by pressing the spacebar until the correct DLCI number appears, then select it.

4. Change the DLCI Type from Multiplexed to Standard.

   The **`DLCI in connections. Update DLCI usage as follows:`** prompt appears.

5. Select the **`Delete EDLCI Connections and Make a Mgmt Only PVC`** option.

   PVC connections for the selected DLCI are broken, the Port-1 DLCI mapped to this network DLCI and the embedded management DLCI (EDLCI) are deleted, and the selected DLCI will be reconfigured as a management PVC using the Node IP Address.

See Table 4-8, DLCI Record Options, for configuration information.

Setting Up Back-to-Back Operation

Using this special feature, you can set up two FrameSaver units that are connected back-to-back without frame relay switches between them, as in a test bench setup.

Changing Operating Mode

When setting up back-to-back operation:

- One unit must be configured for Standard operation, which is the setting for normal operation.
- The other unit must be configured for Back-to-Back operation so it presents the network side of the UNI (user-network interface).

Only one of the units will have its operating mode changed.

▶ Procedure

To set up back-to-back operation:

1. On the unit to be configured for Back-to-Back operation, manually configure DLCIs; DLCIs should be configured before connecting the two units.
2. Access the Change Operating Mode screen.

   Main Menu → *Control* → *Change Operating Mode*
3. Select Back-to-Back Operation, and respond Yes to the **`Are you sure?`** prompt.
4. Save the change.

▶ Procedure

To return the unit to normal operation:

1. Return to the Change Operating Mode screen and switch back to Standard Operation.
2. Respond Yes to the prompt and save the change. The units can be reconnected to a standard frame relay network.

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 them 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 Data Port Physical Interface Options
- Table 4-6. User Data Port Physical Interface Options
- Table 4-7. Interface Frame Relay Options
- Table 4-8. DLCI Record Options
- Table 4-9. PVC Connection Options
- Table 4-10. Node IP Options
- Table 4-11. Management PVC Options
- Table 4-12. General SNMP Management Options
- Table 4-13. Telnet and FTP Session Options
- Table 4-14. SNMP NMS Security Options
- Table 4-15. SNMP Traps and Trap Dial-Out Options
- Table 4-16. Ethernet Port Options (Model 9820-45M)
- Table 4-17. Communication Port Options
- Table 4-18. External Modem (COM Port) Options (Models 9820, 9820-2M, 9820-8M)
- Table 4-19. Modem Port Options (Model 9820-45M)

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

See *Configuring Frame Relay for an Interface* to set an interface's frame relay options.

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: **Independent**
Configures the device to allow the state of the LMI to be passed from one interface to another, determining how the unit will handle a change in the LMI state. Sometimes referred to as LMI pass-through. **Independent** – Handles the LMI state of each interface separately so that the LMI state of one interface has no effect on the LMI state of another interface. Provides LMI Spoofing. This is the recommended setting when backup is configured, and for Network Service Providers (NSPs). **Net1-FR1_Follows_Port-1** – Brings LMI down on the network interface when LMI on Port-1 goes down, disabling the network interface and deasserting its control leads. When LMI on Port-1 comes back up, the network interface is reenabled. The LMI state on the network interface has no effect on the LMI state on Port-1. That is, the network interface's LMI follows Port-1's LMI. 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 when LMI on the network interface goes down, disabling Port 1 and deasserting its control leads. When LMI on the network interface comes back up, Port-1 is reenabled and its control leads are reasserted. The LMI state on Port-1 has no effect on the LMI state on the network interface. That is, Port-1's LMI follows the network interface's LMI. 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 LMI down on the network interface when LMI on Port-1 goes down (or LMI down on Port-1 when LMI on the network interface goes down), and allows LMI to come back up when LMI comes back on the other interface. That is, the LMI state for one interface is dependent on the other. Use this setting when backup is through the router instead of the unit. It is *not* recommended since it makes fault isolation more difficult.
Traffic Policing
Possible Settings: **Disable, Enable** Default Setting: **Disable**
Determines whether the Committed Information Rate (CIR) and Excess Information Rate (EIR) are enforced for frames sent to the network frame relay link. *Display Conditions* – This option appears only for Model 9820-45M. **Disable** – CIR and EIR are not enforced. **Enable** – CIR and EIR are 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 SLV devices. Inband communications are used to pass frames that calculate latency, as well as transmission success and other SLV information. **10 – 3600** – Sets the SLV Sample Interval (secs) in seconds.
SLV Delivery Ratio
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether communication of Frame and Data Delivery Ratios (FDR/DDR) between FrameSaver SLV devices is enabled. To use this capability, both ends of all PVCs must be FrameSaver SLV 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 a DLCI is declared Inactive after the configured threshold for SLV Timeout has been exceeded. NOTE: This option does not apply to multiplexed DLCIs connected to a far-end unit with hardware bypass capability. **Enable** – After the configured threshold for missed SLV packets has been exceeded, the DLCI's status is changed to Inactive. **Disable** – An SLV Timeout Error Event does not affect DLCI status.
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 SLV devices. **Tributary** – Uses network timing received from incoming SLV communications and provides network-based synchronization information to other devices in the network. **Controller** – Uses its own internal time-of-day clock and provides synchronization information to other devices in the network based upon its own clock. NOTE: Only one device in the network should be configured as the SLV synchronization controller. **None** – Incoming timing information is ignored and no timing information is sent out. This setting should only be used when network synchronization is not desirable, or when a single unit connects multiple networks or network segments.

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. **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 the tests. *Display Conditions* – This option only appears when Test Timeout is set to Enable. **1 – 120** – Sets the Test Timeout period in minutes (inclusive).
Power Up Selftest
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether a self-test runs when the unit is powered on. Disabling the self-test reduces the time it takes for the unit to become operational. *Display Conditions* – This option only appears for Model 9820-45M. **Enable** – The power-on self-test runs. **Disable** – The power-on self-test does not run.

Configuring the Physical Interfaces

Characteristics for the following physical interfaces can be configured:

- Network Data Port Physical Interface Options
- User Data Port Physical Interface Options

Configuring the Network Data Port

Select Physical to display or change the physical configuration options for the port being used as the network interface (see Table 4-5).

Main Menu → *Configuration* → *Network* → *Physical*

The network data port physical interface acts as a DTE. The network interface automatically detects the rate offered by the external NTU, CSU/DSU, or inverse multiplexer.

Table 4-5. Network Data Port Physical Interface Options (1 of 2)

Port Type
Possible Settings: **E530, V.35, X.21** Default Setting: **V.35**
Selects the type of port to be used for the network data port. *Display Conditions* – This option does not appear for Model 9820-45M, for which the port type is HSSI. **E530** – The port is configured as an EIA-530-A-compatible DTE. An EIA-530 compatible DCE can be directly connected to the DB25 connector for this port on the rear of the FrameSaver unit. **V.35** – The port is configured as a V.35-compatible DTE. A V.35-compatible DCE can be connected to the DB25 connector for this port using an adapter cable on the rear of the FrameSaver unit. **X.21** – The port is configured as a V.11/X.21-compatible DTE. A V.11/X.21-compatible DCE can be connected to the DB25 connector for this port using an adapter cable on the rear of the FrameSaver unit.
Invert Internal Clock
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether the internal clock (used for timing data transmitted to the DCE) will be phase-inverted with respect to the clock received at the interface. This option is useful when long cable lengths between the FrameSaver device and the DCE are causing errors. *Display Conditions* – This option does not appear for Model 9820-45M. **Enable** – The internal clock used to transmit data to the DCE is phase inverted with respect to the clock supplied by the DCE to this port. **Disable** – The internal clock is not inverted (normal).

Table 4-5. Network Data Port Physical Interface Options (2 of 2)

Monitor DSR
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the DCE Ready (DSR) circuit on the network data port will be used to determine when valid data communication is possible with the unit. When this condition is detected, an alarm is generated, LMI is declared down, and no further transfer of frame relay data can occur on this interface. *Display Conditions* – This option does not appear when when Port Type is set to X.21. The signal is assumed to be asserted. **Enable** – Interchange circuit CC (ITU/CCITT 107) – DSR is monitored to determine when valid data is being sent from the DCE. **Disable** – DSR is not monitored. DSR is assumed to be asserted and data is transmitted, regardless of the actual state of the lead.
Monitor CTS
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the Clear to Send (CTS) circuit on the network data port will be used to determine when valid data communication is possible with the unit. When this condition is detected, an alarm is generated, LMI is declared down, and no further transfer of frame relay data can occur on this interface. *Display Conditions* – This option does not appear for Model 9820-45M, or when Port Type is set to X.21. The signal is assumed to be asserted. **Enable** – Interchange circuit CB (ITU/CCITT 106) – CTS is monitored to determine whether data should be transmitted to the DCE. **Disable** – CTS is not monitored. CTS is assumed to be asserted and data is transmitted, regardless of the actual state of the lead.
Monitor RLSD
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the Received Line Signal Detector (RLSD) circuit on the network data port will be used to determine when valid data communication is possible with the unit. When this condition is detected, an alarm is generated, LMI is declared down, and no further transfer of frame relay data can occur on this interface. *Display Conditions* – This option does not appear for Model 9820-45M. If Port Type is set to X.21, the Indication interchange circuit is monitored instead of RLSD. **Enable** – Interchange circuit CF (ITU/CCITT 109) – RLSD is monitored to determine when valid data communication is possible with the DCE. **Disable** – RLSD is not monitored. RLSD is assumed to be asserted and data is transmitted, regardless of the actual state of the lead.

Configuring the User Data Port

Select Physical to display or change the physical characteristics of the user data port connected to the DTE (see Table 4-6).

Main Menu → Configuration → Data Ports → Physical

The data rate of the user data port is automatically set to the rate of the network interface.

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

Port Type
Possible Settings: **E530, V.35, X.21** Default Setting: **V.35**
Selects the type of port to be used for the user data port. *Display Conditions* – This option does not appear for Model 9820-45M, for which the port type is HSSI. **E530** – The port is an EIA-530-A-compatible DCE. An EIA-530-A-compatible DTE can be directly connected to the DB25 connector. **V.35** – The port is a V.35-compatible DCE. A V.35-compatible DTE can be connected to the DB25 connector by using an adapter cable. **X.21** – The port is a V.11/X.21-compatible DCE. A V.11/X.21-compatible DTE can be connected to the DB25 connector by using an adapter cable.
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. *Display Conditions* – This option does not appear for Model 9820-45M, or when Port Type is set to X.21. **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.

Table 4-6. User Data Port Physical Interface Options (2 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). *Display Conditions* – This option does not appear for Model 9820-45M. **Auto** – The port checks the clock supplied by the DCE on TXC. If necessary, the port automatically phase inverts 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.
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. *Display Conditions* – This option does not appear when Port Type is set to X.21 (the signal is assumed to be asserted). **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.
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. *Display Conditions* – This option does not appear for Model 9820-45M. **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.
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) for Models 9802, 9820-2M, and 9820-8M, or LA (ITU 143) for Model 9820-45M. *Display Conditions* – This option does not appear when Port Type is set to X.21. **Local** – The DTE attached to the port controls the local external DTE Loopback. **Disable** – The DTE cannot control the local external DTE Loopback.

Configuring Frame Relay for an Interface

Select Frame Relay from the interface's menu to display or change the Frame Relay options for an individual interface (see Table 4-7).

Main Menu → Configuration → [Network/Data Ports] → Frame Relay

See *Configuring Frame Relay and LMI for the System* for additional information.

Table 4-7. Interface Frame Relay Options (1 of 3)

LMI Protocol
Possible Settings: **Initialize_From_Net1FR1**, **Initialize_From_Interface, Auto_On_LMI_Fail, Standard, Annex-A, Annex-D** Default Setting: *For user data port links:* **Initialize_From_Interface** *For network data port links:* **Auto_On_LMI_Fail**
Specifies either the LMI protocol supported on the frame relay interface or the discovery source for the LMI protocol. **Initialize_From_Net1FR1** – The LMI type supported on this frame relay link will be configured to match the LMI protocol initially discovered on the primary Network frame relay link (Net1FR1). LMI Protocol is set to None internally, but once a protocol has become active or is set on the primary Network link, the protocol will be set to the same value on this link (Standard, Annex-A or Annex-D). The protocol will *not* be updated based on changes to Net1FR1 after being set initially. *Display Conditions* – This option value only appears for a user data port. **Initialize_From_Interface** – The LMI type supported on this frame relay link will be configured to match the LMI protocol discovered from the attached Network line or 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. Frame relay links on the user data port discover 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 user data port and network data ports. Frame relay links on the user data port discover the LMI protocol from LMI status polls on attached DTE devices. Frame relay links on the network data port discover LMI protocol by sending polls to an attached Network line and "listening" for correct poll response messages. **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.

Table 4-7. Interface Frame Relay Options (2 of 3)

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.
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.

Table 4-7. Interface Frame Relay Options (3 of 3)

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.

Manually Configuring DLCI Records

The Auto-Configuration feature automatically configures DLCI Records and their PVC Connections. DLCI Records can also be created manually (see Table 4-8).

Main Menu→ Configuration→ [Network/Data Ports]→ DLCI Records

Typically, DLCI Records only need to be configured when building Management PVCs between the NOC and the central site unit; the unit automatically configures non-management DLCI Records and PVC Connections.

Table 4-8. 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 – 15 and 1008 – 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.
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 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. For user data port DLCIs, this is the only selection available. **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.

Table 4-8. DLCI Record Options (2 of 3)

CIR (bps)
Possible Settings: *For FrameSaver SLV 9820:* **0 – 128000** *For FrameSaver SLV 9820-2M:* **0 – 2048000** *For FrameSaver SLV 9820-8M:* **0 – 8128000** *For FrameSaver SLV 9820-45M:* **0 – 44210000** 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 – *maximum CIR rate*** – Specifies the DLCI's 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: *For FrameSaver SLV 9820:* **0 – 128000** *For FrameSaver SLV 9820-2M:* **0 – 2048000** *For FrameSaver SLV 9820-8M:* **0 – 8192000** *For FrameSaver SLV 9820-45M:* **0 – 44210000** Default Setting: **64000**
Allows you to display or change the DLCI's committed burst size, in bits. *Display Conditions* – This option only appears when Committed Burst Size is set to Other. **0 – *maximum burst size*** – Specifies the maximum amount of data that the network has agreed to deliver within the committed rate measurement interval (Tc).

Table 4-8. 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
For FrameSaver SLV 9820: Possible Settings: **0 – 128000** Default Setting: **64000** *For FrameSaver SLV 9820-2M:* Possible Settings: **0 – 2048000** Default Setting: **1984000** *For FrameSaver SLV 9820-8M:* Possible Settings: **0 – 8192000** Default Setting: **8128000** *For FrameSaver SLV 9820-45M:* Possible Settings: **0 – 44210000** Default Setting: **44146000**
Allows you to display or change the DLCI's excess burst size, in bits. **0 – *maximum burst size*** – Specifies the maximum amount of data over the committed burst size that the network will attempt to deliver within the committed rate measurement interval (Tc).
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 user data 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). This option has no effect when there is only one user data port. *Display Conditions* – This option is not available for the network interface or for Model 9820-45M. **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 or for Model 9820-45M. **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 4-9).

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.

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 4-9. PVC Connection Options (1 of 3)

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 4-9. PVC Connection Options (2 of 3)

Primary Destination Link
Possible Settings: **Net1-FR1** Default Setting: Initially blank; no default.
Specifies the frame relay interface used as the primary 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 data port has no DLCIs defined, this interface would not appear as a valid setting. **Net1-FR1** – Specifies the network data port as the destination link.
Primary Destination DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the primary 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. NOTE: Primary Destination DLCI has no value if Primary Destination Link contains no value. **16 – 1007** – Specifies the DLCI number.
Primary Destination EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the primary 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.
Alternate Destination Link
Possible Settings: **Net1-FR1** Default Setting: Initially blank; no default.
Specifies the frame relay interface used as the alternate destination link if the Primary Destination Link fails. 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 data port has no DLCIs defined, this interface would not appear as a valid setting. *Display Conditions* – This option appears only for Model 9820-45M. **Net1-FR1** – Specifies the network data port as the destination link.

Table 4-9. PVC Connection Options (3 of 3)

AlternateDestination DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the alternate 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. NOTE: Alternate Destination DLCI has no value if Alternate Destination Link contains no value. *Display Conditions* – This option appears only for Model 9820-45M. **16 – 1007** – Specifies the DLCI number.
Alternate Destination EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the alternate destination Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection. *Display Conditions* – This option appears only for Model 9820-45M, only when the Alternate 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 and Trap Dial-Out Options
- Ethernet Port Options (Model 9820-45M)
- Communication Port Options
- External Modem (COM Port) Options (Models 9820, 9820-2M, 9820-8M)
- Modem Port Options (Model 9820-45M)

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 4-10). 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 **`This PVC has been designated as the TS Management Link`** message.

NOTE:

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

Table 4-10. 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. On the Model 9820-45M, this address may be shared only among management PVCs. On Models 9820, 9820-2M, and 9820-8M this address may also be used to access the COM port. **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.

Table 4-10. Node IP Options (2 of 3)

Default IP Destination
Possible Settings (Models 9820, 9820-2M, 9820-8M): **None, COM, *PVCname***   Possible Settings (Model 9820-45M): **None, Modem, Ethernet, COM, *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 4-11, Management PVC 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. **Modem** – Specifies that the default destination is connected to the Modem port. Only appears when Port Use is set to Net Link (see Table 4-19, Modem Port Options). **Ethernet** – Specifies that the default destination is connected to the Ethernet port (see Table 4-16, Ethernet Port Options). **COM** – Specifies that the default destination is connected to the COM (Terminal) port. Only appears when Port Use is set to Net Link (see Table 4-17, Communication 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 4-10. Node IP Options (3 of 3)

TS Management Link
Available Settings: **None, *PVCname***   Default Setting: **None**
Specifies a troubleshooting management link for the special needs of network service providers. If the option is changed from the management PVC name to None, the **`Delete the Management PVC PVCname and the associated DLCI 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 will be deleted. **None** – Disables or does not specify a TS 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 link as a DLCI with DLCI Type set to Standard.
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 Management Link. *Display Conditions* – This option does not appear when TS 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 4-13, 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 4-11). First, DLCI records must have been configured for the interface where the Management PVC will reside. See *Manually Configuring 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.

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 Management Link, an ... **`Are You Sure?`** prompt appears to warn you.

Table 4-11. Management PVC Options (1 of 4)

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., London for the London office). 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 4-10, 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 4-11. Management PVC Options (2 of 4)

Intf Subnet Mask
Possible Settings: **Node-Subnet-Mask, Calculate, Special** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-Subnet-Mask**
Specifies the subnet mask needed to access the unit 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 4-10, 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** – (Models 9820, 9820-2M, 9820-8M.) Clears the link and the DLCI field, and suppresses the EDLCI field if the DLCI was multiplexed.

Table 4-11. Management PVC Options (3 of 4)

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** *For Model 9820-45M:* **None**
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** – (Models 9820, 9820-2M, 9820-8M.) 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 4-8, DLCI Record Options). **Standard_out** – The device will send standard RIP messages to communicate routing information only about other FrameSaver SLV 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*.

Table 4-11. Management PVC Options (4 of 4)

Alternate Link
Possible Settings: **Net1-FR1** Default Setting: Initially blank; no default.
Specifies the alternate frame relay interface to use for this management PVC if the primary link has failed. The interface selected must have at least one DLCI (or DLCI with EDLCI) defined, which is not part of a PVC connection or already assigned as a management PVC. *Display Conditions* – This option appears only for Model 9820-45M. **Net1-FR1** – Specifies that the network interface be used in the connection.
Alternate DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the alternate DLCI number used for the management PVC after the frame relay interface is selected and the primary link has failed. 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. *Display Conditions* – This option appears only for Model 9820-45M. 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).
Alternate EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the alternate EDLCI number used for a management PVC when a multiplexed DLCI is selected and the primary link has failed. 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 appears only for Model 9820-45M, and only if the DLCI field references a multiplexed DLCI. NOTE: Clearing the DLCI or changing it to a standard DLCI suppresses EDLCI field. **0 – 62** – Specifies the EDLCI number (inclusive).

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 4-12).

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

Table 4-12. General SNMP Management Options

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.
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 4-13).

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 4-13. 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 Management Link. **Enable** – Requires a login to access a Telnet session. **Disable** – Does not require a login.

Table 4-13. 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 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 (Terminal) 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 4-12, 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 4-13. 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 Management Link. **Enable** – User is prompted for a login ID and password. **Disable** – No login is required for an FTP session.
FTP Max Receive Rate (kbps)
For FrameSaver SLV 9820: Possible Settings: **1 – 128** Default Setting: **128** *For FrameSaver SLV 9820-2M:* Possible Settings: **1 – 2048** Default Setting: **2048** *For FrameSaver SLV 9820-8M:* Possible Settings: **1 – 8192** Default Setting: **8192**
Sets the maximum receive rate of file transfer to the system. 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. *Display Conditions* – This option does not appear for Model 9820-45M, which has a fixed rate. **1 – *maximum receive rate*** – 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 4-14).

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 4-14. 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 and Trap Dial-Out

Select SNMP Traps from the Management and Communication menu to configure SNMP traps and dial-out when a trap is generated (see Table 4-15). Dial-out is not available on the Model 9820-45M.

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 4-15. SNMP Traps and Trap Dial-Out Options (1 of 5)

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 4-15. SNMP Traps and Trap Dial-Out Options (2 of 5)

Initial Route Destination
Possible Settings: **AutoRoute, 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 4-10, Node IP Options). **Modem** – (Model 9820-45M.) Uses the Modem port. This selection is only available when Port Use is set to Net Link (see Table 4-19, Modem Port Options). **Ethernet** – (Model 9820-45M.) Uses the Ethernet port. This selection only appears when the Ethernet port is enabled (see Table 4-16, Ethernet Port Options). **COM** – Uses the COM (Terminal) port. This selection is only available when Port Use is set to Net Link (see Table 4-17, Communication Port Options). ***PVCname*** – Uses the defined management *linkname* (the name given the Management PVC). This selection 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: *Models 9820, 9820-2M, 9820-8M:* **Disable**   *Model 9820-45M:* **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 4-15. SNMP Traps and Trap Dial-Out Options (3 of 5)

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 (Terminal) 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 (Terminal) 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** – (Model 9820-45M.) No linkUp and linkDown 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. **Enable** – Sends trap messages when set thresholds are exceeded. **Disable** – Does not send trap messages when set thresholds are exceeded.

Table 4-15. SNMP Traps and Trap Dial-Out Options (4 of 5)

Trap Dial-Out
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls whether SNMP trap messages initiate a call automatically. If the call cannot be completed and the Call Retry option is set to Enable, the SNMP trap message is held (queued) until the call completes to either the Alarm or alternate directory. *Display Conditions* – This option does not appear for Model 9820-45M. **Enable** – Automatically calls the phone number contained in the Control menu's Modem Call Directories, Directory Number A (Alarm). **Disable** – Automatic calls will not be initiated. Traps sent to the modem are held until a dial-in connection is established.
Trap Disconnect
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the COM port-connected modem disconnects after the SNMP trap message has been sent. This configuration option only applies to modem connections initiated as a result of sending the SNMP trap message. *Display Conditions* – This option does not appear for Model 9820-45M. **Enable** – Disconnects the call after sending an SNMP trap message(s). **Disable** – Does not disconnect the call and holds the line until it is disconnected manually or by the remote modem. This allows the NMS to poll the FrameSaver unit for more information after receiving an SNMP trap.
Call Retry
Possible Settings: **Enable, Disable** Default Setting: **Disable**
If an alternate dial-out directory is specified (see Alternate Dial-Out Directory), the alarm directory's telephone number is called first. If the call cannot be completed, then the alternate directory's telephone number is called (see the Control menu's Modem Call Directories). *Display Conditions* – This option does not appear for Model 9820-45M. **Enable** – Attempts to retry the call, up to one time per SNMP trap message, with a delay between the retry. The delay is specified by the Dial-Out Delay Time (Min) configuration option. **Disable** – Does not retry an incomplete call.
Dial-Out Delay TIme (Min)
Possible Settings: **1 – 10** Default Setting: **5**
Specifies the amount of time between call retries when an SNMP trap message is sent; the wait between call attempts (see Call Retry). *Display Conditions* – This option does not appear for Model 9820-45M. **1 – 10** – Sets the number of minutes for the delay between call retry attempts (inclusive).

Table 4-15. SNMP Traps and Trap Dial-Out Options (5 of 5)

Alternate Dial-Out Directory
Possible Settings: **None, 1 – 5** Default Setting: **None**
Specifies whether an incomplete call (busy, or no answer, etc.) resulting from an attempt to send an SNMP trap message is retried using an alternate telephone number. Up to 5 alternate call directories can be set up, but only one at a time can be used. When Call Retry is enabled, the alarm directory's telephone number is called first. If the call cannot be completed after one additional try, then the specified alternate directory's telephone number is called. *Display Conditions* – This option does not appear for Model 9820-45M. **None** – Does not dial-out using one of the alternate directory telephone numbers. **1 – 5** – Specifies the call directory containing the telephone number to call if a call cannot be completed using the telephone number in the alarm directory (Directory Number A in the Control menu's Modem Call Directories), inclusive.

Configuring the Ethernet Port (Model 9820-45M)

Select Ethernet Port from the Management and Communication menu to display or change the Ethernet port configuration options (see Table 4-16).

Main Menu → Configuration → Management and Communication → Ethernet Port

The Ethernet port is initially disabled. When Interface Status is changed to Enable, the message **`Would you like to set the Node's Default IP Destination to Ethernet?`** appears. Answer **`Yes`** if you intend to access devices through the Ethernet port that are on a different subnet.

Table 4-16. Ethernet Port Options (1 of 2)

Interface Status
Available Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the interface is available for use. **Enable** – The interface is enabled. **Disable** – The interface is disabled. No alarms or traps associated with the Ethernet port will be generated, and any uses of the interface (such as Default IP Destination) are reset to their default values.
IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies a unique IP address for accessing the unit via the Ethernet port. **000.000.000.000 – 223.255.255.255** – Shows the IP address for the Ethernet port, which you can view or edit. The first three digits may not be 127. **Clear** – Clears the IP address for the Ethernet port and fills the 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 needed to access the unit. *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 Ethernet port, which you can view or edit. **Clear** – Clears the subnet mask for the Ethernet 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 4-16. Ethernet Port Options (2 of 2)

Default Gateway Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies an address for packets sent out the Ethernet port that do not have a route. **000.000.000.000 – 223.255.255.255** – Shows the Default Gateway Address, which you can view or edit. The first three digits may not be 127. **Clear** – Clears the Default Gateway Address to 000.000.000.000. Packets without routes are discarded.

Configuring the Communication Port

Select Communication Port from the Management and Communication menu to display or change the COM port (Terminal port on the Model 9820-45M) configuration options (see Table 4-17).

Main Menu → Configuration → Management and Communication → Communication Port

Table 4-17. Communication Port Options (1 of 5)

Port Use
Possible Settings: **Terminal, Net Link** Default Setting: **Terminal**
Assigns a specific use to the COM (Terminal) port. NOTE: If the Default IP Destination is set to COM (see Table 4-10, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. **Terminal** – The COM (Terminal) port is used for the asynchronous terminal connection. **Net Link** – The COM (Terminal) port is the network communications link to the IP network or IP device port. NOTE: If the COM port configured for Net Link is used to connect to an external modem, there is a potential security risk of an unauthorized user gaining access to the NMS or other devices on the LAN for which this device has routing table entries.
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 (Terminal) port in kilobits per second. **9.6 – 115.2 kbps** – Sets the communication port speed. The 57.6 and 115.2 speeds are not available on the Model 9820-45M.
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.

Table 4-17. Communication Port Options (2 of 5)

Parity
Possible Settings: **None, Even, Odd** Default Setting: **None**
Provides a method of checking the accuracy of binary numbers for the COM (Terminal) 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.
Stop Bits
Possible Settings: **1, 2** Default Setting: **1**
Determines the number of stop bits used for the COM (Terminal) 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 (Terminal) 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.

Table 4-17. Communication Port Options (3 of 5)

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 (Terminal) 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.
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).

Table 4-17. Communication Port Options (4 of 5)

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 (Terminal) port. Only in effect when the COM (Terminal) 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 (Terminal) port, which you can view or edit. **Clear** – Clears the IP address for the COM (Terminal) port and fills the address with zeros. For Models 9820, 9820-2M, and 9820-8M, 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 (Terminal) 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 (Terminal) port, which you can view or edit. **Clear** – Clears the subnet mask for the COM (Terminal) 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.
Link Protocol
Possible Settings: **PPP, SLIP** Default Setting: **PPP**
Specifies the link-layer protocol to be used. 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. This option does not appear for Model 9820-45M, for which the Link Protocol is PPP. **PPP** – Point-to-Point Protocol. **SLIP** – Serial-Line Internet Protocol.

Table 4-17. Communication Port Options (5 of 5)

RIP
Possible Settings: **None, Proprietary, 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. **Proprietary** – (Models 9820, 9820-2M, 9820-8M.) A proprietary variant of RIP version 1 is used to communicate routing information only between devices to enable routing of IP traffic. **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 (Terminal) port, configured as the management interface (e.g., Cisco: **`config-t, router RIP, int serial`*`x`*`, IP RIP Receive version 1, ctl-z WR`**). To create this management interface, make sure that Node or COM (Terminal) port IP Information has been set up (*Configuring Node IP Information*).

Configuring the COM Port to Support an External Modem (Models 9820, 9820-2M, 9820-8M)

For all models except Model 9820-45M, 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 4-18).

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

NOTE:

A standard EIA-232-D 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 4-18. External Modem (COM Port) Options (1 of 2)

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.

Table 4-18. External Modem (COM Port) Options (2 of 2)

Alternate IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the Alternate IP Address for the COM port when the alternate phone directory is used. If this configuration option is not configured (i.e., it is zero), the COM port's primary IP Address is used when the alternate telephone directory is used. *Display Conditions* – This option does not appear if External Modem Commands is set to AT. Only in effect when the COM port is configured as a network communication link (Port Use is set to Net Link, see Table 3-15, Communication Port Options). **001.000.000.000 – 223.255.255.255** – Shows the COM port's Alternate IP Address, which you can view or edit. The first byte (i.e., *nnn*.255.255.255) can be any number from 001 through 223, excluding 127. Remaining bytes (i.e., 223.*nnn.nnn.nnn*) can be any number from 000 through 255. Leading zeros are required. **Clear** – Clears the Alternate IP Address for the COM port and fills the address with zeros (i.e., 000.000.000.000).
Alternate Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the Alternate Subnet Mask for the COM port when the alternate phone directory is used. *Display Conditions* – This option does not appear if External Modem Commands is set to AT. Only in effect when the COM port is configured as a network communication link (Port Use is set to Net Link, see Table 4-17, Communication Port Options). **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 (i.e., 000.000.000.000). 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.

Configuring the Modem Port (Model 9820-45M)

Select Modem Port from the Management and Communication menu to display or change the Modem port configuration options (see Table 4-19).

Main Menu → Configuration → Management and Communication → Modem Port

Table 4-19. Modem Port Options (1 of 3)

Port Use
Possible Settings: **Terminal, Net Link** Default Setting: **Terminal**
Assigns a specific use to the Modem port. NOTE: If the Default IP Destination is set to Modem (see Table 4-10, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. **Terminal** – The Modem port is used for the asynchronous terminal connection. **Net Link** – The Modem port is the network communications link to the IP network or IP device port.
Dial-In Access
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether dial-in access to the Modem port is allowed. **Enable** – Dial-in access is permitted. Port Use must be set to Terminal. **Disable** – Dial-in access is not permitted.
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 interface through the Modem 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.

Table 4-19. Modem Port Options (2 of 3)

Port Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies level of user access privilege for the asynchronous terminal interface accessed through the Modem 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.
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).

Table 4-19. Modem Port Options (3 of 3)

IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies a unique IP address for accessing the unit via the Modem port. Only in effect when the Modem 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 Modem port, which you can view or edit. The first three digits may not be 127. **Clear** – Clears the IP address for the Modem port and fills the 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 needed to access the unit. Only in effect when the COM (Terminal) 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 (Terminal) port, which you can view or edit. **Clear** – Clears the subnet mask for the COM (Terminal) 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.

Security and Logins

5

This chapter includes the following:

- *Limiting Access*
- *Controlling Asynchronous Terminal Access*
- *Controlling External COM Port Device Access (Models 9820, 9820-2M, 9820-8M)*
- *Controlling Modem Port Device Access (Model 9820-45M)*
- *Controlling Telnet or FTP Access*
  - *Limiting Telnet Access*
  - *Limiting FTP Access*
  - *Limiting Telnet or FTP Access Over the TS Management Link*
- *Controlling SNMP Access*
  - *Disabling SNMP Access*
  - *Assigning SNMP Community Names and Access Levels*
  - *Limiting SNMP Access Through IP Addresses*
- *Creating a Login*
- *Modifying a Login*
- *Deleting a Login*

Limiting Access

The FrameSaver unit provides access security on the following interfaces:

- Asynchronous (async) terminal
- External devices
- 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

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.

▶ Procedure

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

1. Select the appropriate configuration options screen.

   Main Menu → Configuration → Management and Communication → Communication Port

   or (for Models 9820, 9820-2M, 9820-8M)

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

   or (for Model 9820-45M)

   Main Menu → Configuration → Management and Communication → Modem 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.

3. Save your changes.

See Chapter 4**,** *Configuration Options,* for information about the COM port (Terminal port on the Model 9820-45M), external modem, and Modem port configuration options.

If you inadvertently configure the unit in such a way that communication is no longer possible, see *Resetting the Unit and Restoring Communication* in Chapter 8, *Troubleshooting*.

Controlling External COM Port Device Access (Models 9820, 9820-2M, 9820-8M)

Dial-in access can be controlled on Models 9820, 9820-2M, and 9820-8M when an external device (modem) is connected to the unit's communication (COM) port. The External Device Commands option must be set to AT or Other.

▶ Procedure

To control dial-in access:

1. Select the External Modem options.

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

2. Enable or disable the Dial-In Access configuration option.

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

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 Modem Port Device Access (Model 9820-45M)

Dial-in access through the Modem port can be controlled on the Model 9820-45M.

▶ Procedure

To control dial-in access:

1. Select the Modem Port Options.

   Main Menu → Configuration → Management and Communication → Modem Port

2. Enable or disable the Dial-In Access configuration option.

3. Save your change.

See *Configuring the Modem Port* in Chapter 4**,** *Configuration Options,* for more information about Modem 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. (Models 9820, 9820-2M, 9820-8M.)

▶ 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 (Models 9820, 9820-2M, 9820-8M)	FTP Max Receive 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 Options* 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, 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.

Monitoring

6

This chapter includes the following:

- *Displaying System Information*
- *Front Panel LEDs*
  - *Front Panel Status LEDs*
- *Displaying LEDs and Control Leads*
  - *Display LEDS and Control Leads Screen (Models 9820, 9820-2M, 9820-8M)*
  - *Display LEDs and Control Leads Screen (Model 9820-45M)*
- *Power Module LEDs (Model 9820-45M)*
- *Device Messages*
- *Status Information*
- *System and Test Status Messages*, which includes:
  - *Self-Test Results Messages*
  - *Health and Status Messages*
  - *Test Status Messages*
- *Network LMI-Reported DLCIs Status*
- *PVC Connection Status*
- *Network Interface Status*
- *IP Routing Table (Model 9820-45M)*
- *Performance Statistics*
  - *Clearing Performance Statistics*
  - *Service Level Verification Performance Statistics*
  - *DLCI Performance Statistics*
  - *Frame Relay Performance Statistics*
  - *Ethernet Performance Statistics (Model 9820-45M)*
- *Trap Event Log (Model 9820-45M)*

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 unit installed, referred to as a network access module, or NAM (i.e., DP FR NAM). This card type is supported by the SNMP SysDescr Object.
Serial Number	Unit's 7-character serial number.
Ethernet MAC Address (9820-45M)	Media Access Control (MAC) address assigned to the Ethernet port during manufacturing.
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
Hardware Revision	Unit's hardware version. Format *nnnn-nnx* consists of a 4-digit number, followed by two digits and one alphabetic character.

Front Panel LEDs

The FrameSaver SLV 9820 unit's faceplate includes LEDs (light-emitting diodes) that provide status on the FrameSaver unit, its network data port, and its user data port.

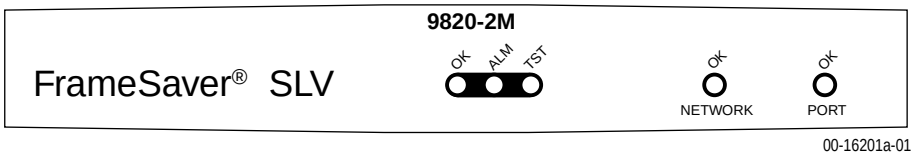


Figure 6-1. Model 9820-2M Front Panel

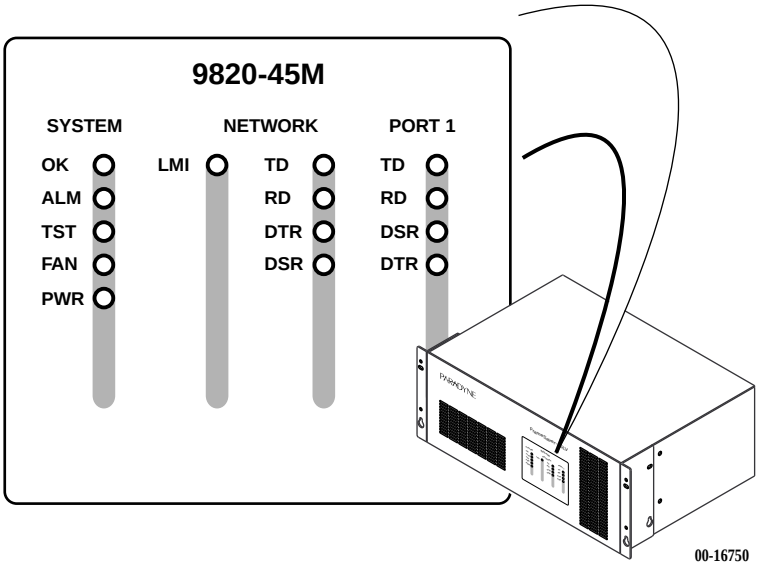


Figure 6-2. Model 9820-45M Front Panel

Front Panel Status LEDs

Table 6-1. System Status LEDs

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. Error/fault/alarm conditions: ■ Clock Out of Range ■ CTS Down ■ DLCI Down ■ DTR Down ■ LMI Down ■ Loss of Signal (LOS) ■ Self-Test Failed ■ SLV Timeout ■ Two Level-1 Users Accessing Device OFF – No failures have been detected. These alarms appear on the System and Test Status screen. See *Health and Status Messages* for additional information.
TST	Test Mode	Yellow	ON – Loopback or test pattern is in progress, initiated locally, remotely, or from the network. OFF – No tests are active.
FAN (9820-45M)	Fan Failure	Yellow	ON – At least one fan has failed and the unit is in danger of overheating. OFF – Fans are operational.
PWR (9820-45M)	Power Failure	Yellow	ON – One of the power supplies has failed and redundant power is no longer available. OFF – Both power supplies are operational, or only one power supply is installed.

Table 6-2. NETWORK Status LEDs

Label	Indication	Color	What It Means
OK	Operational Status	Green	(Models 9820, 9820-2M, 9820-8M) 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 configured to monitor DSR, CTS, or RLSD and the leads are not asserted, or TM is asserted on the DCE, or a valid clock signal cannot be detected on the port.
LMI	LMI OK	Green	(Model 9820-45M) The Local Management Interface is running on the frame relay link on the network interface.
TD	Transmit Data	Green	(Model 9820-45M) Data is being sent or received on the circuit.
RD	Receive Data	Green	
DTR	Data Terminal Ready	Green	(Model 9820-45M) Current state of the control lead.
DSR	Data Set Ready	Green	

Table 6-3. PORT Status LEDs

Label	Indication	Color	What It Means
OK	Operational Status	Green	(Models 9820, 9820-2M, 9820-8M) 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 configured to monitor DTR and/or RTS and the lead(s) is not asserted.
TD	Transmit Data	Green	(Model 9820-45M) Current state of the control lead.
RD	Receive Data	Green	
DTR	Data Terminal Ready	Green	
DSR	Data Set Ready	Green	

Displaying LEDs and Control Leads

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

Main Menu → Status → Display LEDs and Control Leads

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

Display LEDs and Control Leads Screen (Models 9820, 9820-2M, 9820-8M)

Display LEDs & Control Leads Screen (Models 9820, 9820-2M, 9820-8M)

```
main/status/leds                                                    9820-2M
Device Name: Node A                                          5/13/2000 05:01

                        DISPLAY LEDS & CONTROL LEADS

                                 DP FR NAM

          GENERAL        NETWORK1        Port-1
          OK             OK              OK
          Alarm          TXD             TXD
          Test           RXD             RXD
                         RLSD(Ind)       DTR
                         DSR             RTS(Control)
                         CTS
                         TM




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

Table 6-4. General LEDs

Label	Indication	What It Means
OK	Operational Status	The unit has power and is operational.
Alarm	Operational Alarm (Fail)	The unit has just been reset, or an error or fault has been detected.
Test	Test Mode	A test is in progress.

Table 6-5. Network and User Data Port LEDs and Control Leads

Label	Indication	What It Means
Both Network and User Data Ports		
OK	Operational Status	The data port is operational.
TXD	Transmit Data	Data is being sent to the far-end device on the data port.
RXD	Receive Data	Data is being received from the far-end device on the data port.
Additional Network Data Port Control Leads		
RLSD	Receiver Line Signal Detector	If Port Type is set to V.35 or EIA530: Shows the current state of the RLSD control lead. If Port Type is set to X.21: Shows the current state of the Indication interface control lead.
DSR	Data Set Ready	Shows the current state of the DSR control lead. This lead is not used when Port Type is set to X.21.
CTS	Clear to Send	Shows the current state of the CTS control lead. This lead is not used when Port Type is set to X.21.
TM	Test Mode	A test is currently running in the NTU. This lead is not used when Port Type is set to X.21.
Additional User Data Port Control Leads		
DTR	Data Terminal Ready	Shows the current state of the DTR control lead. This lead is not used when Port Type is set to X.21.
RTS	Request to Send	If Port Type is set to V.35 or EIA530: Shows the current state of the RTS control lead. If Port Type is set to X.21: Shows the current state of the Control interface control lead.

See *Configuring the Physical Interfaces* in Chapter 4, *Configuration Options*, for additional information.

Display LEDs and Control Leads Screen (Model 9820-45M)

Display LEDs & Control Leads Screen (Model 9820-45M)

```
main/status/leds                                                    9820-45M
Device Name: Node A                                          5/13/2000 05:02

                        DISPLAY LEDS & CONTROL LEADS

                                 DP FR NAM

          GENERAL        NETWORK1       Port-1
          OK             TD             TD
          Alarm          RD             RD
          Test           DTR            DTR
          Backup         DSR            DSR
          Fan Fail       TM
          Pwr Fail       LMI OK

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

Table 6-6. General LEDs

Label	Indication	What It Means
OK	Operational Status	The unit has power and is operational.
Alarm	Operational Alarm (Fail)	The unit has just been reset, or an error or fault has been detected.
Test	Test Mode	A test is in progress.
Backup	Backup	When flashing, the unit is originating or answering a backup session. When on, a backup link has been established.
Fan Fail	Fan Failure	At least one fan has failed.
Pwr Fail	Power Supply Failure	One of the power modules has failed.

Table 6-7. Network and User Data Port Control Leads

Label	Indication	What It Means
Both Network and User Data Ports		
TD	Transmit Data	Data is being transmitted on the circuit.
RD	Receive Data	Data is being received on the circuit.
DTR	Data Terminal Ready	Shows the current state of the DTR control lead.
DSR	Data Set Ready	Shows the current state of the DSR control lead.
Additional Network Data Port Control Leads		
TM	Test Mode	Shows the current state of the TM interface control lead.
LMI OK	LMI OK	Local Management Interface is running successfully on the frame relay link on the network interface.

See *Configuring the Physical Interfaces* in Chapter 4, *Configuration Options*, for additional information.

Power Module LEDs (Model 9820-45M)

Each power module has a green LED which remains lit while power is applied and the power module is functioning.

When the yellow front panel System PWR LED is lit, one of the power modules has failed. The failed power module can be identified from the back of the DSU by its unlit LED.

Table 6-8. Power Module Troubleshooting

Configuration	Symptom	What to Do (in order, if problem persists)
One Power Module	No front panel LEDs are lit.	1. Verify that the receptacle in use provides 120 Vac. 2. Verify that the power module switch is in the On position. 3. Replace the power module. See *Replacing a Power Module* in Chapter 12, *Hardware Maintenance*. 4. Call your service representative.
Two Power Modules	No front panel LEDs are lit.	1. Verify that the receptacles in use provide 120 Vac. 2. Verify that the power module switches are in the On position. 3. Replace the power modules. See *Replacing a Power Module* in Chapter 12, *Hardware Maintenance*. 4. Call your service representative.
	The front panel System PWR LED is lit.	1. Check the power module LEDs from the back of the unit and replace the failed power module (the one whose LED is off). See *Replacing a Power Module* in Chapter 12, *Hardware Maintenance*. 2. Call your service representative.

Device Messages

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

Table 6-9. Device Messages (1 of 5)

Message	What It Indicates	What To Do
Access level is *n*, Configuration is Read-only.	The user's access level is 2 or 3; the user is not authorized to change configurations.	No action needed.
Already Active	The test selected is already running.	■ Allow test to continue. ■ Select another test. ■ Stop the test.
Cannot Modify TS Management Link	The Management PVC you are attempting to modify is defined as the TS Management Link.	■ No action needed. ■ Modify a different PVC.
Cannot save - no Level 1 Login IDs	You are attempting to save a configuration which has no Level 1 Login ID.	Create a Login ID with an access level of 1, then save the configuration.
Command Complete	Configuration has been saved or all tests have been aborted.	No action needed.
Connection Refused	Two menu-driven user interface sessions are already in use when a Telnet session was attempted.	Wait and try again.
DLCI in connection. Delete connection first	You 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 number entered is a duplicate of an existing DLCI record.	Enter another DLCI number.
DLCI Number Reserved	The number entered is a special excluded DLCI in the product.	Enter another DLCI number.
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*.

Table 6-9. Device Messages (2 of 5)

Message	What It Indicates	What To Do
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*)	An invalid character was entered.	Reenter information using valid printable ASCII 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 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 – Was Already Active	A test was already in progress when it was selected.	No action 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.
IP addresses must be unique	The address entered matches that of another NMS already defined.	Enter a different IP address.
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.

Table 6-9. Device Messages (3 of 5)

Message	What It Indicates	What To Do
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.
Link Inactive	You attempted to start a PVC test on an inactive link.	Activate the link or test a different link.
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 circuits 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 available for connection	New was selected from the PVC Connection Table, but all configured DLCIs have been connected.	■ No action needed. ■ Configure more DLCIs and try again.
	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 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.
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 more PVCs allowed	CreatePVC was selected on the DLCI Records configuration screen, and the maximum numbers of PVCs for the device has already been created.	Delete a PVC, then create the new PVC.
No Security Records to Delete	Delete was selected from the Administer Login screen, and no security records had been defined.	■ No action needed. ■ Enter a security record.

Table 6-9. Device Messages (4 of 5)

Message	What It Indicates	What To Do
Not enough circuits available	A new TS Access DLCI was selected, but the maximum number of network DLCIs or management PVCs has already been created.	Delete a DLCI, then create the new DLCI.
Note: This PVC has been designated as the TS Management Link	The Management PVC you displayed is defined as the TS Management Link.	No action needed. The PVC cannot be modified.
No VCIs available on VPI	All virtual circuits for the VPI have been assigned in other DLCI records or Management PVCs.	Select a different VPI.
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.
Resetting Device, Please Wait ...	Yes (or y) was entered in the *Reset COM Port usage* field of the System Paused menu.	No action needed.

Table 6-9. Device Messages (5 of 5)

Message	What It Indicates	What To Do
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 (Terminal) 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 (Terminal) port is now available.	Log on to the FrameSaver unit.
	Session has been ended due to timeout.	No action needed.
Value Out of Range (*n*–*m*)	The value entered is not within the valid limits of *n* through *m*, inclusive.	Enter a valid value.

Status Information

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

Status Menu

```
main/status                                                          9820-45M
Device Name: Node A                                          5/13/2000  5:03

                                    STATUS


                            System and Test Status
                            LMI Reported DLCIs
                            PVC Connection Status
                            Network Interface Status
                            IP Routing Table   (Model 9820-45M only)
                            Performance Statistics
                            Trap Event Log     (Model 9820-45M only)
                            Display LEDs and Control Leads
                            Identity




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

NOTE:

Status messages contained 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*
- *Health and Status Messages*
- *Test Status Messages*

Self-Test Results Messages

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

Table 6-10. 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.
Last Reset (Model 9820-45M)	Date and time the unit was powered on or reset.	No action needed.
Passed	No problems were found during power-on or reset.	No action needed.

Health and Status Messages

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

Table 6-11. Health and Status Messages (1 of 2)

Message	What It Indicates
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.
Backup Active	(Model 9820-45M) A backup has been established and data is flowing over an alternate DLCI.
Clock Out of Range at Network 1	A valid network data port rate cannot be detected because the: ■ Unit is trying to detect a valid port rate. ■ Rate detected is greater than the highest port rate supported by the unit. – FrameSaver SLV 9820 rates: 56/64 or 128 kbps in 56 or 64 kbps increments – FrameSaver SLV 9820-2M rates: 64 – 2048 kbps in 64 kbps increments – FrameSaver SLV 9820-8M rates: 1024 – 8192 kbps in 8 kbps increments – FrameSaver SLV 9820-45M rates: 1024 – 44210 kbps in 8 kbps increments
CTS down to Port-1 Device	(Models 9820, 9820-2M, 9820-8M) 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.

[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 6-11. Health and Status Messages (2 of 2)

Message	What It Indicates
Ethernet Link Down	(Model 9820-45M) The Ethernet port is administratively enabled, but communication is not possible.
Fan Failure	(Model 9820-45M) At least one fan has failed.
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 Discovery in Progress, *frame relay link* [2]	Local Management Interface protocol discovery is in progress to determine which protocol will be used on the specified frame relay link.
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 data port. Either the control leads on the network data port are deasserted, the TM lead is asserted, or no clock is detected from the NTU.
Network Com Link Down	The communication link for the COM (Terminal) port is down, and the port is configured for Net Link.
Power Supply Failure	(Model 9820-45M) Power supply voltage has dropped below an acceptable level.
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.
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.

[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 6-12. Test Status Messages

Message	What It Indicates
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.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the faceplate to flash on and off.
Monitor *Pttn* Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	The unit is monitoring a test pattern on the specified DLCI on the specified frame relay link.
No Test Active	No tests are currently running.
PVC Loopback Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	A PVC Loopback is active on the specified DLCI on the frame relay link.
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.

[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.

Network LMI-Reported DLCIs Status

Network LMI-reported DLCI statuses are selected from the Status menu.

Main Menu → Status → LMI Reported DLCIs

The LMI Reported DLCIs screen displays the status and CIR (if supported by the switch) for each DLCI, whether the DLCI is configured or not.

LMI-Reported DLCIs Status Screen Example

```
main/status/lmi_dlcis                                                  9820-2M
Device Name: Node A                                          05/13/2000  5:04

                    frame relay link LMI REPORTED DLCIs        Page 1 of 2



    DLCI   STATUS        CIR (bps)            DLCI   STATUS        CIR (bps)
 *   300   Active           16000          *   622   Active           32000
 *   305   Inactive                         *   624   Active           32000
 *   400   Deleted                          *   625   Deleted
 *   410   Inactive                         *   713   Active           32000
     411   Inactive                         *   822   Active           32000
     420   Inactive         32000           * 1002   Active           32000
     430   Active
     501   Inactive
     511   Active          256000
     520   Active           64000

      * – DLCI is configured on the Frame Relay Link.
--------------------------------------------------------------------------------
                                ESC for previous menu        MainMenu   Exit
Refresh   PgUp  PgDn                NextLink     PrevLink
```

An asterisk (*) next to the DLCI indicates that the DLCI has been configured for the link.

DLCIs without an asterisk have not been configured in the unit. These DLCIs pass through the unit transparently, without being monitored and with no demultiplexing/multiplexing of management diagnostics or user data being performed. Only DLCIs on the Net1-FR1 and Port-1 frame relay links appear on this screen; nonconfigured DLCIs on other links are discarded.

Table 6-13. Network LMI-Reported DLCIs Status

Field	Status	What It Indicates
DLCI	16 through 1007	Identifies the Local Management Interface-reported DLCI numbers assigned to the selected interface – the identifying number assigned to the path between two frame relay FrameSaver units' ports. DLCI statuses are listed in ascending order (i.e., lowest number first).
Status	Active Inactive Deleted [1] New [1]	LMI-reported status of the DLCI: ■ Whether the DLCI is active (capable of carrying data) in the frame relay network, ■ Whether it is inactive in the frame relay network, ■ Whether it has been deleted by the frame relay network, or ■ Whether it has been created by the frame relay network.
CIR (bps)	FrameSaver SLV 9820: 0–128000 FrameSaver SLV 9820-2M: 0–2048000 FrameSaver SLV 9820-8M: 0–8192000 FrameSaver SLV 9820-45M: 0–44210000	Displays the committed information rate reported by the Stratacom switch. CIR information only appears in this column when LMI Protocol is set to Standard. If blank, the switch does not support this feature.

[1] Appears for 10 seconds only, before the network changes **`Deleted`** to **`Inactive`** and **`New`** to **`Active`**.

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.

PVC Connection Status Screen Example

```
main/status/connections                                              9820-45M
Device Name: Node A                                          05/13/2000  5:05

                                                                  Page 1 of 2
                          PVC CONNECTION STATUS

        Source          Primary Destination          Alternate Destination
 Link   DLCI  EDLCI  Link     DLCI  EDLCI   Status    LINK    DLCI EDLCI Status

 Port-1 201        Net1-FR1    300    1     Active
 Port-1 202        Net1-FR1   1001    4     Active
 Port-1 100        Net1-FR1   1001    2     Active
 Port-1 204        Net1-FR1   1001    5     Active
 Mgmt PVC Dunedin  Net1-FR1   1001    3     Active
 Port-1 206        Net1-FR1   1001          Active
 Port-1 207        Net1-FR1   1001          Active    west     400      Inactive
 Port-1 208        Net1-FR1    500          Active    west     302      Active
 Port-1 209        Net1-FR1    502          Inactive  west     304      Active
 Port-1 210        Net1-FR1    504          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.

The Alternate Destination columns appear only for the Model 9820-45M.

Table 6-14. 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 – the network data port.
	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.

Table 6-14. PVC Connection Status (2 of 2)

Field	Status	What It Indicates
DLCI	16 to 1007	For standard DLCIs. Identifies an individual link/ connection embedded within a DLCI.
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 selected from the Status menu.

Main Menu → Status → Network Interface Status

Network Interface Status Screen Example

```
main/status/network                                                  9820-45M
Device Name: Node A                                          05/13/2000  5:06


                        NETWORK  1 INTERFACE STATUS

                    Operating Rate (Kbps):       44120









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

Table 6-15. Network Interface Status

Field	Value	What It Indicates
Operating Rate (Kbps)	0–52000	The clock rate detected on the network interface.
	Disconnected	The line is disconnected.

IP Routing Table (Model 9820-45M)

The IP Routing Table display is selected from the Status menu.

Main Menu → Status → IP Routing Table

IP Routing Table Screen Example

```
main/status/connections                                              9820-45M
Device Name: Node A                                          05/13/2000  5:07

                                                                  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  255.255.255.255  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  2  Loc   Modem        999
135.001.220.010  255.255.255.000  135.042.001.254  1  Loc   COM          999
135.001.222.000  255.255.255.000  135.026.001.254  1  RIP   Modem         30
135.001.001.010  255.255.255.255  135.026.001.254  1  RIP   PVCMgmt1003   30
135.001.001.011  255.255.255.255  135.026.001.254  1  NMS   PVCMgmt1004    2
135.001.001.012  255.255.255.255  135.026.001.254  1  NMS   PVCMgmt1005   48
135.001.001.013  255.255.255.255  135.026.001.254  1  NMS   PVCMgmt1006   21


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

Table 6-16. IP Routing Table (1 of 2)

Field	What It Indicates
Destination	The IP address of the route.
Mask	The subnet mask of the route.
Gateway	The network gateway IP address for the route.
Hop	The number of hops to the destination for the route.
Type	The method that was used to add the route: **RIP** – The route was discovered through RIP. **Loc** – The route was added as part of the unit's configuration. **NMS** – The route was added by an NMS using SNMP. **Tmp** – The route was added as a temporary route to answer an IP packet that was received. The route is deleted when its TTL expires or when the unit is reset. **–** (Hyphen) – The source of the route is not maintained in the table.

Table 6-16. IP Routing Table (2 of 2)

Field	What It Indicates
Interface	The interface used to get to the destination: **COM** – The COM (Terminal) port is used. **Modem** – The Modem port is used. **Ethernet** – The Ethernet port is used. **PVC*name*** – The specified management PVC is used. **Internal** – An internal route is used (for loopbacks or internal functions).
TTL	Time To Live, in seconds. TTL can have a value 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                                          9820-45M
Device Name: Node A                                      5/13/2000  5:08

                            PERFORMANCE STATISTICS


                            Service Level Verification
                            DLCI
                            Frame Relay
                            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 ClrStats function key to reset the Ethernet performance statistics.

  Performance Statistics → Ethernet

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.

Table 6-17. 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.
■ Above EIR	■ The number of frames transmitted by the far-end device that were above the excess information rate and were dropped in transit.

Table 6-17. Service Level Verification Performance Statistics (2 of 2)

Statistic	What It Indicates
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.

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, Frame Relay Delivery Ratio (FDR), and Data Delivery Ratio (DDR) 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

Table 6-18. DLCI Performance Statistics (1 of 2)

Statistic	What It Indicates
DLCI Up Since [1]	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 [1]	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 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 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 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.

[1] Only appears for the network interface.

Table 6-18. 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.

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 6-19. Frame Relay Performance Statistics (1 of 3)

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 forward 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.

Table 6-19. Frame Relay Performance Statistics (2 of 3)

Statistic	What It Indicates
Frame Relay Errors *(cont'd)*	
Short Rx Frames	The number of frames received over the Network or Port-1 interface that were less than 5-octets (five 8-bit bytes) in length. There may be 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.
Invalid DLCI	The number of frames received over the interface that were addressed to DLCIs outside the valid range; that is, a number less than 16 or greater than 1007. The device on the far end of the circuit may have been configured incorrectly, or the DLCIs configured for the FrameSaver unit may not match the DLCIs supplied by the service provider.
Unknown DLCI	The number of frames received over the interface that were addressed to unknown DLCIs. The DLCI may not have been configured, or it has been configured to be Inactive. Indicates that the FrameSaver units or devices at both or either end of the circuit have been configured incorrectly.
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.

Table 6-19. Frame Relay Performance Statistics (3 of 3)

Statistic	What It Indicates
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 Overruns	The number of receiver overruns (too many bits) on the interface.
Rx Non-Octet Frames	The number of non-octet frames received on the interface.
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.
Tx Underruns	The number of transmitter underruns (too few bits) on the interface.

Ethernet Performance Statistics (Model 9820-45M)

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

Main Menu → Status → Performance Statistics → Ethernet

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

Table 6-20. Frame Relay Performance Statistics

Field or Statistic	What It Indicates
Port Rate (Mbps)	The operating rate detected on the Ethernet interface. One of: **10** – The Ethernet port rate is 10 Mbps. **100** – The Ethernet port rate is 100 Mbps. **Disabled** – The Ethernet interface was disabled after this screen was first displayed.
Duplex	The duplexing mode of the Ethernet port. One of: **Full** – The Ethernet port is operating in full duplex (4-wire) mode. **Half** – The Ethernet port is operating in half duplex (2-wire) mode. **Disabled** – The Ethernet interface was disabled after this screen was first displayed.
Frames Transmitted	The number of frames transmitted over the interface.
Frames Received	The number of frames received over the interface.
Errored Frames	The number of frames with internal transmit and receive errors, transmitter and receiver overruns, receive checksum errors, alignment errors, and long frame errors.
Excessive Collisions	The number of frames for which transmission failed due to excessive collisions.
Carrier Sense Errors	The number of times the lack of carrier caused an error in transmission.
Deferred Transmissions	The number of frames whose transmission was delayed because the medium was busy.

Trap Event Log (Model 9820-45M)

The Trap Event Log display is selected from the Status menu.

Main Menu → Status → Trap Event Log

Trap Event Log Screen Example

```
main/status/connections                                              9820-45M
Device Name: Node A                                          05/13/2000  5:09

                              TRAP EVENT LOG
                                                    Total Trap Events:    3
 Time Elapsed
 Since Event                          Event
  0d 09:01:32 DLCI 101 of Sync Data Port S01P1 frame relay link “Port-1” up.
  1d 22:21:19 Unit Reset.
  1d 22:25:01 Primary Clock Failed.









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

Table 6-21. Trap Event Log

Field	What It Indicates
Total Trap Events	The number of entries in the log.
Time Elapsed Since Event	The number of days, hours, minutes, and seconds since the specified event occurred.
Event	The trap text string, up to 255 characters.

FTP Operation

7

This chapter includes the following:

- *FTP File Transfer*
  - *Upgrading System Software*
  - *Determining Whether a Download is Completed*
  - *Changing Software*
  - *Transferring Collected Data*

FTP File Transfer

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 (Terminal) 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.

FrameSaver SLV 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 (Terminal) port if Port Use is set to Net Link (see Table 4-17, 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, *Monitoring*, 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. For Models 9820, 9820-2M, and 9820-8M, the rate at which the data file is transferred is the rate set by the FTP Max Receive Rate (Kbps) option (see Table 4-13, Telnet and FTP Session Options in Chapter 4, *Configuration Options*). For Model 9820-45M, the rate is fixed.

NOTE:

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	■ 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. ■ Perform a **get** of the **lmitrace.syc** file. One of the following responses appears: – **`File Transfer Complete`** – **`File Transfer Failed`** – **`Permission Denied`** – The LMI Packet Capture data was not readable, or was a null file. Stop the LMI Packet Capture Utility and try again.

5. Close the FTP session.

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

Troubleshooting

8

This chapter includes the following:

- *Problem Indicators*
- *Resetting the Unit and Restoring Communication*
  - *Resetting the Unit from the Control Menu*
  - *Resetting the Unit By Cycling the Power*
  - *Restoring Communication with an Improperly Configured Unit*
- *Troubleshooting Management Link Feature*
- *LMI Packet Capture Utility Feature*
  - *Viewing Captured Packets from the Menu-Driven User Interface*
- *Alarms*
- *Troubleshooting Tables*
  - *Device Problems*
  - *Frame Relay PVC Problems*
- *Tests Available*
  - *Test Timeout Feature*
- *Starting and Stopping a Test*
  - *Aborting All Tests*
- *PVC Tests*
  - *Network or Port (Internal) PVC Loopback*
  - *Send Pattern*
  - *Monitor Pattern*
  - *Connectivity*

- *Physical Tests*
  - *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	*Displaying LEDs and Control Leads* and *Front Panel LEDs* in Chapter 6, *Monitoring*, 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, *Monitoring*. *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, *Monitoring*, 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 (Terminal) 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

Cycling the power resets the unit. This is an emergency procedure that should be executed only if the Control menu is inaccessible, and never be executed while the unit is in use.

- **Models 9820, 9820-2M and 9820-8M:** Disconnect then reconnect the power cord.
- **Model 9820-45M:** Switch off both power supplies then switch on both power supplies.

Restoring Communication with an Improperly Configured Unit

Configuring the unit improperly can 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 (Terminal) 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 (Terminal) 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 Operations*, 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                              9820-2M
Device Name: Node A                                          5/13/2000  6:01

                              LMI TRACE LOG                    Page 1 of 3

Packets Transmitted to Net1-FR!        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
Clock Out of Range at Network	A valid port rate cannot be detected because the: ■ Unit is auto-rating on the network data port, trying to detect a valid port rate. ■ Rate detected is greater than the highest port rate supported by the unit. – FrameSaver SLV 9820 rates: 64 or 128 kbps – FrameSaver SLV 9820-2M rates: 64 – 2048 kbps in 64 kbps increments – FrameSaver SLV 9820-8M rates: 1024 – 8192 kbps in 8 kbps increments – FrameSaver SLV 9820-45M rates: 1024 – 144210 kbps in 8 kbps increments	If the message continues to appear: ■ Check that the DCE is connected to the network data port, and that the cable is securely attached at both ends. ■ Confirm that there is a valid clock on the cable. ■ Manually configure the NTU for a rate supported by the FrameSaver unit. ■ If necessary, replace the FrameSaver unit with a higher speed FrameSaver unit capable of supporting the NTU clock rate.
CTS down to Port-1 Device (Models 9820, 9820-2M, 9820-8M)	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.

[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 data port, 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
DTR Down from Port-1 Device	The DTR control lead on the device connected to Port-*n* is off.	Examine the attached DTE and cable connected to the FrameSaver unit's port. ■ Check that the Port-1 cable is securely attached at both ends. ■ Check the status of the attached equipment.
Fan Failure (9820-45M)	One of the fans has failed.	Notify your service representative. Have the fan assembly replaced as soon as possible. See *Replacing the Front Panel Assembly* in Chapter 12, *Hardware Maintenance (9820-45M)*.

Table 8-1. Alarm Conditions (3 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 data port: ■ 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.
		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.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network data port, 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
LOS at Network 1	A Loss of Signal (LOS) condition is detected. Either the control leads on the network data port are deasserted, the TM lead is asserted, or no clock is detected from the NTU. ■ Network cable problem. ■ No signal is being transmitted at the far-end FrameSaver unit. ■ NTU or network facility problem.	■ Check that the network cable is securely attached at both ends. ■ Contact your network provider.
Power Supply Failure (9820-45M)	The power supply output voltage has dropped below the specified tolerance level.	Notify your service representative. See *Replacing a Power Module* in Chapter 12, *Hardware Maintenance (9820-45M)*.
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. 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.
Two Level-1 Users Accessing Device	Two users with Level 1 security access are in session with the device.	Alert the other user before starting tests or altering configuration options.
Yellow at Network 1 (9820-45M)	A yellow alarm signal is received on the network. ■ Cable problem. ■ T3 facility problem.	■ Check that the associated cables are securely attached. ■ 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 data port, Network 1.

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

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. The 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).
Cannot access the FrameSaver unit or the menu-driven user interface.	Login or password is incorrect, COM (Terminal) port is misconfigured, or the FrameSaver unit is otherwise configured so it prevents access.	■ Reset the FrameSaver unit (*Main Menu* → *Control* → *Reset Device)*. ■ Contact your service representative.

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

Symptom	Possible Cause	Solutions
Failure *xxxxxxxx* appears at the top of the System and Test Status screen, at Self-Test Results.	The unit detects 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.

Frame Relay PVC Problems

Table 8-3. 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 PVC Connection Status 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.	CIR and Excess Burst Size are inadequate for the throughput required.	Verify the configured Network PVC settings, then increase the settings, as needed, or decrease throughput on the PVC.
	Frame relay network is experiencing problems.	Run PVC Loopback and Pattern tests to isolate the problem, then contact the service provider.
`Out of Sync` message.	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 SLV 9820 model.

Test Menu Example

```
main/test                                                          9820-2M
Device Name: Node A                                        5/13/2000  6:02

                                    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
```

PVC Tests menu selections are suppressed 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 5.*x* management solution using its 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*).

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 test:

1. Follow this menu selection sequence:

   Main Menu → *Test*

2. Select an interface to be tested (Network or Data Port PVC Tests, or Data Port Physical Tests) and press Enter.

   The selected test screen appears. **`Start`** appears in the Command column. **`Inactive`** appears in the Status column.

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

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

4. 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.

5. Press Enter to stop the test.

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

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

Aborting All Tests

Use the Abort All Tests selection from the Test menu to abort all tests running on all interfaces, 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.

- 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                                                  9820-2M
Device Name: Node A                                          5/13/2000  6:03

                                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:

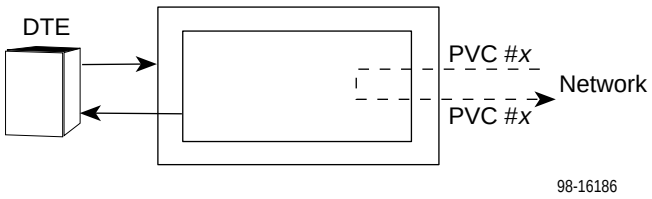
Errors encountered during these tests may be caused by mismatched CIRs in the two FrameSaver devices. If errors are detected, verify the CIR configuration and retest.

Network or Port (Internal) 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.

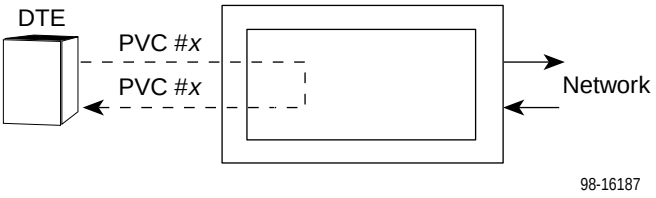
Main Menu → Test → Network PVC Tests → PVC Loopback

Network PVC Loopback



Main Menu → Test → Data Port PVC Tests → PVC Loopback

Port PVC Loopback



Send Pattern

This test sends frames filled with a hexadecimal 55 test pattern and sequence number over the selected interface on a per-DLCI basis.

To send a pattern test on a link:

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

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] → Monitor Pattern

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

The Connectivity test is only available for multiplexed DLCIs.

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

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

Selecting Connectivity sends a frame to the FrameSaver device 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 device 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.

Physical Tests

Physical Tests can be commanded for the user data port.

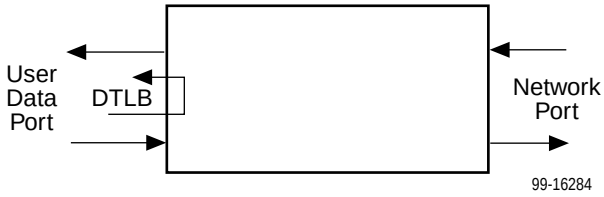
CAUTION:

You should not run these tests with frame relay equipment attached; you must disconnect the frame relay equipment and use external test equipment.

DTE Loopback

The DTE external Loopback (DTLB) test loops the received signal on a user data port back to the DTE. Use this test for isolating problems on the user data port.

An attached device or test equipment must generate data to be looped back.



CAUTION:

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

To start and stop a DTE Loopback, follow this menu selection sequence:

Main Menu → Test → Data Port Physical Tests

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

IP Ping Test

An IP Ping test can be run to test connectivity between the FrameSaver unit and any FrameSaver device, router, or NMS to which it has a route.

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

- To test connectivity between the FrameSaver unit and any FrameSaver device in the network to verify that the path is operational. Select Procedure 1 to ping any far-end FrameSaver device.
- To verify the entire path between a newly installed remote site FrameSaver device 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 device 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 device 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 device:

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 device has just initialized, it may take about a minute for the devices to learn the routes via the proprietary RIP.

3. Verify the results of the IP Ping test.

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

   — When the test is finished, **`Alive. 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*
- *Setting Up the OpenLane SLM System*
- *Setting Up FrameSaver SLV Support*

OpenLane Support of FrameSaver Devices

Paradyne's OpenLane Service Level Management (SLM) system supports all FrameSaver and FrameSaver SLV devices with 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
- On-demand polling of FrameSaver devices
- Web-based diagnostic tests: end-to-end, PVC loopbacks, connectivity, and physical interface tests
- Basic device configuration
- Automatic SLV device and PVC discovery of SLV devices with their SLV Delivery Ratio configuration option enabled
- Easy firmware downloads to an entire network or parts of the network
- Device reset capability
- HP OpenView adapters for integrating OpenLane with the OpenView Web interface

Setting Up the OpenLane SLM System

Instructions for installing Paradyne's OpenLane Service Level Management (SLM) System can be 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 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 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.

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

Setting Up NetScout Manager Plus for FrameSaver Devices

10

This chapter includes NetScout Manager Plus information as it relates to FrameSaver SLV devices. It includes the following:

- *Getting Started*
- *Configuring NetScout Manager Plus*
  - *Adding FrameSaver SLV Units to the NetScout Manager Plus Network*
  - *Verifying Domains and Groups (Models 9820 and 9820-2M)*
  - *Correcting Domains and Groups (Models 9820 and 9820-2M)*
  - *Adding SLV Alarms Using a Template*
  - *Editing Alarms*
  - *Adding SLV Alarms Manually*
  - *Creating History Files*
  - *Installing the User-Defined History Files*
- *Monitoring a DLCI's History Data*
- *Monitoring the Agent Using NetScout Manager Plus (Models 9820 and 9820-2M)*
- *Statistical Windows Supported (Models 9820 and 9820-2M)*

Release 5.5 or higher of the NetScout Manager Plus software provides FrameSaver SLV-specific support.

Getting Started

Before configuring NetScout Manager Plus, you need to copy some OpenLane directories to a NetScout Manager Plus user directory. OpenLane provides these directories as a starting point for loading new alarms and creating history files. A template of alarms and values for configuring alarms and several templates for creating history files specific to the FrameSaver unit are available.

OpenLane paradyne directories include the following:

- **Properties:**
  `paradyne.fsd` file found in **`OpenLane/netscout/alarms/directory`**
- **Properties:**
  `paradyne.fst` file found in **`OpenLane/netscout/alarms/directory`**
- **Alarms:**
  `slvtemplate.fct` file found in
  `OpenLane/netscout/alarms/directory`
- **User history:**
  `pd*.udh` files found in **`OpenLane/netscout/userHistory/directory`**

These files should be moved to **`$NSHOME/usr`** so they can be used.

See *Adding SLV Alarms Using a Template* and *Creating History Files* for additional information.

Configuring NetScout Manager Plus

For the NetScout Manager Plus main window to appear, make sure your environment is set up exactly as specified in your NetScout Readme file.

You need to:

- Copy the OpenLane directory to a user directory.
- Add frame relay agents to the NetScout Manager.

In addition, for Models 9820 and 9820-2M you need to:

- Configure agent properties.
- Verify and correct domains and groups.
- Monitor the agent and DLCIs.

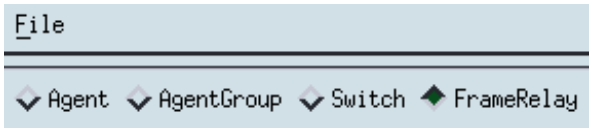
Refer to the NetScout documentation for additional information about accessing and managing the FrameSaver SLV unit through NetScout Manager Plus, refer to the:

- *NetScout Manager/Plus User Guide* to help you install the application, monitor traffic, and diagnose emerging problems on network segments.
- *NetScout Manager/Plus & NetScout Server Administrator Guide* to help you configure agents, remote servers, and report templates using the various NetScout products.
- *NetScout Probe User Guide* to help you install the NetScout Probe between the FrameSaver unit and its router, and configure the probe on network segments you want to monitor.

Adding FrameSaver SLV Units to the NetScout Manager Plus Network

▶ Procedure

1. Bring up the NetScout Manager Plus main window.
2. Select the FrameRelay radio button from the agent type selection bar (on the left side of the window).



   A list of configured frame relay agents appear in the list box below the Name and IP Address headings. If this is a new NetScout Manager Plus installation, the list box below the selection bar is blank since no agents are configured yet.

3. Select the Admin radio button from the application selection bar (to the far right of the screen). Applicable configuration and administration icons appear in the box below the application bar.

4. Click on the Config Manager icon to open the Configuration Manager main window.
5. Select the Add... button (down the center of the screen).
6. Minimally, enter the following:
   - — Agent name
   - — IP address
   - — Properties File: Select paradyne.
7. Select the OK button at the bottom of the screen to add the agent, discover its DLCIs, and return to the Configuration Manager main window.

   The frame relay agent just entered appears in the agent list box, with its DLCIs in the DLCI list box at the bottom of the screen.

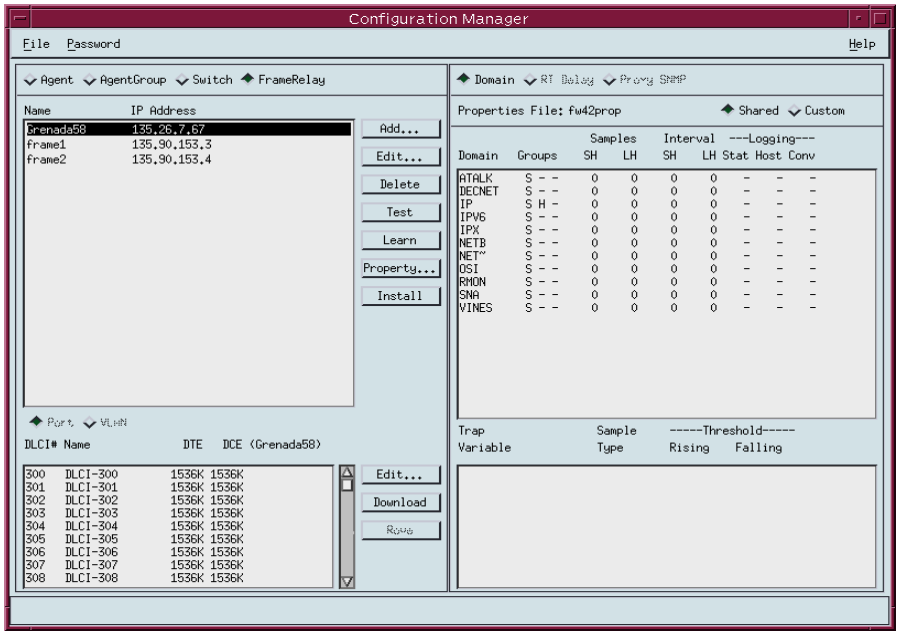
8. Select the Test button (fourth button down, center of the screen) to make sure you can communicate with the agent.

Refer to *Adding Frame Relay Agents* in the *NetScout Manager/Plus & NetScout Server Administrator Guide* for additional information.

Verifying Domains and Groups (Models 9820 and 9820-2M)

▶ Procedure

1. From the NetScout Manager Plus main window, with the FrameRelay and Admin radio buttons still selected, click on the Config Manager icon to open the Configuration Manager main window.



2. Verify that only FrameSaver SLV-supported domains appear listed in the Domain column. FrameSaver SLV-supported domains include:

— ATALK	— IPX	— RMON
— DECNET	— NETB	— SNA
— IP	— NET~	— VINES
— IPV6	— OSI	

3. Verify that:

   — S (statistics collection) appears for each domain listed in the Group column.

   — H (hosts) appears for the IP domain only.

   — Dashes occupy all other positions under the Group column.

   — Zeros appear under the Samples and Interval SH and LH columns.

   — Dashes appear under all Logging columns: Stat, Host, Conv.

4. If all these requirements are met, no further action is required. Close the Configuration Manager window.

   If all these requirements are not met, a FrameSaver SLV-supported domain needs to be added, or if an unsupported domain needs to be deleted, the Properties File must be edited.

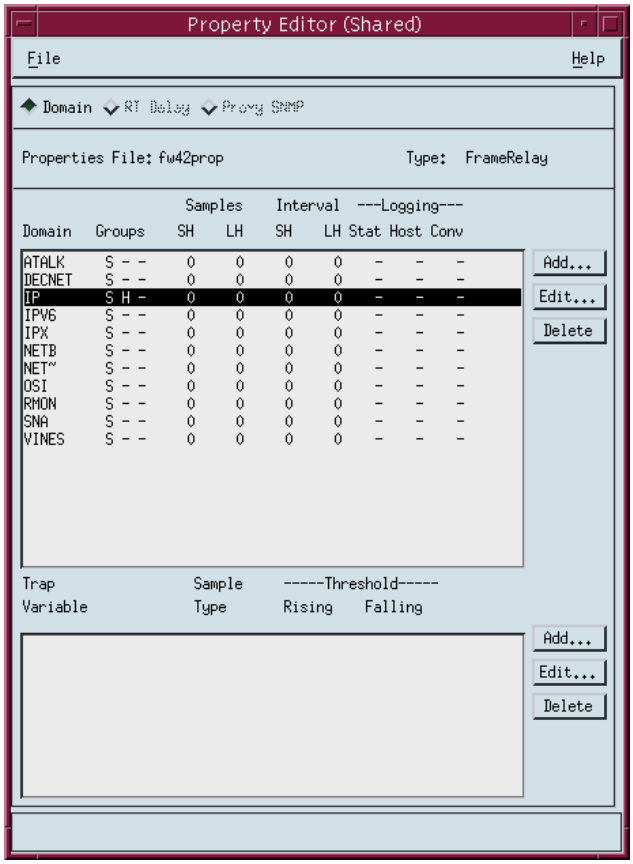
Correcting Domains and Groups (Models 9820 and 9820-2M)

Properties need to be edited when not using the Paradyne-provided file and when:

- An unsupported domain needs to be deleted.
- A missing domain needs to be added.
- Groups, Samples, Interval, and Logging are not configured as specified in Step 3 of *Verifying Domains and Groups*.

▶ Procedure

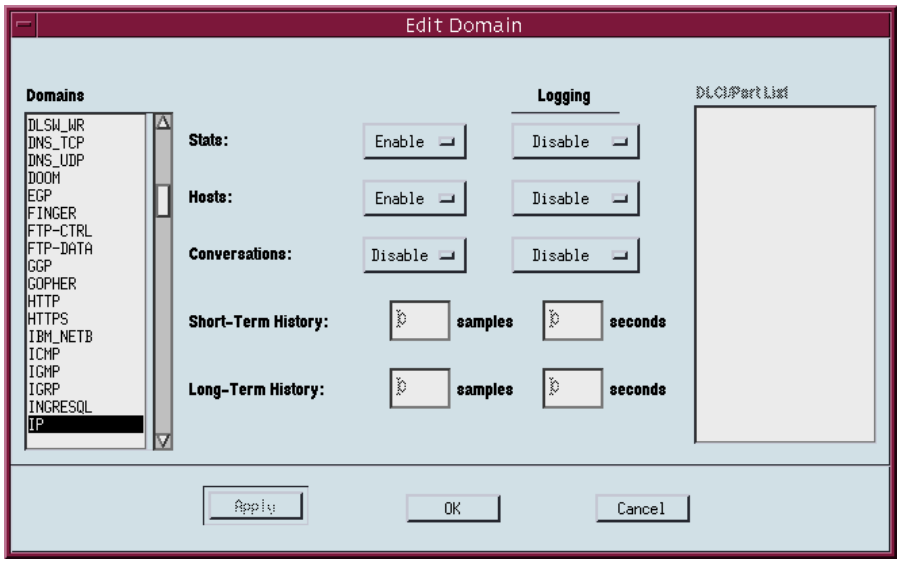
1. Select the the Property... button (down the center of the Configuration Manager main window). The Property Editor window opens.



2. To delete an unsupported domain, click on the domain from the Domains list, then select the Delete button.

   The **`Are you sure?`** prompt appears. Select Yes. The unsupported domain disappears from the list.

3. To add a FrameSaver SLV-supported domain or correct property settings, select the Edit... button (to the right of the Domain section of the Property Editor window). The Edit Domain window opens.



4. Click on the domain from the Domains list and configure the following:

Property		Description	Setting
Groups	Stats (S)	Statistics collection	Enabled for all domains.
	Hosts (H)	Level 3 information (network)	Enabled for IP domain only. Disabled for all other domains.
	Conversations (C)	Protocols being used	Disabled for all domains.
Logging		Event logging	Disabled for all domains and groups.

5. Select the OK button (at the bottom of the screen) to apply the changes.

Refer to *Configuring Domains in Properties Files* in the *NetScout Manager/Plus & NetScout Server Administrator Guide* for additional information.

Adding SLV Alarms Using a Template

Once DLCIs have been discovered, SLV alarms should be configured and assigned to each DLCI. OpenLane provides a template for configuring alarms. DLCI alarms can be configured manually, but using the Paradyne alarm defaults template greatly reduces configuration time.

The following alarms are configured for each DLCI included in the Paradyne MIB:

- Frames Sent (SLVFramesSnt)
- Tx CIR Utilization (SLVTxCIRUtil)
- Tx DLCI Utilization (SLVTxDLCIUtil)
- Frames Received (SLVFramesRec)
- Rx DLCI Utilization (SLVrxDLCIUtil)
- Frames Sent Above CIR (SLVFramesTxAbvCIR)
- Average Latency (AverageLatency)
- Current Latency (CurrentLatency)

These alarms and current values can be found in $NSHOME/usr/slvtemplate.fct, which is used as a starting point for loading new alarms. This file can be copied and edited so the alarm threshold values match service level agreement values. The copied .fct file can then be used to replicate alarm threshold values for all DLCIs on the unit using the eztrap utility. All .fct files must be in $NSHOME/usr.

To configure alarms manually, see *Adding SLV Alarms Manually*.

NOTE:

Perl must be installed in your system to use the eztrap utility in the procedure below. If you have an NT system, please install Perl before proceeding.

▶ Procedure

1. Open a terminal window and go to **$NSHOME/usr**.
2. Type **eztrap -i** *filename***.fct -o** *agentname***.fct** *agentname* and press Enter to run the eztrap utility to create alarm threshold values across all DLCIs for the copied .fct file.

   The message **`eztrap done`** appears when the .fct file is transferred.
3. From the NetScout Manager Plus main window, with the FrameRelay and Admin radio buttons still selected, click on the Config Manager icon to open the Configuration Manager main window.
4. Edit any alarm values that need to be changed.
5. Select the Install button (down the center of the Configuration Manager main window) to load alarms for the unit. This may take some time, so please be patient.

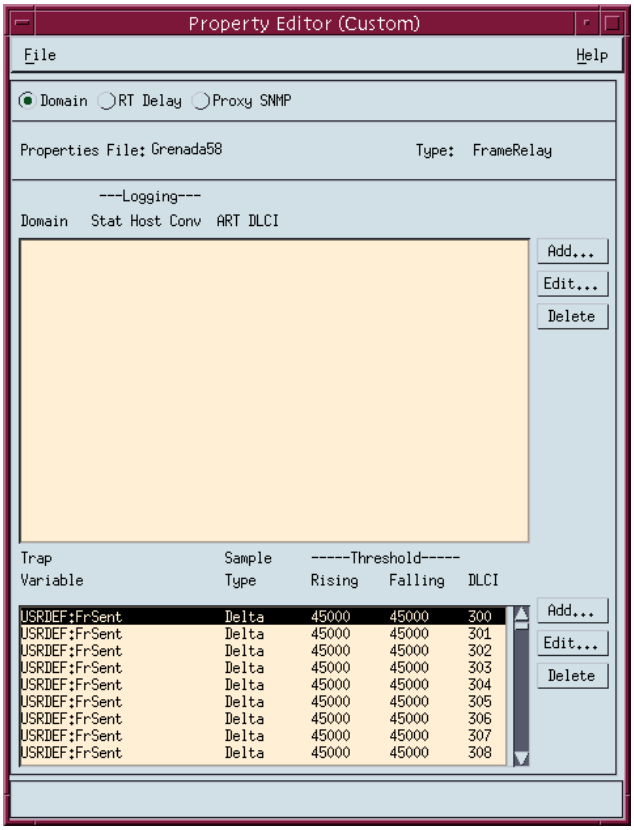
See *Editing Alarms* if any default settings need to be changed.

Editing Alarms

▶ Procedure

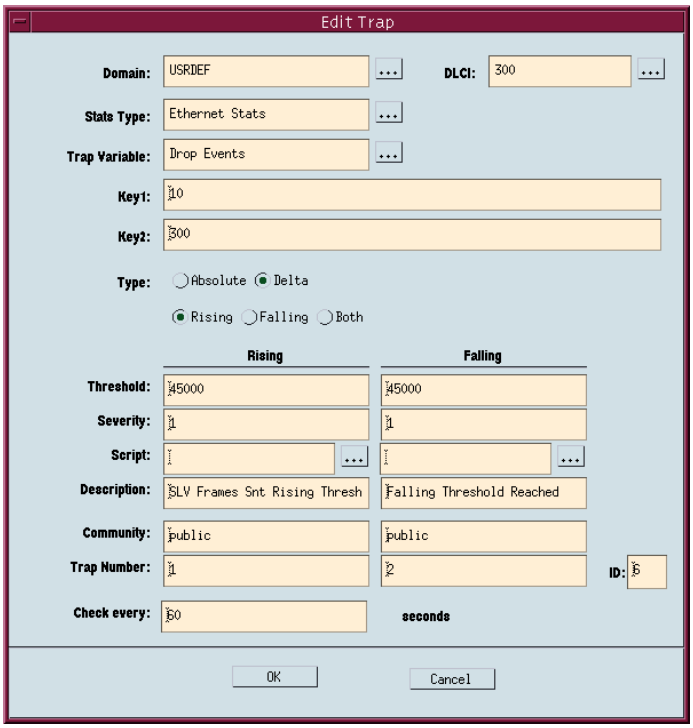
1. From the NetScout Manager Plus main window, with the FrameRelay and Admin radio buttons still selected, click on the Config Manager icon to open the Configuration Manager main window.
2. Select the Custom radio button from the Properties File area (in the upper right of the window), then Property... (down the center of the screen).

   The Custom Property Editor window opens.



3. Select a DLCI from the Trap list, and select the Edit... button (to the right of the list).

   The Edit Trap window opens.



4. Edit any trap defaults that may be required. See Step 4 of *Adding SLV Alarms Manually* for field settings you may want to change.
5. Select the OK button (at the bottom of the screen) to apply your changes. The window closes and the Configuration Manager main window reappears.
6. Select the Install button (down the center of the Configuration Manager main window) to apply your changes.

Refer to *Editing Alarms* in the *NetScout Manager/Plus & NetScout Server Administrator Guide* to change alarm thresholds.

Adding SLV Alarms Manually

Once DLCIs have been discovered, SLV alarms should be defined and assigned to each DLCI.

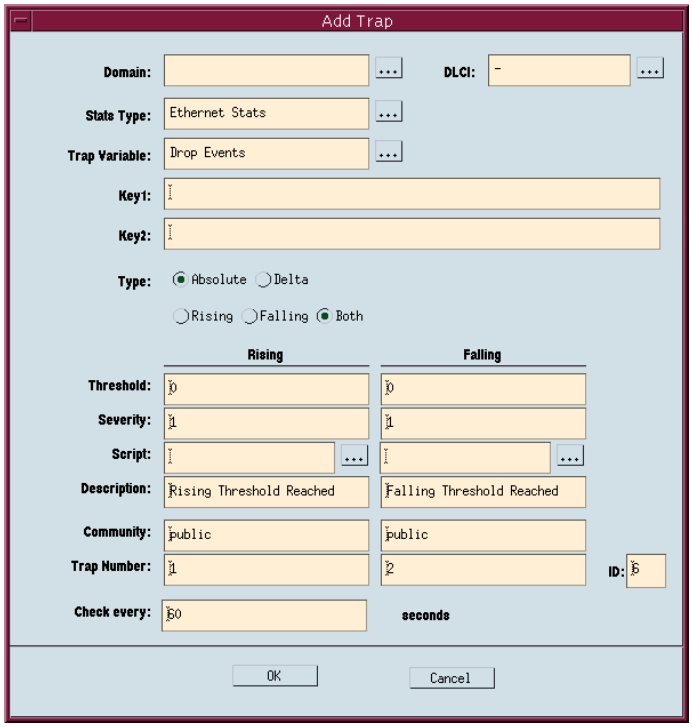
When configuring alarms manually, every alarm must be configured for each DLCI; that is, if there are eight alarms and 20 DLCIs, 160 trap configurations must be created (8 x 20). For this reason, it is recommended that the OpenLane defaults be used. Follow the procedure below to configure alarms manually.

To load OpenLane default settings for alarms, see *Adding SLV Alarms Using a Template*.

▶ Procedure

1. From the NetScout Manager Plus main window, with the FrameRelay and Admin radio buttons still selected, click on the Config Manager icon to open the Configuration Manager main window.
2. Select the Custom radio button from the Properties File area (in the upper right of the window), then Property... (down the center of the screen).

   The Custom Property Editor window opens (see the window in *Editing Alarms*).
3. Select a DLCI from the Trap list, and select the Add... button (to the right of the list). The Add Trap window opens.



4. Click on the ... button to the right of indicated fields for a drop-down list from which selections can be made. Minimally, configure the following fields:

Field	**Select or Enter . . .**
Domain	User Defined
DLCI	DLCI number for trap being assigned
Stats Type	PARADYNE
Trap Variable	Trap variable to be configured
Key1	The ifIndex for the frame relay logical interface is 1
Key2	DLCI number (same as DLCI above)
Type	Absolute or Delta radio button [1] Rising, Falling, or Both radio button [2]
Threshold	Value that will trigger a trap.
[1] Latency MIB variables should be Absolute; all others should be Delta. [2] Generally, Rising is selected.	

5. Select the OK button (at the bottom of the screen) to add this alarm.
6. Repeat Steps 3 through 5 until all traps are configured for all DLCIs.

Refer to *Configuring Alarms in* the *NetScout Manager/Plus & NetScout Server Administrator Guide* for additional information.

Creating History Files

Up to 14 additional user history tables can be created in the FrameSaver unit for each interface. An interface is a specific DLCI or the entire frame relay interface. A table must be created for each DLCI or frame relay link to be monitored. Additional user history tables are created using the command-line prompt in NetScout Manager Plus to load a file that contains the OIDs (Object IDs) to be monitored into the unit.

OpenLane provides several useful examples, including three files containing a complete set of OIDs appropriate to the interface to be monitored: one for a DLCI, one for a frame relay link, and one containing system-type OIDs. Any of these files can be used as a template when creating customized history files specific to the FrameSaver unit.

These files have a **`pdn*.udh`** (user-defined history) format and are found in the **`OpenLane/netscout/userHistory`** directory. The userHistory files should be moved to **`$NSHOME/usr`** so they can be used.

A separate *.udh file must be created and loaded for each DLCI or link that will be monitored before a customized user history table can be loaded. Use a text editor to create these *.udh files by:

- Copying one of the interface-specific files (DLCI or link) and editing it using one of the examples provided as a guide.
- Copying one of the examples provided and editing the extensions to fit the FrameSaver unit.

CAUTION:

Two user history table files are already configured and installed in the unit, UserHistory1 and UserHistory2. These files must not be modified. These two tables are used to keep SLV data for reports.

It is always a good idea to rediscover agents and their DLCIs before starting to be sure your agent and DLCI lists are current. To rediscover agents and their DLCIs, select the Learn button on the NetScout Manager Plus main window (the FrameRelay and Admin radio buttons still selected).

▶ Procedure

1. Open a terminal window and go to **$NSHOME/usr**.
2. Copy an example or interface-specific file to a new file that contains the user history table number.
3. Open the new file using a text editor.

   The variables in the file are listed with their OIDs (Object IDs). The frame relay interface number 101016002 must replace @IFN, and the DLCI number to be monitored must replace @DLCI.

   Example: frCircuitSentFrames
   Change "**`1.3.6.1.2.1.10.32.2.1.6.@IFN.@DLCI`**"
   to "**`1.3.6.1.2.1.10.32.2.1.6.101016002.301`**"

   The only valid interface number for a FrameSaver 9820 model is 101016002.
4. Edit the new file, as needed.

Refer to *Creating .UDH Files* and *Using Custom History* in the *NetScout Manager Plus User Guide* for additional information.

See Appendix B, *SNMP MIBs and Traps, and RMON Alarm Default*, for OID information for an interface.

Installing the User-Defined History Files

Once the user-defined history files have been created, the files need to be installed. History files are installed from the command-line prompt in NetScout Manager Plus. Should the FrameSaver unit be reset, these files will need to be reinstalled. The command used to install a new user history table is located in $NSHOME/bin.

CAUTION:

Do not use user_history_table_1 or 2. UserHistory1 and UserHistory2 are the default user history files used to keep SLV data for reports. Editing either of these files will destroy SLV reporting capability.

▶ Procedure

1. Type **dvuhist -f** *agentname user_history_table_number* **config** *number_of_buckets interval download_file***.udh** to load user-defined history files for the frame relay link.

   Example:
   `dvuhist -f Dallas51 3 config 30 60 Dallas51k.udh`

   The interval must be entered in seconds.

2. Type **dvuhist -f "***agentname DLCI_number***"** *user_history_table_number* **config** *number_of_buckets interval download_file***.udh** to load user-defined history files for a specific DLCI.

   Example:
   `dvuhist -f "Dallas51 301" 3 config 30 60 Dallas301.udh`

   The same user history table number can be used for both the link and DLCI. For these examples, user history table number 3 will appear as UserHistory3 on the History List.

See Step 5 in *Monitoring a DLCI's History Data* to verify that the user-defined history files have been loaded.

Refer to *Installing .UDH Files* in *Using Custom History* of the *NetScout Manager Plus User Guide* for additional information.

Monitoring a DLCI's History Data

Once the monitoring variables have been defined, a problem DLCI can monitored.

▶ Procedure

To monitor user history data:

1. From the NetScout Manager Plus main window, with the FrameRelay radio button still selected, select the Traffic radio button.

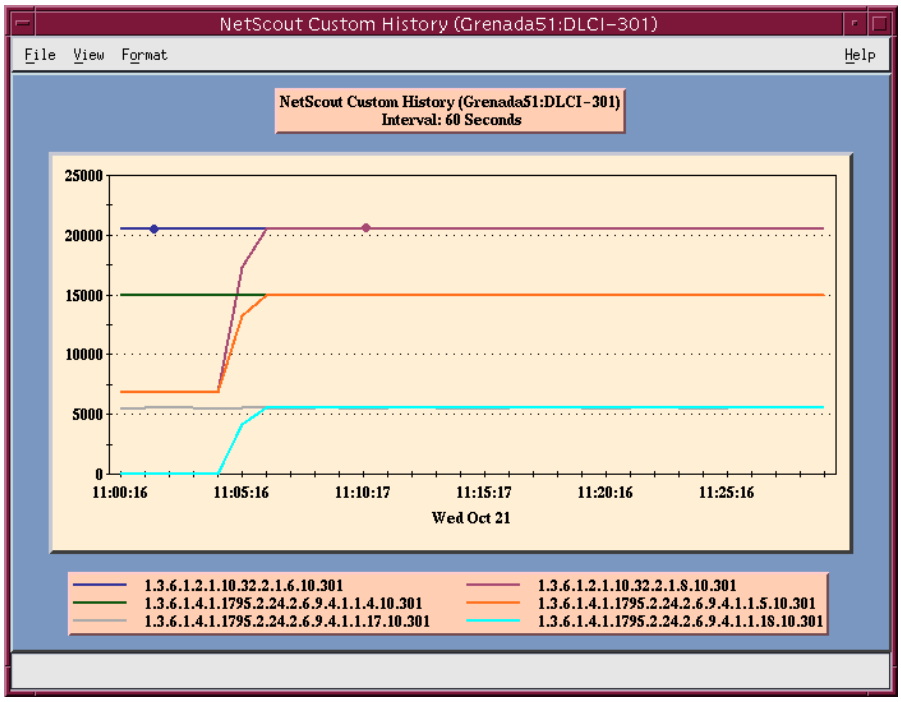
   The appropriate icons appear.

2. Highlight an agent in the agent list box so that its DLCIs appear in the DLCI list box (under the agent list box).

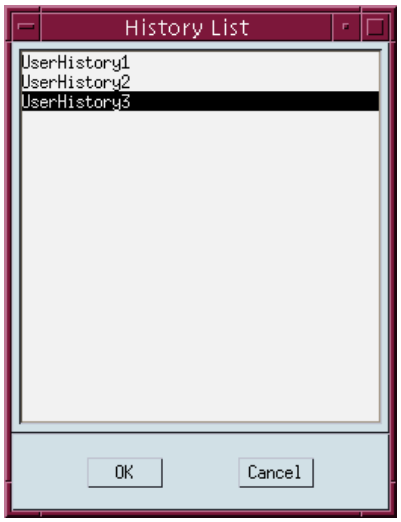
3. Highlight the DLCI to be monitored.

4. Click on the Custom History icon. The NetScout Custom History window opens.

   Adjust the size of the window so the entire report can be viewed.



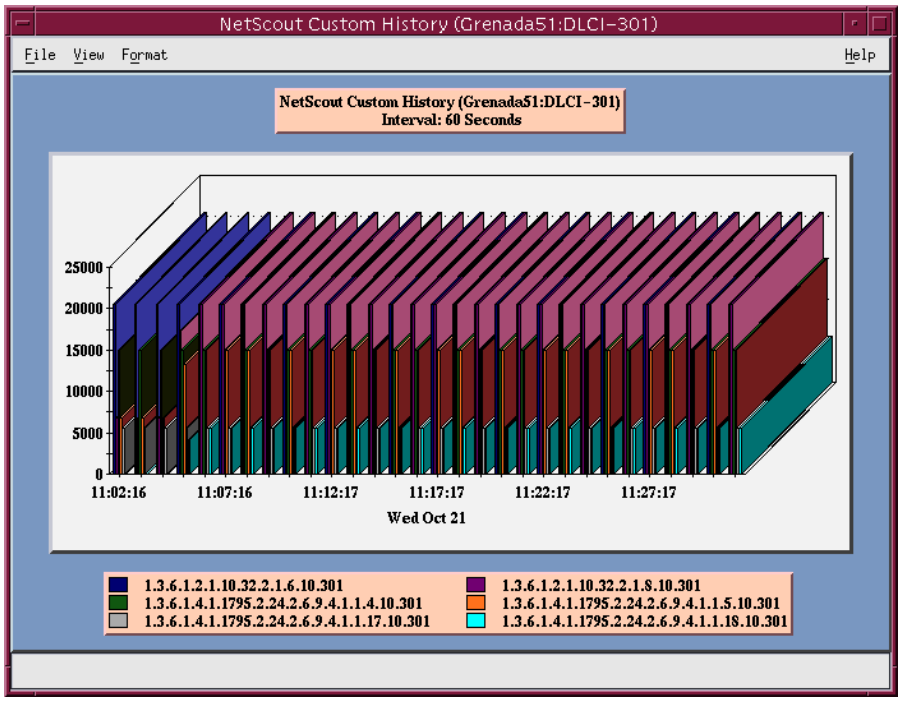
5. Select History List from the View menu. The History List window opens. The newly defined user history variables should appear on this list.



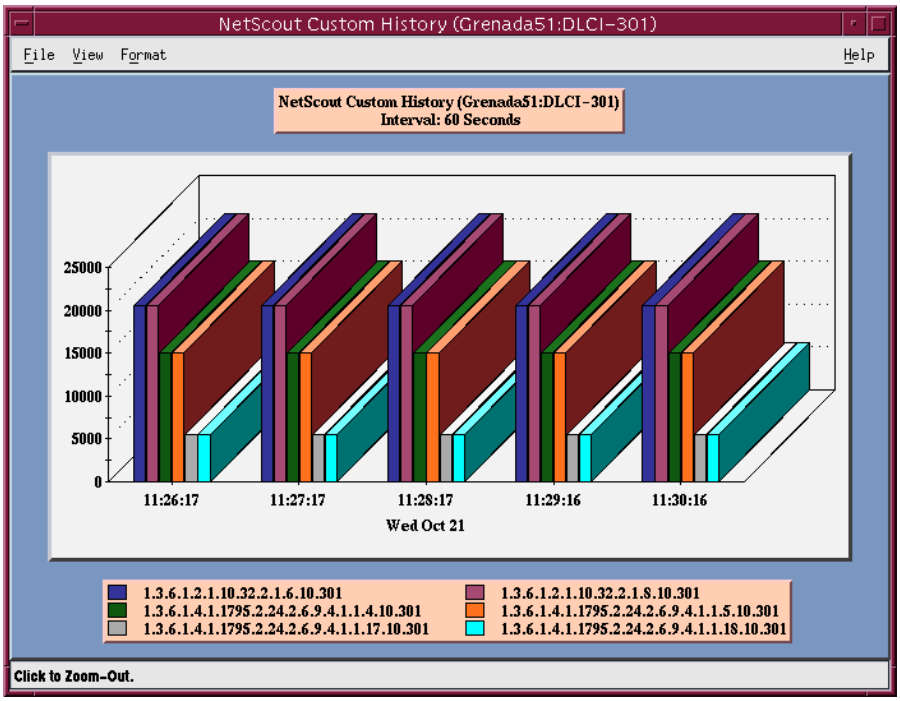
6. Highlight the desired set of user history variables, and select the OK button.

   Data is gathered based upon the configured user history variables. This may take some time, so please be patient.

7. Select 2D or 3D Bar from the Format menu, if desired (3D Bar is shown).



Using the 2D or 3D Bar to view the user history data collected, you can click on a particular bar and get an expanded view of the data.



8. Click anywhere on this window to return to the previous window view (see Step 7 of this procedure).

Refer to *Launching User History* and *Understanding Custom History Display* in *Using Custom History* of the *NetScout Manager Plus User Guide* for additional information.

See *Object ID Cross-References (Numeric Order)* in Appendix B, *SNMP MIBs and Traps, and RMON Alarm Default*, to identify OID information being shown.

Monitoring the Agent Using NetScout Manager Plus (Models 9820 and 9820-2M)

Once the FrameSaver SLV agent has been added to NetScout Manager Plus, select either the Traffic or Protocol radio button to monitor the newly added agent, or one of its DLCIs.

NOTE:

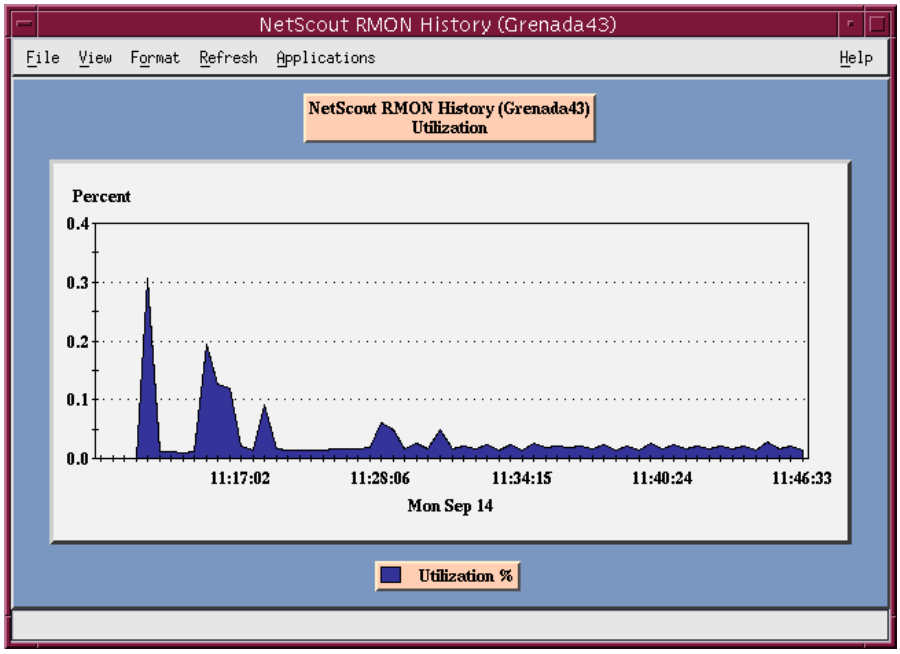
Only the Traffic and Protocol radio buttons on the application selection bar are supported for FrameSaver SLV agents.

The procedure below describes how to monitor an agent's traffic. The procedure is the same for protocol monitoring, but you may be prompted to select a Domain Group as well as an agent or DLCI.

▶ Procedure

1. Select the Traffic radio button to monitor the newly added agent, or one of its DLCIs.
2. Highlight an agent in the agent list box so that its DLCIs appear in the DLCI list box (under the agent list box).
3. If you want to monitor one of the agent's DLCIs, highlight the DLCI to be monitored.
4. Click on an applicable icon. The selected graphical report should open.

   Traffic icons that would be of particular interest are Traffic Monitor and Domain History. In the example below, the Domain History icon was selected, which is actually a real-time report.



NOTE:

If Size Distribution is the selected View and distribution size has been changed via OpenLane, the values shown for the distribution will not be accurate. Only default size distributions are tracked.

Statistical Windows Supported (Models 9820 and 9820-2M)

Not all icons that appear on the NetScout Manager Plus main window are supported for FrameSaver units. For example, All Convs (conversations) and TopNConv icons appear when the Protocol radio button is selected, but conversations are not supported.

Of the icons that appear on the NetScout Manager Plus main window, the following are supported:

Traffic Statistics	**Protocol Statistics**
Traffic Monitor	Protocol Monitor
Segment Zoom	Protocol Zoom
Segment Details[1]	TopNTalkers
Domain History[1]	All Talkers

[1] Size distribution statistics are provided for a DLCI only, not a link. If a link is selected, all size distribution statistics on the table or graph will be zero.

When a DLCI is selected, the first and last size distribution statistics are ignored for FrameSaver units and the statistics for those buckets appear in the next valid bucket (i.e., bucket size <64 and 64 statistics appear in the 65..127 bucket, and >1518 statistics appear in the 1024..1518 bucket).

Conversations and Long-Term and Short-Term Histories are not supported in this release. As a result, no data will appear on windows that include these panes.

Setting Up Network Health for FrameSaver Devices

11

FrameSaver units are compatible with Concord Communication's Network Health software. In addition, 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 11-9). To get this report, you need Network Health R4.01 or higher.

This chapter includes Network Health information as it relates to FrameSaver SLV 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 SLV Devices*

For additional information about installing, accessing, and managing FrameSaver SLV 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 SLV 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 SLV 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 SLV 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 SLV 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 SLV 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 SLV 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 an SLV 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 SLV 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 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.

Using the FrameSaver SLV report on page 11-9, 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 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 SLV Devices

The following frame relay reports support FrameSaver SLV 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.

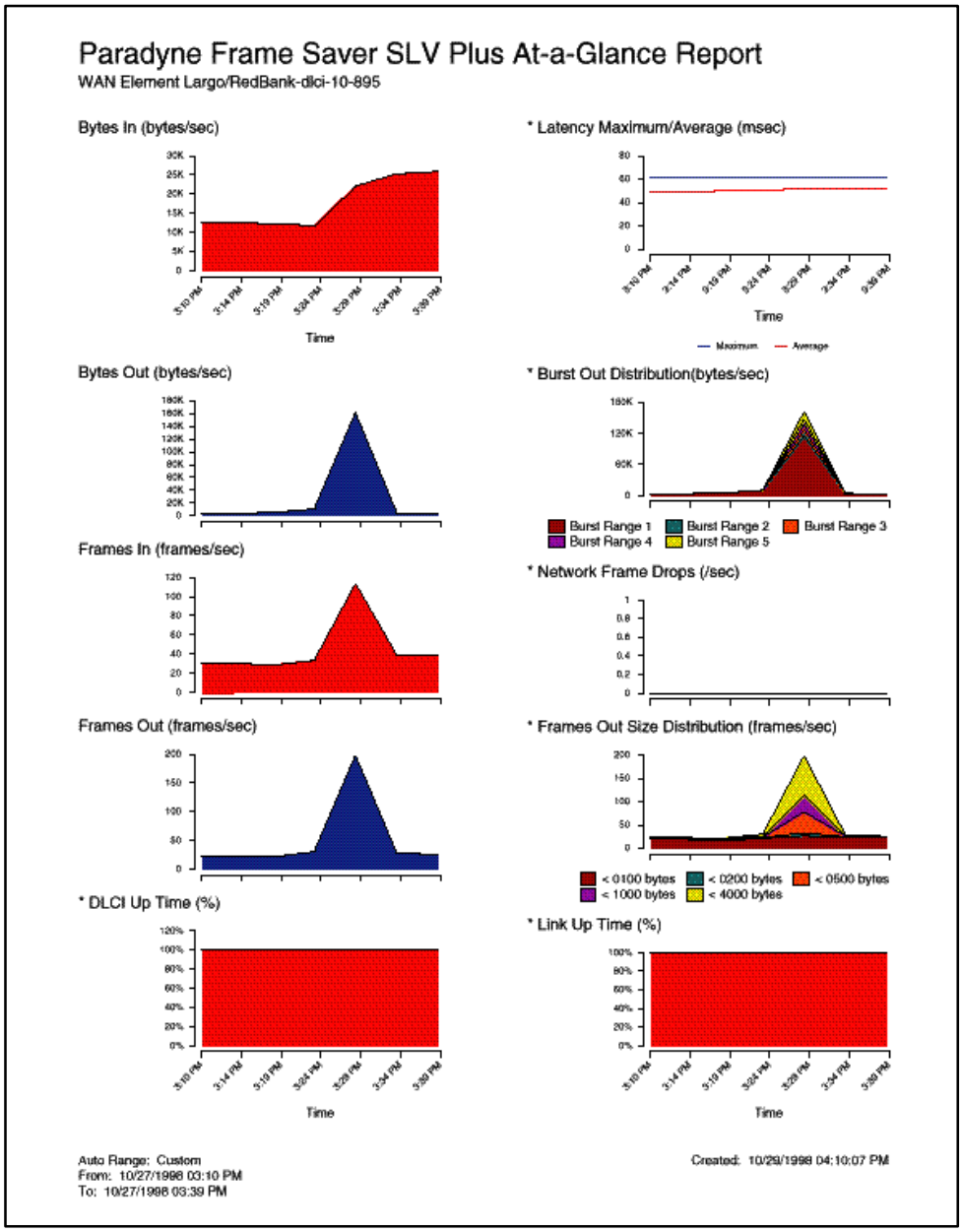
  Use this chart and table to alert you to possible problems. Problems to look for include: a normally high-volume DLCI is dropped from the list, a new DLCI appears on the list (check Element Summaries), a DLCI has a high Health Index rating, but low volume, significant differences between a DLCI's average 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** – Performs trend analysis on up to ten specified variables for DLCIs (see page 11-9 for an example). This is the first Network Health report to integrate the FrameSaver SLV's unique monitoring capabilities, using the unit's SLV-enhanced 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.

Hardware Maintenance (9820-45M)

12

Overview

The FrameSaver SLV 9820-45M is designed for years of trouble-free service. There are actions you can take to further reduce the likelihood and amount of down time:

Area of Concern	Action
Front Panel Assembly	1. Vacuum dust from air vents whenever a buildup is visible. See *Cleaning the Front Panel Assembly* on page 12-2. 2. Monitor LEDs for fan failures. Replace the front panel assembly immediately upon failure. See *Replacing the Front Panel Assembly* on page 12-3. 3. Test LEDs periodically. Replace the front panel assembly immediately upon failure. See *Replacing the Front Panel Assembly* on page 12-3.
Power Modules	Monitor LEDs for power module failures. Replace a failed power module immediately. See *Replacing a Power Module* on page 12-4.

Cleaning the Front Panel Assembly

The substantial airflow through the unit's four fans may cause dust to collect on the outside of the front air vents. When dust becomes visible at the air vents, run the brush attachment of a vacuum cleaner gently over the front panel to remove it.

In extremely dusty environments it may be necessary to remove the front panel assembly to clean the blades of the fans. Refer all service to qualified personnel.

The procedure may be performed while the unit is running.

▶ Procedure

To clean the fans:

1. Loosen the captive screws holding on the front panel.

⚠ WARNING:

The fans continue to run until the fan power cable is removed. Keep your hair and clothes away from the fan blades.

2. Carefully pull the front panel toward you.
3. Remove the fan power cable and LED ribbon cable.
4. Lay the front panel face-down on a flat surface.
5. Vacuum the fan blades and cages with the brush attachment of a vacuum cleaner.

⚠ WARNING:

Each fan starts spinning as soon as the fan power cable is reconnected. Keep your hair and clothes away from the fan blades.

6. Reconnect the LED ribbon cable, then reconnect the fan power cable. Verify that all four fans are running.
7. Replace the front panel and tighten the captive screws.

CAUTION:

Do not leave the front panel assembly off the unit for extended periods, or the unit will overheat.

Replacing the Front Panel Assembly

The System FAN LED on the front panel turns on when one or more of the front panel fans has failed. Replace the front panel assembly as soon as possible after this occurs. Refer all service to qualified personnel.

The procedure may be performed while the unit is running.

▶ Procedure

To replace the front panel:

1. Loosen the captive screws holding on the front panel.

⚠ WARNING:

The fans continue to run until the fan power cable is removed. Keep your hair and clothes away from the fan blades.

2. Carefully pull the front panel toward you. Verify that at least one of the fans has failed.
3. Remove the fan power cable and LED ribbon cable, and set the old front panel assembly aside.

⚠ WARNING:

Each fan starts spinning as soon as the fan power cable is reconnected. Keep your hair and clothes away from the fan blades.

4. Take the new front panel and connect the LED cable, then connect the fan power cable. Verify that all four fans are running.
5. Replace the front panel and tighten the captive screws. Verify that the FAN LED is turned off.

CAUTION:

Do not leave the front panel assembly off the unit for extended periods, or the unit will overheat.

Replacing a Power Module

A power module requires replacement in a FrameSaver SLV 9820-45M when:

- The front panel System PWR LED is lit. This means that one of the power modules has failed.
- Power is applied to a power module and it is switched on, but the power module LED does not light.

Refer all service to qualified personnel.

▶ Procedure

To replace a power module:

1. For a system with redundant power, determine which power module still has its power LED lit. This is the functional power supply.

⚠ WARNING:

Do not pull out a power module until the power cord has been removed.

2. Remove the power cord from the failed power module.
3. Unscrew the captive screw holding the failed power module in place.
4. Pull out the power module and set it aside.
5. Slide in the new power module until it seats in its connector. Verify that the switch is in the Off position.
6. Tighten the captive screw.
7. Replace the power cord. Move the power module switch to the On position.
8. Verify that the power module LED is lit and that the front panel System PWR LED is off.

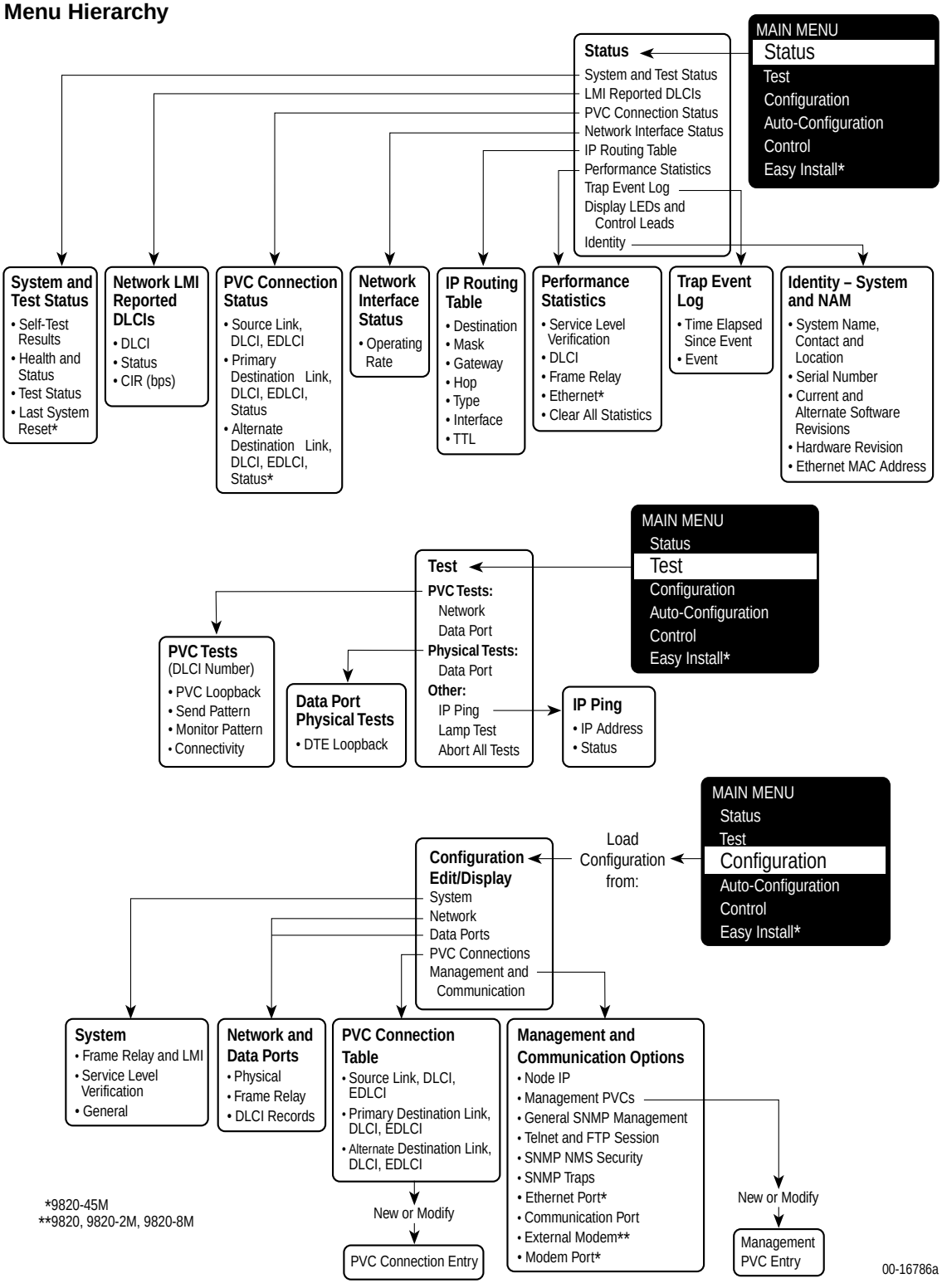
Menu Hierarchy

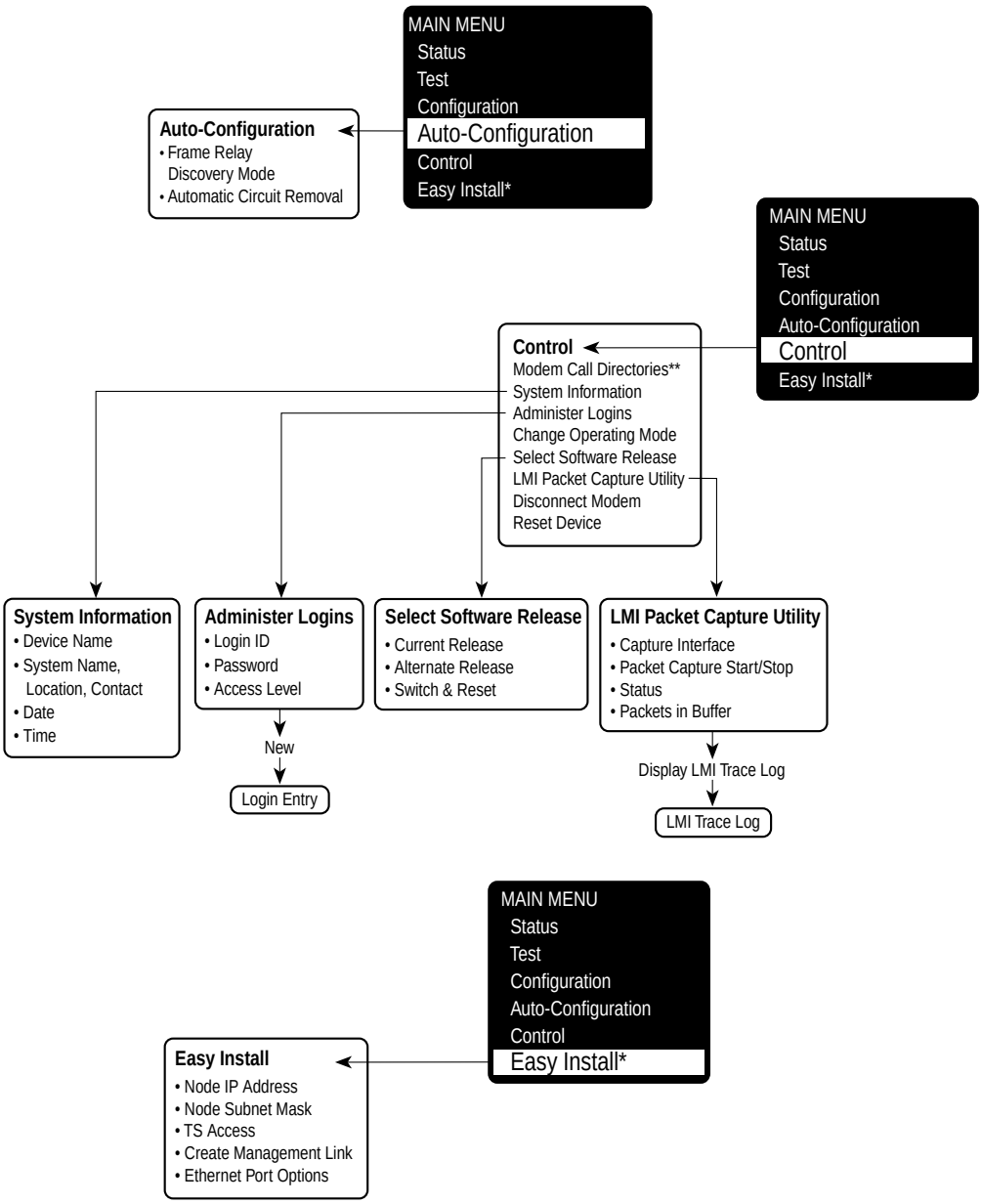
A

Menus

The following is a graphical representation of the FrameSaver SLV unit's menu organization.

Menu Hierarchy





*9820-45M
**9820, 9820-2M, 9820-8M

00-16786b

SNMP MIBs and Traps, and RMON Alarm Defaults

B

This appendix contains the following:

- *MIB Support*
- *Downloading MIBs and SNMP Traps*
- *System Group (mib-2)*
  - *FrameSaver Unit's sysDescr (system 1)*
  - *FrameSaver Unit's sysObjectID (system 2)*
- *Interfaces Group (mib-2)*
  - *Paradyne Indexes to the Interface Table (ifTable)*
  - *NetScout Indexes to the Interface Table (ifTable)*
- *Standards Compliance for SNMP Traps*
  - *Trap: warmStart*
  - *Trap: authenticationFailure*
  - *Traps: linkUp and linkDown*
  - *Traps: enterprise-Specific*
  - *Traps: RMON-Specific*
- *RMON Alarm and Event Defaults*
  - *Network Synchronous Port Physical Interface Alarm Defaults*
  - *Frame Relay Link Alarm Defaults*
  - *DLCI Alarm Defaults – Paradyne Area*
  - *DLCI Alarm Defaults*
- *Object ID Cross-References (Numeric Order)*

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 a FrameSaver SLV 9820 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 SLV 9820 unit:

> PARADYNE DP FrameSaver SLV; Model: *[9820, 9820-2M, 9820-8M, or 9820-45M]*; 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 following FrameSaver SLV 9820 units:

- FrameSaver SLV 9820: 1.3.6.1.4.1.1795.1.14.2.4.7.1
- FrameSaver SLV 9820-2M: 1.3.6.1.4.1.1795.1.14.2.4.7.2
- FrameSaver SLV 9820-8M: 1.3.6.1.4.1.1795.1.14.2.4.7.3
- FrameSaver SLV 9820-45M: 1.3.6.1.4.1.1795.1.14.2.4.7.4

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			
Sync Data Port S01P1	Synchronous Data Port	Synchronous Data Port, Slot: 1, Port: 1; DP FR NAM; Hardware Version: *hhhh-hhh*	101003001
Network Sync Data Port S01P2	Network Synchronous Data Port	Network Synchronous Data Port, Slot: 1, Port: 2; DP FR NAM; Hardware Version: *hhhh-hhh*	101003002
COM	Communications port (Terminal port on 9820-45M)	COM Port; DP FR NAM; Hardware Version: *hhhh-hhh*	101004001
Modem	Modem port (9820-45M only)	Modem Port; DP FR NAM; Hardware Version: *hhhh-hhh*	101005001
Ethernet	LAN port	Ethernet Port; DP FR NAM; Hardware Version: *hhhh-hhh*	101006001
Frame Relay Logical Layer			
FR UNI	Frame relay logical link on the Synchronous Data Port	*For the user side:* Synchronous Data Port of FR DTE, Slot: 1, Port: 1; DP FR NAM; Hardware Version: *hhhh-hhh*	101016001
		For the network side: Synchronous Data Port of FR SERVICE, Slot: 1, Port: 1; DP FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on the Network Synchronous Data Port	*For the user side:* Network Synchronous Data Port of FR DTE, Slot: 1, Port: 1; DP FR NAM; Hardware Version: *hhhh-hhh*	101016002
		For the network side: Network Synchronous Data Port of FR SERVICE, Slot: 1, Port: 1; DP 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 4 Network V.35/X.21	Network Synchronous Data Port	*For the user side:* RMON (IN/OUT); Network Synchronous Data Port of FR DTE, Slot: 1, Port: 2; DP FR NAM; Hardware Version: *hhhh-hhh*	4
		For the network side: RMON (IN/OUT); Network Synchronous Data Port of FR SERVICE, Slot: 1, Port: 2; DP FR NAM; Hardware Version: *hhhh-hhh*	
RMON Logical Layer			
RMON Frame Relay Logical Interfaces (9820 and 9820-2M)	These values are calculated. ■ For the DTE: (ifIndex –1) * 2 +17 ■ For the DCE: DTE calculated value +1	OUT – RMON (IN); [*ifName of the interface*]	17–48
		OUT – RMON (OUT); [*ifName of the interface*]	
RMON Virtual Interfaces	These values are calculated based on the probe's internal circuit index: circuit index +65.	—	65–512 (9820 and 9820-2M) 65 – 100000000 (9820-8M and 9820-45M)
RMON Virtual Logical Interfaces (9820 and 9820-2M)	These values are calculated. ■ For the DTE: (virtual interface ifIndex –65) * 2 +513 ■ For the DCE: DTE calculated value +1	IN – VIRTUAL PVC [*interface number*] [*DLCI number*] DTE	513–1023
		OUT – VIRTUAL PVC [*interface number*] [*DLCI number*] DCE	

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" 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.

Example:
'DLCI 100 of Sync Data Port S01P1 frame relay'
In this example, a DLCI and a frame relay link are associated with the trap.

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:

- Network and synchronous data ports – Physical sublayer interfaces
- 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.

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 2)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer		
Network 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. If the interface is configured to monitor the control lead, alarms are generated as shown in Table B-7. *String:* '$ifString $alarmString down.' (e.g., 'Sync Data Port S01P2 DTR and RTS down.') '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the port. If the interface is configured to monitor the control lead, alarms are generated as shown in Table B-7. *String:* '$ifString up.'
User Synchronous Data Port (Supported by the media-specific RS232-like MIB.)		■ linkDown – One or more alarm conditions are active on the port. If the interface is configured to monitor the control lead, alarms are generated as shown in Table B-7. *String:* '$ifString $alarmString down.' (e.g., 'Sync Data Port S01P1 DTR down.') '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the port. If the interface is configured to monitor the control lead, alarms are generated as shown in Table B-7. *String:* '$ifString up.'

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

Interface	Variable-Bindings	Possible Cause
Physical Sublayer, continued		
Ethernet Port	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – Communications are not possible on the port. *String:* 'Ethernet $alarmString down.' ■ linkUp – Communications are now possible on the port. *String:* 'Ethernet up.'
Logical Link Sublayer		
Frame Relay (Supported by the media-specific Frame Relay Services MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured, or Frame Relay link is disabled. If the LMI Protocol is not configured, a linkUp/linkDown trap is based solely upon whether the interface is enabled or disabled. *Strings:* '$ifString down.' No alarms exist on the link due to LMI. '$ifString LMI down.' No alarms exist on the link because LMI is down. '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$ifString up.'

Table B-7. Input Control Leads That Generate linkDown and linkUp Traps

Signal Name	V.35 and EIA-530-A		X.21		HSSI	
	DCE	DTE	DCE	DTE	DCE	DTE
RTS (Control)	S	U	S	U	U	U
CTS	U	S	U	U	U	U
DSR (CA)	U	S	U	U	U	S
DTR (TA)	S	U	U	U	S	U
RLSD (Indication)	U	S	U	S	U	U
S = Supported, U = Unsupported						

Traps: enterprise-Specific

These traps indicate that an enterprise-specific event has occurred. Supported enterprise-specific traps are listed below.

Table B-8. enterprise-Specific Traps and Variable-Bindings (1 of 2)

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.'
enterpriseLinkSpeed-Change(14)	■ ifIndex (RFC 1573) ■ ifSpeed (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib	Speed has changed as a result the Autorate algorithm. *String:* 'Speed of $ifName changed to $ifSpeed bps.'

Table B-8. enterprise-Specific Traps and Variable-Bindings (2 of 2)

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.)
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.')

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-9. 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.' (e.g., 'Octets received on Sync Data Port S01P1 frame relay rose to threshold of 1.') $typeString is 'rose to' if alarmValue equals alarmRisingThreshold; otherwise, it is 'exceeded'.
fallingAlarm	■ alarmIndex (RFC 1757) ■ alarmVariable (RFC 1757) ■ alarmSampleType (RFC 1757) ■ alarmValue (RFC 1757) ■ alarmFallingThreshold (RFC 1757) ■ devLastTrapString (devHealthAndStatus.-mib)	Object being monitored has fallen below the set threshold. *String:* 'Change in $variableName $typeString threshold of $alarmRisingThreshold by $(alarmFallingThreshold – alarmValue).' (e.g., 'Octets received on Sync Data Port S01P1 frame relay rose to threshold of 1.') $typeString is 'fell to' if alarmValue equals alarmFallingThreshold; otherwise, it is 'fell below'.

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	eventCommunity
1	Default SLV Rising Event	log-and-trap(4)	0
2	Default SLV Falling Event	log-and-trap(4)	0

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*

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.

Network Synchronous Port Physical Interface Alarm Defaults

These alarms only apply to the FrameSaver unit's network data port interface. They are created during RMON initialization and put into the Paradyne-defined alarm area.

Table B-10. Network Synchronous Port 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_SyncPortStats.mib (E) *Tag:* devSyncPortStatsUASs *OID:*.1.3.6.1.4.1.1795.2.24.-2.6.6.5.1.1.2.**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-11. 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
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

[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-11. 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
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-12. DLCI Alarm Defaults – Paradyne Area (1 of 2)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
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
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 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
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
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
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

Table B-12. DLCI Alarm Defaults – Paradyne Area (2 of 2)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Maximum Latency	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyMax *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.6.**I**.**D**	60 secs (1 min)	Rising	1	1

[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.

DLCI Alarm Defaults

These alarms can be created during RMON initialization or when a DLCI is created. For Models 9820 and 9820-2M, they are put into the NetScout alarm area; for Models 9820-8M and 9820-45M they are grouped with the DLCI Alarm Defaults in the Paradyne area.

Table B-13 identifies alarm defaults that do not change, and Table B-14 identifies alarm defaults that change when the interface's line speed changes.

The thresholds for these alarms can be edited using NetScout Manager Plus so they match the values in the SLA between the customer and service provider. Up to eight alarms per interface are allowed. Any additional alarms are added to the Paradyne Area alarms and they cannot be changed using NetScout software.

See *Editing Alarms* in Chapter 10, *Setting Up NetScout Manager Plus for FrameSaver Devices*.

Table B-13. Static DLCI Alarm Defaults (1 of 2)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
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
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
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
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
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.

Table B-13. Static DLCI Alarm Defaults (2 of 2)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
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

[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-14. Dynamic DLCI Alarm Defaults

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
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
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

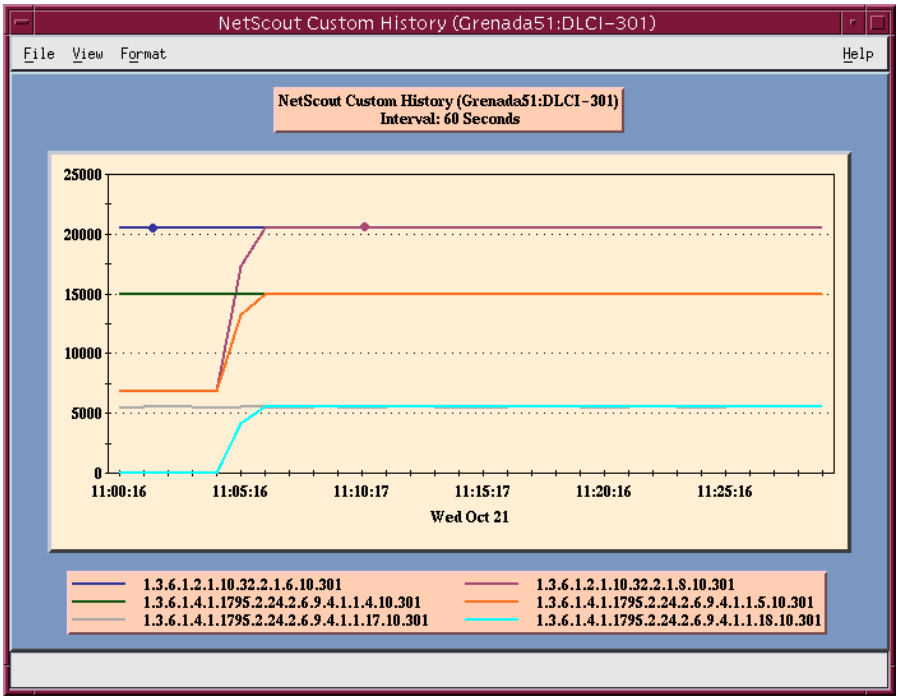
[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute. Indicates that the exact value for the item is contained in the MIB.

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

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-15 for an RMON history OID cross-reference and Table B-16 for an RMON alarm OID cross-reference.

Table B-15. History OID Cross-Reference (1 of 4)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.2.1.2.2.1. . .		
.1.3.6.1.2.1.2.2.1.**5.I**	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
.1.3.6.1.2.1.16.12.2.1. . .		
.1.3.6.1.2.1.16.12.2.1.**2.P**	Protocol Octets (for 11 protocols)	*MIB:* RMON II (RFC 2021) *Tag:* protocolDistStatsOctets

[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-15. History OID Cross-Reference (2 of 4)

Object ID (OID) [1]	Item	MIB/Tag
.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
.1.3.6.1.4.1.1795.2.24.2.**13**.**1.2.1.4.H.T.N**	IP Top Listeners (1–6)	*MIB:* pdn_FrExt.mib (E) *Tag:* devRmonIPTopNDstIP
.1.3.6.1.4.1.1795.2.24.2.**13**.**1.2.1.6.H.T.N**	IP Top Talkers (1–6)	*MIB:* pdn_FrExt.mib (E) *Tag:* devRmonIPTopNSrcIP
.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] **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-15. History OID Cross-Reference (3 of 4)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**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
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**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**	DLCI 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] **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-15. History OID Cross-Reference (4 of 4)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1. . .		
.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.**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.**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
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1. . .		
.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-16 for an RMON alarm OID cross-reference.

Table B-16. 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. . .		
.1.3.6.1.4.1.1795.2.24.2.**6.6.5.1.1.2.I**	Unavailable Seconds	*MIB:* pdn_SyncPortStats.mib (E) *Tag:* devSyncPortStatsUAS
.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**	DLCI 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-16. 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

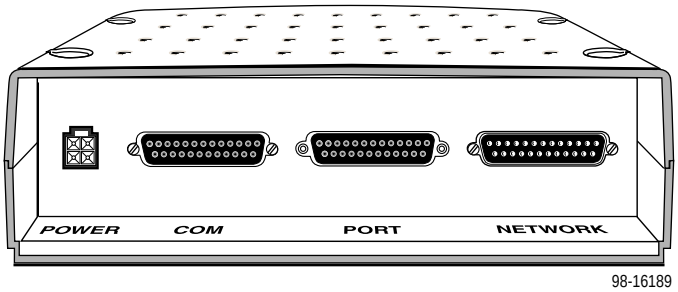
This appendix shows the FrameSaver unit rear panels, and pin assignments for the connectors/interfaces and cables.

NOTE:

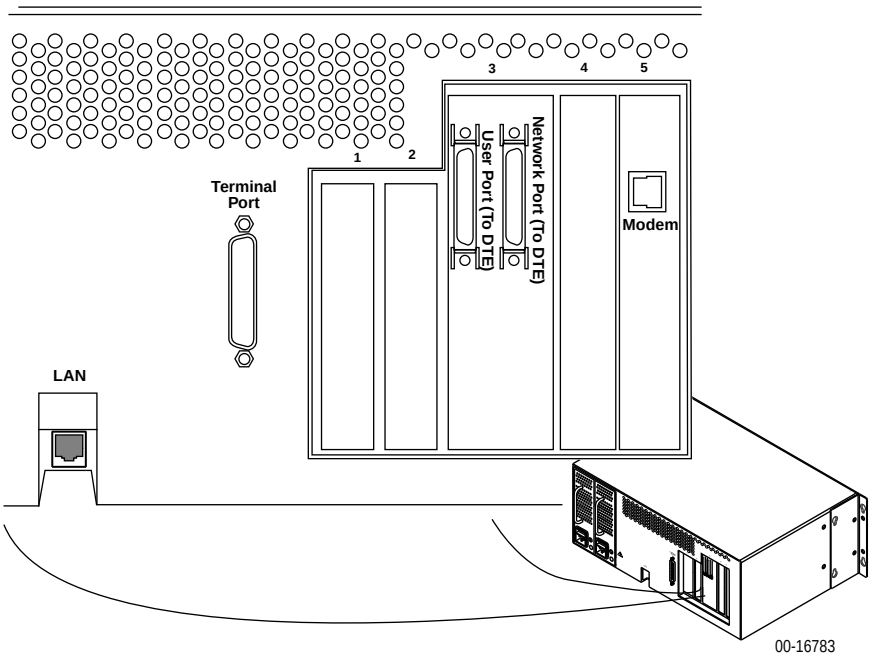
In the pin assignment tables of this appendix, if the pin number is not shown, it is not being used.

Rear Panels

The following illustration shows the rear panel of the FrameSaver 9820, 9820-2M, and 9820-8M models.



The following illustration shows the rear panel of the FrameSaver 9820-45M.



COM (Terminal) Port Connector

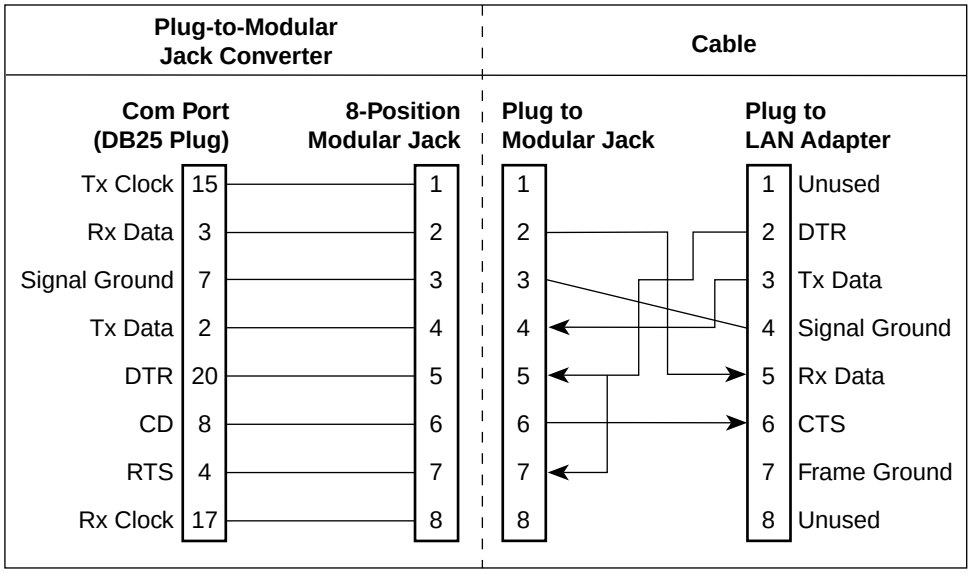
The following table shows the signals and pin assignments for the DB25 communication port connector. The communication port is called the Terminal port on the Model 9820-45M.

Signal	Direction	Pin #
Shield	—	1
Transmit Data (TXD)	To COM port (In)	2
Received Data (RXD)	From COM port (Out)	3
Request to Send (RTS)	To COM port (In)	4
Carrier Detect (CD)	From COM port (Out)	5, 6, 8
Signal Ground (SG)	To/From COM port	7
Data Terminal Ready (DTR)	To COM port (In)	20

LAN Adapter Converter and Cable (Models 9820, 9820-2M, 9820-8M)

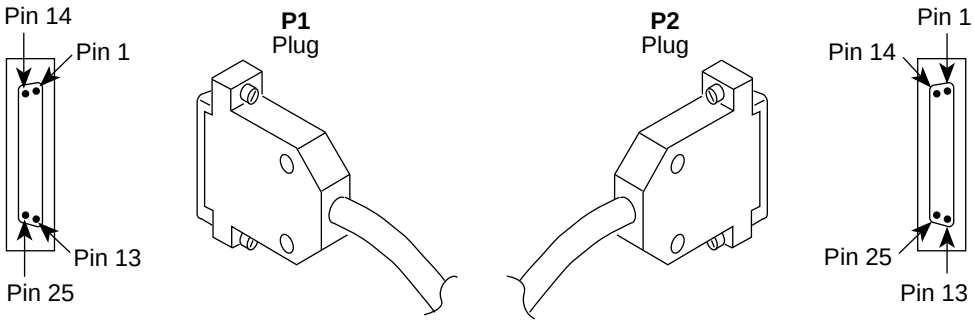
The following shows the pin assignments for the:

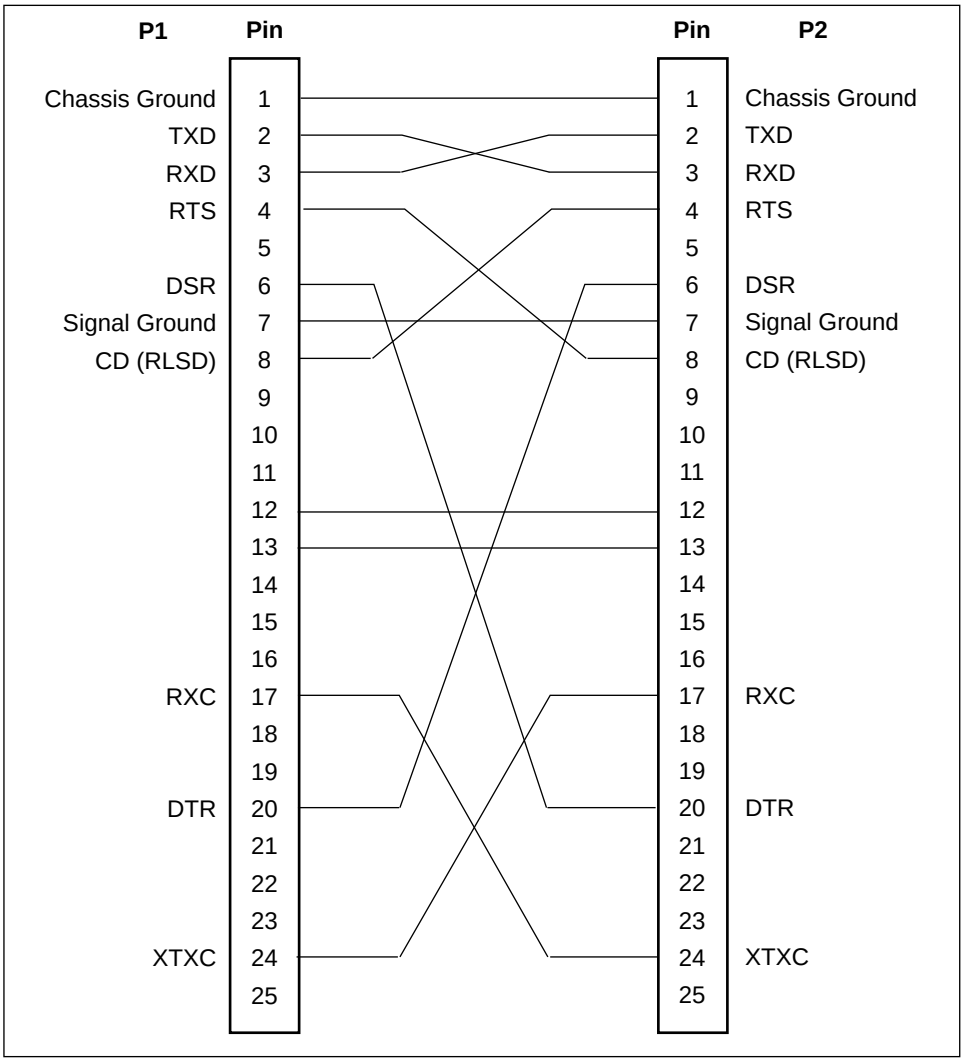
- DB25 plug-to-modular jack converter between the COM (Terminal) port and the 8-conductor LAN Adapter cable (Feature No. 3100-F1-920)
- Custom 8-conductor cable (with modular plugs on both ends) between the converter and the LAN Adapter (Feature No. 3100-F2-910)



Standard EIA-232 Crossover Cable (Models 9820, 9820-2M, 9820-8M)

A standard EIA-232 crossover cable can be used to connect the COM port to an external modem. This is an EIA-232 plug-to EIA-232 plug (DB25-to-DB25) cable. The external modem must be configured so it is compatible with the FrameSaver unit. See page C-5 to configure an external modem.





99-16332

▶ 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.

User and Network Data Port Connectors (Models 9820, 9820-2M, 9820-8M)

The following table provides the pin assignments for the EIA-530-A connector to the DTE or NTU.

Signal	Circuit Mnemonic	ITU #	Direction	25-Pin Pin #
Shield	—	—	—	1
Transmit Data (TXD)	BA	103	To DCE	2 (A) 14 (B)
Received Data (RXD)	BB	104	From DCE	3 (A) 16 (B)
Request to Send (RTS)	CA	105	To DCE	4 (A) 19 (B)
Clear to Send (CTS)	CB	106	From DCE	5 (A) 13 (B)
Data Set (or DCE) Ready (DSR)	CC	107	From DCE	6
Signal Ground/Common (SG)	AB	102A	To/From DCE	7
Received Line Signal Detector (RLSD or LSD)	CF	109	From DCE	8 (A) 10 (B)
Transmit Signal Element Timing (TXC – DTE Source)	DA	113	To DCE	11 (B) 24 (A)
Transmit Signal Element Timing (TXC – DCE Source)	DB	114	From DCE	12 (B) 15 (A)
Received Signal Element Timing (RXC – DCE Source)	DD	115	From DCE	17 (A) 9 (B)
Local Loopback (LL)	LL	141	To DCE	18
Data Terminal (or DTE) Ready (DTR)	CD	108/1, /2	To DCE	20
Test Mode Indicator (TM)	TM	142	From DCE	25

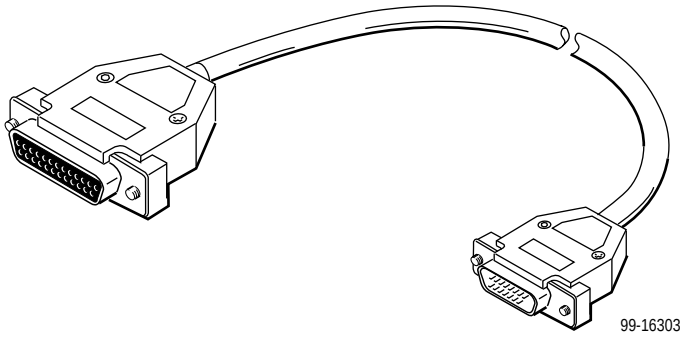
NOTE:

The user data port has a DCE personality, while the network data port has a DTE personality.

X.21 Network Cable (Models 9820, 9820-2M, 9820-8M)

This cable is used to connect the network data port to an NTU with an X.21 interface. It is a 25-position EIA-530A-to-15-pin X.21 (DB25-to-X.21) cable.

This cable (Part No. 035-0384-1031) is part of the X.21 Cable Kit (Feature No. 9008-F1-521).



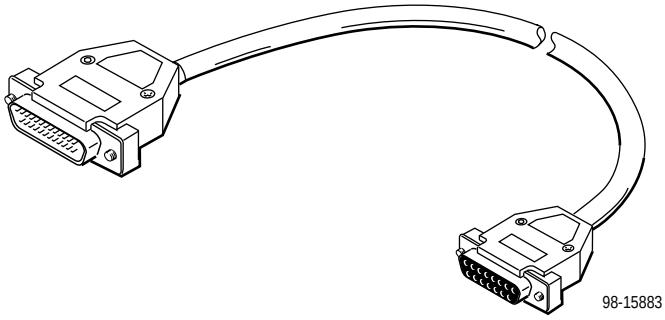
The following table provides the pin assignments for the DB25-to-X.21 network cable.

Signal	ITU #	25-Pin Socket Pin #	Direction	15-Pin Plug Pin #
Transmit Data (TXD)	103	2 (A) 14 (B)	To DCE	2 (A) 9 (B)
Received Data (RXD)	104	3 (A) 16 (B)	From DCE	4 (A) 11 (B)
Request to Send (RTS)	105	4 (A) 19 (B)	To DCE	3 (A) 10 (B)
Signal Ground/Common (SG)	102	7	—	8
Data Channel Received Line Signal Detector (RLSD or LSD)	109	8 (A) 10 (B)	From DCE	5 (A) 12 (B)
Transmit Signal Element/ Terminal Timing (TT) — DTE Source	113	24 (A) 11 (B)	To DCE	7 (A) 14 (B)
Received Signal Element Timing (RXC) — DCE Source	115	17 (A) 4 (B)	From DCE	13 (A) 3 (B)

X.21 DTE Adapter Cable (Models 9820, 9820-2M, 9820-8M)

This adapter is used to connect the user data port to a DTE with an X.21 cable. It is a 25-pin EIA-530A-to-15-pin X.21 (DB25-to-X.21) adapter cable.

This cable (Part No. 035-0302-0131) is part of the X.21 Cable Kit (Feature No. 9008-F1-521).



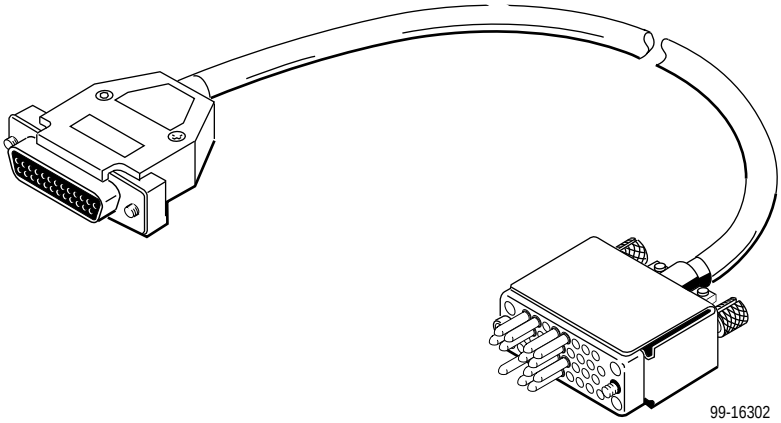
The following table provides the pin assignments for the DB25-to-X.21 adapter cable.

Signal	ITU #	25-Pin Plug Pin #	Direction	15-Pin Socket Pin #
Transmit Data (TXD)	103	2 (A) 14 (B)	To DCE	2 (A) 9 (B)
Received Data (RXD)	104	3 (A) 16 (B)	From DCE	4 (A) 11 (B)
Received Signal Element Timing (RXC) — DCE Source	115	17 (A) 9 (B)	From DCE	6 (A) 13 (B)
Request to Send (RTS)	105	4 (A) 19 (B)	To DCE	3 (A) 10 (B)
Data Channel Received Line Signal Detector (RLSD or LSD)	109	8 (A) 10 (B)	From DCE	5 (A) 12 (B)
Transmit Signal Element/ Terminal Timing (TT) — DTE Source	113	24 (A) 11 (B)	To DCE	7 (A) 14 (B)
Signal Ground/Common (SG)	102	7	—	8

V.35 Network Cable (Models 9820, 9820-2M, 9820-8M)

This cable is used to connect the network data port to an NTU with a V.35 interface. It is a 25-position EIA-530A-to-34-pin V.35 (DB25-to-V.35) cable.

This cable (Part No. 035-0383-1031) is part of the V.35 Cable Kit (Feature No. 9008-F1-522).



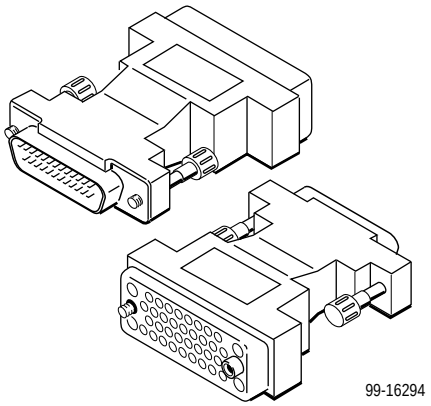
The following table provides the pin assignments for the DB25-to-V.35 network cable.

Signal	ITU #	25-Pin Socket Pin #	Direction	34-Pin Plug Pin #
Transmit Data (TXD)	103	2 (A) 14 (B)	To DCE	P (A) S (B)
Received Data (RXD)	104	3 (A) 16 (B)	From DCE	R (A) T (B)
Transmit Signal Element Timing (TXC) — DCE Source	114	15 (A) 12 (B)	From DCE	Y (A) AA (B)
Received Signal Element Timing (RXC) — DCE Source	115	17 (A) 9 (B)	From DCE	V (A) X (B)
Transmit Signal Element/ Terminal Timing (TT) — DTE Source	113	24 (A) 11 (B)	To DCE	U (A) W (B)
Request to Send (RTS)	105	4	To DCE	C
Clear to Send (CTS)	106	5	From DCE	D
Data Terminal (or DTE) Ready (DTR)	108/1, /2	20	To DCE	H
Data Channel Received Line Signal Detector (RLSD or LSD)	109	8	From DCE	F
Loopback/Maintenance (RL)	140	21	To DCE	N
Local Loopback (LL)	141	18	To DCE	L
Test Mode Indicator (TM)	142	25	From DCE	NN
Data Set (or DCE) Ready (DSR)	107	6	From DCE	E
Signal Ground/Common (SG)	102	7, 23	—	B

V.35 DTE Adapter (Models 9820, 9820-2M, 9820-8M)

This adapter is used to connect the user data port to a DTE with an V.35 cable. It is a 25-pin EIA-530A-to-34-position V.35 (DB25-to-V.35) adapter.

This adapter (Part No. 002-0095-0031) is part of the V.35 Cable Kit (Feature No. 9008-F1-522).

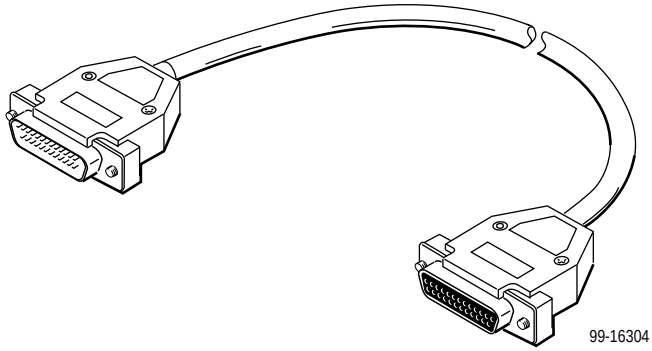


The following table provides the pin assignments for the DB25-to-V.35 adapter.

Signal	ITU #	25-Pin Plug Pin #	Direction	34-Pin Socket Pin #
Shield	—	1	—	A
Transmit Data (TXD)	103	2 (A) 14 (B)	To DCE	P (A) S (B)
Received Data (RXD)	104	3 (A) 16 (B)	From DCE	R (A) T (B)
Transmit Signal Element Timing (TXC) — DCE Source	114	15 (A) 12 (B)	From DCE	Y (A) AA (B)
Received Signal Element Timing (RXC) — DCE Source	115	17 (A) 9 (B)	From DCE	V (A) X (B)
Request to Send (RTS)	105	4	To DCE	C
Clear to Send (CTS)	106	5	From DCE	D
Data Terminal (or DTE) Ready (DTR)	108/1, /2	20	To DCE	H
Data Channel Received Line Signal Detector (RLSD or LSD)	109	8	From DCE	F
Data Set (or DCE) Ready (DSR)	107	6	From DCE	E
Signal Ground/Common (SG)	102	7	—	B
Loopback/Maintenance (RL)	140	21	To DCE	N
Local Loopback (LL)	141	18	To DCE	L
Signal Ground/Common (SG)	102	23	—	B
Transmit Signal Element/ Terminal Timing (TT) — DTE Source	113	24 (A) 11 (B)	To DCE	U (A) W (B)

EIA-530-A Straight-through Cable (Models 9820, 9820-2M, 9820-8M)

A standard straight-through cable (Feature No. 9008-F1-523) is used to connect the network data port to the NTU or the user data port to a DTE when the Port Type is E530 (EIA-530-A). It is a 25-pin EIA-530A-to-25-pin EIA-530-A (DB25-to-DB25) cable.



The following table provides the pin assignments for the DB25-to-DB25 straight-through cable.

Signal	ITU #	25-Pin Plug Pin #	Direction	25-Pin Socket Pin #
Shield	—	1	—	1
Transmit Data (TXD)	103	2 (A) 14 (B)	To DCE	2 (A) 14 (B)
Received Data (RXD)	104	3 (A) 16 (B)	From DCE	3 (A) 16 (B)
Request to Send (RTS)	105	4, 19	To DCE	4, 19
Clear to Send (CTS)	106	5, 13	From DCE	5, 13
Data Set (or DCE) Ready (DSR)	107	6	From DCE	6
Data Terminal (or DTE) Ready (DTR)	108/1, /2	20	To DCE	20
Signal Ground/Common (SG)	102	7	—	7
Data Channel Received Line Signal Detector (RLSD or LSD)	109	8, 10	From DCE	8, 10
Transmit Signal Element Timing (TXC) — DCE Source	114	15 (A) 12 (B)	From DCE	15 (A) 12 (B)
Received Signal Element Timing (RXC) — DCE Source	115	17 (A) 9 (B)	From DCE	17 (A) 9 (B)
Local Loopback (LL)	141	18	To DCE	18
Loopback/Maintenance (RL)	140	21	To DCE	21
Transmit Signal Element/ Terminal Timing (TT) — DTE Source	113	24 (A) 11 (B)	To DCE	24 (A) 11 (B)
Test Mode Indicator (TM)	142	25	From DCE	25

EIA-612/613 HSSI Connectors (Model 9820-45M)

The 50-pin HSSI connectors on the Model 9820-45M use standard EIA-612/613 signaling.

Signal	ITU #	Pin # (Positive Side)	Pin # (Negative Side)	Direction
Signal Ground (SG)	102	1	26	—
Receive Timing (RT)	115	2	27	From DCE
DCE Available (CA)	107	3	28	From DCE
Receive Data (RD)	104	4	29	From DCE
Send Timing (ST)	114	6	31	From DCE
Signal Ground (SG)	102	7	32	—
DTE Available (TA)	108/2	8	33	To DCE
Terminal Timing (TT)	113	9	34	To DCE
Loopback Circuit A (LA)	143	10	35	To DCE
Send Data (SD)	103	11	36	To DCE
Signal Ground (SG)	102	13	38	—
Signal Ground (SG)	102	19	44	—
Test Mode (TM)	142	24	49	From DCE
SIgnal Ground (SG)	102	25	50	—

LAN Connector (Model 9820-45M)

The LAN connector on the Model 9820-45M uses a standard IEEE 802.3 8-pin modular jack.

Signal	Pin #	Direction
Transmit Data (TD) +	1	Out
Transmit Data (TD) –	2	Out
Receive Data (RD) +	3	In
Not Connected	4	—
Not Connected	5	—
Receive Data (RD) –	6	In
Not Connected	7	—
Not Connected	8	—

Modem Connector (Model 9820-45M)

The MODEM connector on the Model 9820-45M uses a 6-position, 4-contact modular jack with the following pin assignments.

Signal	Pin #
Not Connected	1
Ring	2
Tip	3
Not Connected	4

Technical Specifications

D

Table D-1. FrameSaver SLV Unit Technical Specifications (1 of 3)

Specification	Criteria
Approvals – Models 9820, 9820-2M, 9820-8M	
EMC (Class A)	FCC Part 15, ICES-003, CISPR22, VCCI
Network	CTR1, CTR2
ICE	73/23/EEC, 89/336/EEC, 91/263/EEC
Safety	CSA 950, EN 60950, AS 3260
Approvals – Model 9820-45M	
EMC (Class A)	FCC Part 15, ICES-003
Network (Modem)	FCC Part 68, CS-03
Safety	CSA 950, UL 1950
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

Table D-1. FrameSaver SLV Unit Technical Specifications (2 of 3)

Specification	Criteria
Weight – Models 9820, 9820-2M, 9820-8M	2.6 lbs. (1.2 kg)
Weight – Model 9820-45M	19.0 lbs. (8.4 kg)
Physical Dimension – Models 9820, 9820-2M, 9820-8M	
Height	2.9 inches (7.4 cm)
Width	8.5 inches (21.6 cm)
Depth	12.5 inches (31.8 cm)
Physical Dimensions – Model 9820-45M	
Height	7 inches (18 cm)
Width	17.2 inches (44 cm)
Depth	13 inches (33 cm)
Power – Models 9820, 9820-2M, 9820-8M	
Input	100 – 240 VAC, 50/60 Hz, 0.7A
Output	12 Vdc, 2.5A, 1.0A minimum
Power – Model 9820-45M	
Input	120 VAC, 60 Hz
Power Consumption and Dissipation - Models 9820 and 9820-2M	4.8 watts, 100 mA at 100 Vac Result: 16.38 Btu per hour 5.0 watts, 90 mA at 120 Vac Result: 17.06 Btu per hour 5.6 watts, 60 mA at 240 Vac Result: 19.11 Btu per hour
Power Consumption and Dissipation - Model 9820-8M	9.7 watts, 186 mA at 100 Vac Result: 33.10 Btu per hour 9.9 watts, 164 mA at 120 Vac Result: 33.78 Btu per hour 10.8 watts, 110 mA at 240 Vac Result: 36.85 Btu per hour
Power Consumption and Dissipation - Model 9820-45M	74.1 Watts, 1.06 A at 120 Vac Result: 252.8 Btu per hour

Table D-1. FrameSaver SLV Unit Technical Specifications (3 of 3)

Specification	Criteria
COM Port (9820, 9820-2M, 9820-8M)	DB25 connector
Data rates	9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 kbps
Terminal Port (9820-45M)	DB25 connector
Data rates	9.6, 14.4, 19.2, 28.8, 38.4 kbps
LAN Port	8-pin modular socket
Specifications	Receive: Ethernet Version 2 and IEEE 802.3 Transmit: Ethernet Version 2
Data rates	10 or 100 Mbps
Network Data Port	Models 9820, 9820-2M, 9820-8M: 25-position (DB25) subminiature connector Selectable EIA-530, V.35, X.21 Model 9820-45M: HSSI (EIA-613)
Data rates	Model 9820: 56/64 kbps and 112/128 kbps (auto-detected) Model 9820-2M: 56–2048 kbps in 56/64 kbps increments (auto-detected) Model 9820-8M: 1024–8192 kbps in 8 kbps increments (auto-detected) Model 9820-45M: 0–44.21 kbps in 8 kbps increments (auto-detected)
User Data Port	Models 9820, 9820-2M, 9820-8M: 25-position (DB25) subminiature connector Selectable EIA-530-A, V.35, X.21 Model 9820-45M: HSSI (EIA-613)
Data rates	Automatically set to same values as the Network interface

Equipment List

E

Equipment

See page E-3 for cables you can order.

Description	Model/Feature Number
FrameSaver SLV In-Line Units	
FrameSaver SLV 9820 In-Line unit (128 Kbps) for up to 16 PVCs *Includes Standalone Housing, Universal 100–240 VAC Power Supply, Power Cord, Installation Instructions, and Quick Reference.*	9820-A2-443-*nnn*[1]
FrameSaver SLV 9820-2M In-Line unit (2 Mbps) for up to 120 PVCs *Includes Standalone Housing, Universal 100–240 VAC Power Supply, Power Cord, Installation Instructions, and Quick Reference.*	9820-A2-444-*nnn*[1]
FrameSaver SLV 9820-8M In-Line unit (8 Mbps) for up to 250 PVCs *Includes Standalone Housing, Universal 100–240 VAC Power Supply, Power Cord, Installation Instructions, and Quick Reference.*	9820-A2-445-*nnn*[1]
FrameSaver SLV 9820-45M In-Line unit (45 Mbps) for up to 512 PVCs *Includes Rack-Mount Housing, Redundant Power Supplies, Power Cords, Network Cable, Installation Instructions, and Quick Reference.*	9820-A2-429
User Manual	
FrameSaver SLV, Models 9820, 9820-2M, 9820-8M, and 9820-45M, User's Guide (Paper Manual)	9820-A2-GB20
[1] Model number may include the country code *nnn*. Contact your Paradyne sales office.	

Description	Model/Feature Number
Power Supply	
100 – 240 VAC Power Supply (Models 9820, 9820-2M, 9820-8M)	9001-F1-040
120 VAC Power Module (Model 9820-45M)	9580-F1-020
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
LAN Adapter, DB25 plug-to-8-position modular receptacle	002-0069-0031	3100-F1-920
COM Port-to-LAN Adapter Cable (14 ft /4.3 m)	035-0315-1431	3100-F2-910
50-position to 50-position, 0.5-inch straight exit connector HSSI cable (10 ft/3 m)	035-0399-1031	9008-F1-514
X.21 Cable Kit, which includes a:		9008-F1-521
X.21 Network Cable (10 ft/3 m)	035-0384-1031	
X.21 DTE Adapter Cable, EIA-530-A-to-X.21 (1 ft /.3 m)	035-0302-0131	
V.35 Cable Kit, which includes a:		9008-F1-522
V.35 Network Cable (10 ft/3 m)	035-0383-1031	
V.35 DTE Adapter, EIA-530-A-to-V.35	002-0095-0031	
EIA-530 Straight-Through Cable, DB25-to-DB25 (10 ft/3 m)	035-0385-1031	9008-F1-523
50-position, 0.5-inch straight exit connector to MS34 connector (HSSI to V.35) adapter cable (1 ft/0.3 m)	035-0375-0031	9580-F1-570
Ethernet 10BaseT cable with 8-pin modular connectors (14 ft/4.3 m)	035-0349-1431	
Power Cable (6 ft/1.8 m; North America)	125-0057-0031	

Index

Numbers

55 hexadecimal, test pattern, 8-19

A

aborting tests, 8-16
Access
  Dial-In, 4-57
  Name, 4-40
  Type, 4-44
Access Level, 5-10, 5-11
  assigning, 5-9
  COM port, 4-54
  Modem port, 4-60
  security, 2-1
  Session, 4-42
adding, SLV units to network, 11-3
Alarm, 8-7
  (Fail), 6-4, 6-6, 6-8
  adding manually, 10-11
  conditions, 8-2, 8-7
  editing, 10-9
  LED is lit, 8-11
  RMON defaults, B-15
  using template, 10-8
ALM, LED, 6-4, 6-6, 6-8
Alternate
  Dial-Out Directory, 4-49
  IP Address, 4-58
  software revision, 6-2
  Subnet Mask, 4-58
Alternate Destination
  DLCI, 4-31
  EDLCI, 4-31
  Link, 4-30
Alternate Frame Relay Link, 4-39
Annex A and D, LMI Protocol, 4-23
ARP, inverse, 1-4
assigning, community names and access levels, 5-9
AT commands, 4-57
At-a-Glance report, 11-6
authentificationFailure trap, B-7
Auto-Configuration, 1-3, 2-4
  Active, 6-18
  setting up, 4-6
Auto-rating, 8-7
availability, LMI and PVC, 1-4

B

back door access when locked out, 8-4
Back-to-Back
  Mode Active, 6-18
  operation, setting up, 4-12
Backspace, 2-6
Bc, 4-27
Be, 4-28
blank, field value, 2-9
branches/menus, 2-4
bursting, port, 1-4

C

Call Directories, 4-5
Call Retry, 4-48
central clock, 1-4
changing
  configuration options, 3-5
  domains and groups, 10-6
  operating mode, 4-12
  software release, 7-5
Character
  Length, 4-52
  matching, 2-9
CIR, 4-27
  statistics, 6-30
Clearing
  Event, LMI, 4-15, 4-24
  existing information, 4-4
clearing statistics, 6-29
Clock
  Invert Transmit, 4-22
  out of range, 6-18, 8-7
  setting system, 4-4
  Source, Transmit, 4-21

COM port, 4-46, 4-57
  as default IP destination, 4-34
  configuration options, 4-52
  connector, C-3
  set up for trap dial-out, 4-5
Committed Burst Size Bc (Bits), 4-27
Committed Information Rate (CIR), 4-27
Communication Port, configuration options, 4-52
Community Name, 4-40
  assigning, 5-9
Concord Network Health, compatibility, 11-1
Configuration
  Auto, Active, 6-18
  displaying and changing options, 3-4
  menu, 3-2
  menu/branch, 2-4
  option areas, 3-3
  option tables, 4-13
  saving options, 3-6
  tables, 3-3
  upload/download, 1-5
configuring
  added SLV units/elements, 11-4
  DLCI records manually, 4-26
  frame relay options, 4-23
  NetScout Manager Plus, 10-3
  System options, 4-13
  the system, 3-2
Connectivity, setting up service provider, 4-11
connectivity, 8-19
Control
  keys, 2-6
  lead descriptions, 6-6, 6-8
  menu/branch, 2-4
Control Leads
  displaying status, 6-6
  Ignore, 4-53
controlling
  async terminal access, 5-3
  external device access, 5-4
  FTP access, 5-5
  SNMP access, 5-8
  Telnet access, 5-5
conversation elements, 11-3
copyrights, A
CRC, 6-36
creating
  a login, 5-11
  new PVC connections/management links, 3-5
  user history files, 10-13
crossover cable, EIA-232, C-4
CTS
  control lead, 6-7
  down alarm, 8-7
  down Health and Status message, 6-18
current software revision, 6-2

D

Data
  Delivery Ratio (DDR), 1-3
  Link Control Identifier (DLCI), 4-38, 4-39
  Port, physical options, 4-21
  Rate (Kbps), 4-52
  rate, network interface, 4-19
  rate, user data port, 4-21
  rates supported, D-3
  selection criteria, 2-1
  uploading SLV and packet capture, 7-6
Data Port, network interface options, 4-19
Date & Time setting, 4-4
DB25, COM Port, connector, C-3
DB25-to-DB25
  crossover cable, C-4
  straight-through cable, C-13, C-14
DB25-to-V.35
  DTE adapter, C-11, C-12
  network cable, C-10
  V.35 network cable, C-9
DB25-to-X.21
  adapter cable, C-8
  network cable, C-7
DBM
  Health and Status messages, 6-18
  test status messages, 6-20
DDR, 1-3
DE, Set, 4-37
Default Gateway Address, for Ethernet port, 4-51
Default IP Destination, 4-34
Delete key, 2-6
deleting, a login, 5-12
Destination, 4-46
  Default IP, 4-34
  DLCI, 4-30
  EDLCI, 4-30, 4-31
  Link, 4-30

Device
messages, 6-11
troubleshooting problems, 8-11
Dial-In Access
external modem, 4-57
Modem port, 4-59
Dial-Out
Delay Time (Min), 4-48
Directory, 4-49
options, 4-5, 4-45
Trap, 4-48
Directory, Alternate Dial-Out, 4-49
disabling, SNMP access, 5-8
Discard Eligible (DE), 4-37
Disconnect Time
COM port, 4-54
Modem port, 4-60
Telnet session inactivity, 4-42
discovering elements/DLCIs, 11-3
Discovery
frame relay (FR), 4-7
Frame Relay Mode, saving a mode change, 4-9
displaying
configuration options, 3-4
identity information, 6-2
LEDs and control leads, 6-6
DLCI, 4-38, 4-39
Destination, 4-30, 4-31
Down, 6-18, 8-7
on SLV Timeout, 4-16
interface status, 6-22
monitoring user history, 10-16
Number, 4-26
Priority, 4-28
Records, 4-26
Source, 4-29
statistics, 6-32
status, 6-21
Traps on Interfaces, 4-47
Type, 4-26
domains and groups
correcting, 10-6
verifying, 10-5
download, 7-4
capability, 1-5
downloading
determining when completed, 7-5
MIBs and SNMP traps, B-2
SLV alarms, 10-8
software, 7-2
user history file, 10-13
DSR, control lead, 6-7, 6-9
DTE
Loopback, 8-20
port-initiated loopbacks, 4-22
DTLB, 8-20
DTR
control lead, 6-7, 6-9
down from Port-1 Device, 6-18, 8-8
Ignore Control Leads, 4-53

E

Easy Install, configuration options, 4-3
EDLCI, 4-38, 4-39
Destination, 4-30, 4-31
Source, 4-29
EIA-232, crossover cable, C-4
EIA-530-A
connector, C-6
straight-through cable, C-13
to-V.35
DTE adapter, C-11
network cable, C-9
to-X.21
adapter cable, C-8
network cable, C-7
EIR, statistics, 6-30
elements/DLCIs, 11-3
Embedded Data Link Connection Identifier (EDLCI), 4-29, 4-30, 4-31, 4-38, 4-39
ending a session, 2-3
enforcement, of CIR and EIR, 4-14
Enter (Return) key, 2-6
entering, system information, 4-4
enterprise-specific traps, B-12
enable/disable, 4-46
equipment list, E-1
Error, Event, LMI, 4-15, 4-24
Errors, frame relay statistics, 6-34, 6-35
Esc key, 2-6

Ethernet, statistics, 6-37
Ethernet port
  as default IP destination, 4-34
  MAC address, 6-2
  user interface options, 4-50
even parity, 4-53
Event Log, Traps, 6-38
exception points, 11-7
Excess Burst Size (Bits), 4-28
External
  Device, controlling access, 5-4
  Modem
    (on Com Port) options, 4-57
    Commands, 4-57
    set up for trap dial-out, 4-5
  Transmit Clock, 4-21

F

faceplate, 6-3
fan assembly
  cleaning, 12-2
  replacing, 12-3
FDR, 1-3
features, 1-3
field is blank/empty, 2-9
file transfer, 7-2
file transfer protocol (FTP), configuration options, 4-43
Frame Delivery Ratio (FDR), 1-3
Frame Relay
  configuring interface, 4-23
  configuring system, 4-14
  Discovery, 4-7
    saving a mode change, 4-9
  statistics, 6-34
  troubleshooting PVC problems, 8-13
frames, 4-37
front panel assembly
  cleaning, 12-2
  LEDs, 6-3
  replacing, 12-3
FTP, 1-5, 7-2
  configuration options, 4-43
  file transfers, 7-2
  initiating a session, 7-2
  limiting access, 5-5, 5-6
  Login Required, 4-43
  Max Receive Rate (kbps), 4-43
  Session, 5-6
function keys, 2-5, 2-7

G

General
  LEDs, 6-4
  options, 4-18
  SNMP management, options, 4-40
  Traps, 4-46
generating reports, 11-6
glossary, x
grouping elements for reports, 11-5

H

hardware bypass, 1-6
hardware revision, NAM, 6-2
HDLC errors, frame relay statistics, 6-36
Health and Status, 8-2
  messages, 6-18
history
  adding files, 10-13
  installing files, 10-15
  monitoring DLCI, 10-16
hyperlink to more information, highlighted text, xii

I

Identity, displaying, 6-2
Ignore Control Leads, 4-53
Inactivity Timeout, 4-42
  COM port, 4-54
  Modem port, 4-60
indicator LEDs, power supply, 6-10
Initial Route Destination, 4-46
installation and setup, Network Health, 11-2
installing
  Network Health, 11-2
  user history files, 10-15
interface specifications, D-3
Internal, Transmit Clock, 4-21
Inverse ARP, 1-4
Invert Internal Clock, 4-19
Invert Transmit Clock, 4-22
IP
  default destination, 4-34
  node information, 4-32
  Ping test, 8-21
  Validation, NMS, 4-44

IP Address, 4-36, 4-58
for COM port, 4-55
for Ethernet port, 4-50
for Modem port, 4-61
limiting SNMP access through, 5-10
NMS number, 4-44, 4-45
Node, 4-3, 4-33
IP Routing Table, Status screen, 6-26

K

keyboard keys, 2-6
keys
keyboard, 2-6
screen function, 2-5, 2-7

L

Lamp Test, 6-20, 8-22
LAN, adapter and cable, C-3
latency, 1-4
LEDs, 8-2, 8-11
and control leads, displaying, 6-6
descriptions, 6-4
front panel, 6-3
power supply, 6-10
lights, power supply, 6-10
limiting
async terminal access, 5-3
FTP access, 5-6
SNMP access, 5-8
through IP addresses, 5-10
Telnet access, 5-5
Link
Destination, 4-30
frame relay statistics, 6-34
Protocol, 4-55
Source, 4-29
Traps, 4-47
Traps Interfaces, 4-47
troubleshooting management, 8-5
TS Management, 4-35
linkUp and linkDown
events, 4-47
traps, B-8
LMI
and PVC availability, 1-4
Behavior, 4-14
Clearing Event (N3), 4-15, 4-24
configuring frame relay and, 4-14
Down, 6-19, 8-9
Error Event (N2), 4-15, 4-24
frame relay statistics, 6-35
Heartbeat (T1), 4-15, 4-25
Inbound Heartbeat (T2), 4-15, 4-25
N4 Measurement Period (T3), 4-15, 4-25
packet utility, 8-5
Parameters, 4-24
pass-through, 4-14
Protocol, 4-23
Status Enquiry (N1), 4-15, 4-24
uploading packet capture data, 7-6
local
external DTE loopback, 4-22
setting up management, 4-10
locked out, 5-11, 8-4
logging in, 2-2
logging out, 2-3
Login
creating, 5-11
ID, 5-11
modifying and deleting, 5-12
Required, 4-41, 4-53, 4-59, 5-3, 5-5, 5-6
security information, 5-1
Loopback
DTE, 8-20
Port (DTE) Initiated, 4-22
PVC, 8-18
LOS
at Network, 6-19, 8-10
LED, 6-4

M

MAC address, 6-2
Main Menu, screen/branch, 2-4
making input selections, 2-9
Management
  and Communication, options, 4-32
  General SNMP, options, 4-40
  OpenLane 5.0, 1-5
  PVCs, 4-36
    total number dedicated, 1-4
  setting up local, 4-10
  SNMP, 4-40
  troubleshooting link, 4-32, 8-5
menu
  branches, 2-4
  Configuration, 3-2
  main, 2-4
  path, 2-5
  selecting from, 2-8
  structure, A-1
messages
  Device, 6-11
  Health and Status, 6-18
  Self-Test Results, 6-17
  system, 2-5
  System and Test Status, 6-17
  Test Status, DBM, 6-20
MIB
  access, 5-9
  downloading, B-2
  support, B-2
minimal remote configuration, 3-6
Mode
  changing Operating, demos, 4-12
  Test, 6-4, 6-6, 6-8
model number, 2-5
modem
  Health and Status messages, 6-18
  setting up, 4-5
    trap dial-out, 4-5
Modem port
  as default IP destination, 4-34
  controlling access, 5-4
  user interface options, 4-59
modifying, a login, 5-12
Monitor
  DTR, 4-22
  RTS, 4-22
  test pattern, 8-19
Monitor CTS, 4-20
Monitor DSR, 4-20
monitoring
  DLCI history data, 10-16
  FrameSaver unit, 6-16
  LEDs and control leads, 6-6
  using NetScout Manager Plus, 10-19
monitoring the unit, 6-1
Multiplexed
  DLCI, 4-29, 4-30, 4-31, 4-38, 4-39
  DLCI Type, 4-26
  PVCs, 8-19

N

N1, LMI Status Enquiry, 4-15, 4-24
N2, LMI Error Event, 4-15, 4-24
N3, LMI Clearing Event, 4-15, 4-24
Name, 4-36
  1 or 2 Access, 5-9
  Access, 4-40
  Community, 4-40
navigating the screens, 2-6
Net Link, Port Use, 4-52, 4-59
NetOnly, 4-7
NetScout
  Manager Plus, NMS support, 1-6
  NMS support, 1-1
Network
  Com Link Down, 6-19
  data port, LED, 6-5
  data port connector, C-6
  data rate, 4-19
  data rates supported, D-3
  DLCI records, options, 4-26
  Health (Concord) reports, 11-1
  interface status, 6-25
  latency, 1-4
  physical options, 4-19
  PVC Loopback, 8-18
  reference time, 1-4
Network Health, installation and setup, 11-2
NMS
  IP Address, 4-44, 4-45, 5-10
  IP Validation, 4-44, 5-10
  OpenLane management solution, 1-5
  SNMP security, options, 4-44
Node
  IP Address, 4-3, 4-33
  Subnet Mask, 4-3, 4-33

Node IP, configuration option tables, 4-32
NSP, 4-14
NTU, 1-1
Number of
  Managers, 4-44, 5-10
  Trap Managers, 4-45

O

odd parity, 4-53
OID
  (object identification), user history file, 10-13
  cross-reference (numeric order), B-24, B-28
OK, LED, 6-4, 6-5
OpenLane
  SLM solution, 1-5
  SLM support, 9-1
operating, changing mode for demos, 4-12
organization of this document, ix
Out of Sync, message, 8-13, 8-19
Outbound Management Priority, 4-28

P

packet capture
  uploading data, 7-6
  utility, 8-5
packets, 4-37
Parity, 4-53
Password, 5-11
patents, A
pattern, send/monitor, 8-18
performance statistics, 6-28, 8-2
  clearing, 6-29
Performance Wizard, copying directory, 10-2
physical
  data port options, 4-21
  tests, 8-20
pin assignments
  COM Port, EIA-232 connector, C-3
  COM port, to-LAN cables, C-3
  crossover cable, EIA-232, C-4
  DB25-to-DB25, straight-through cable, C-14
  EIA-530-A connector, C-6
  V.35 DTE adapter, C-12
  V.35 network cable, C-10
  X.21 DTE adapter cable, C-8
  X.21 network cable, C-7
Ping test, 8-21
policing, of CIR and EIR, 4-14
Port
  (DTE) Initiated Loopbacks, 4-22
  Access Level, 4-54, 4-60, 5-3
  bursting, 1-4
  communication, options, 4-52
  control leads, 6-7, 6-9
  Ethernet, options, 4-50
  Modem, options, 4-59
  PVC Loopback, 8-18
  Type, network data port, 4-19
  Type, user data port, 4-21
  Use, 4-52, 4-59
POST, enable/disable, 4-18
power module, replacing, 12-4
power–on self–test, enable/disable, 4-18
PPP, 4-55
Primary Destination
  DLCI, 4-30
  EDLCI, 4-30
  Link, 4-30
Primary Frame Relay Link, 4-37
Primary Link RIP, 4-38
printed reports, 11-7
problem indicators, 8-2
product-related documents, xi
Proprietary, RIP, 4-38, 4-56
Protocol
  address resolution, 1-4
  Link, 4-55
  LMI, 4-23
  Point-to-Point (PPP), 4-55
  Routing Information (RIP), 4-38, 4-56
  Serial Line, IP (SLIP), 4-55
  Simple Network Management (SNMP), 4-40
PVC
  availability, 1-4
  connection status, 6-23
  connections, 4-29
    total number, 1-4
  Management, 4-36
    total number dedicated, 1-4
  name, 4-34, 4-35, 4-46
  Network Loopback, 8-18
  tests, 8-17
  troubleshooting problems, 8-13

Q

quality of service, 4-28
Quick Reference, 3-3

R

ratios, FDR and DDR, 1-3
RD, control lead, 6-9
rear panel, C-2
remote, units, minimal configuration, 3-6
reports, Network Health, 11-7
resetting
  statistics, 6-29
  the unit, 8-3
  unit default configuration options, 8-4
restoring communication with a misconfigured unit, 8-4
retrieving statistics, 7-6
Return (Enter) key, 2-6
revision, software and hardware, 6-2
RFC 1213 and 1573, B-2
RFC 1315, B-2
RFC 1604, B-2
RFC 1659, B-2
RFC 1757, B-2
RFC 2021, B-2
right arrow key, 2-6
RIP, 1-4, 4-11, 4-56
RLSD, control lead, 6-7
RMON
  alarm and event defaults, B-15
  Specific Traps, B-14
  Traps, 4-47
  user history collection, 1-4
router, setting up to receive RIP, 4-11
router-independence, 1-4, 4-14
Routing, Information Protocol (RIP), 4-56
RTS, control lead, 6-7
running reports, 11-6
RXD, control lead, 6-7

S

Sampling, SLV Inband and Interval, 4-16
saving configuration options, 3-6
screen
  area, 2-5
  function keys area, 2-5
  how to navigate, 2-6
scrolling through valid selections, 2-9
security, 1-3, 2-1, 2-2, 3-5, 5-1
  SNMP NMS, options, 4-44
selecting
  a field, 2-9
  from a menu, 2-8
Self-Test
  enable/disable, 4-18
  results messages, 6-17
Send, test pattern, 8-18
serial number, NAM, 6-2
Service, A
service level
  management, 1-1
  reports, 11-6
  verification
    configuring, 4-16
    statistics, 6-30
  verifier (SLV), 1-1
service provider, management, control/connectivity, 4-11
Session
  Access Level, 4-42, 5-5, 5-7
  ending, 2-3
  starting, 2-2
Set DE, 4-37
setting
  Date & Time (system clock), 4-4
  date and time, 4-4
setting up
  auto-configuration, 4-6
  external modem, 4-5
  local management, 4-10
  service provider connectivity, 4-11
  SNMP trap managers, 4-44
  so router can receive RIP, 4-11
SLA, 1-3, 1-5
SLIP, 4-55
SLM, ix, 1-1
  OpenLane, 9-1

SLV
(service level verifier), 1-1
configuring, 4-16
Delivery Ratio, 4-16
DLCI Down on Timeout, 4-16
Packet Size, 4-17
performance statistics, 6-30
reports, 1-3
Sample Interval (secs), 4-16
Synchronization Role, 4-17
Timeout, Error Event Threshold, 4-16, 4-17
SNMP
assigning community names/access levels, 5-9
limiting access, 5-8, 5-10
Management, 4-40, 5-8
NMS security, options, 4-44
Number of Managers, 4-44
setting up Trap Managers, 4-44
Traps, 4-45
downloading, B-2
standards, B-6
supported, 8-2
software
changing, 7-5
download, 1-5
downloading, 7-2
revision, NAM, 6-2
Source
DLCI, 4-29
EDLCI, 4-29
Link, 4-29
Spacebar, 2-6
specifications, technical, D-1
speed
network interface, 4-19
user data port, 4-21
Standard_out RIP, 1-4
standards compliance for SNMP Traps, B-6
starting
a session, 2-2
a test, 8-15
statistics, 1-4, 6-28
elements, 11-3
uploading to an NMS, 7-6
Status
DLCI, 6-21
Enquiry, LMI, 4-15, 4-24
Health and, 6-18
information, 6-16
LED, 6-4
menu/branch, 2-4
PVC connection, 6-23, 6-24, 6-25
test messages, 6-20
Stop Bits, 4-53
stopping a test, 8-15
Subnet Mask, 4-58
for COM port, 4-55
for Ethernet port, 4-50
for Modem port, 4-61
interface, 4-37
Node, 4-3, 4-33
suggestions, user documentation, A
summary, network report, 11-7
switching
between screen areas, 2-8
to new software, 7-5
System
and test status messages, 6-17
configuring options, 4-13
displaying information, 6-2
Frame Relay and LMI, options, 4-14
General options, 4-18
messages, 2-5
Name, Contact, and Location, 6-2
setting the clock (data & time), 4-4

T

T1, LMI Heartbeat, 4-15, 4-25
T2, LMI Inbound Heartbeat, 4-15, 4-25
T3, LMI N4 Measurement Period, 4-15, 4-25
Tab key, 2-6
Tc, 4-27
TCP, 7-2
TD, control lead, 6-9
technical specifications, D-1
Telnet
limiting access, 5-5
Session, 5-5
user interface options, 4-41
Terminal, Port Use, 4-52, 4-59

Terminal port
as default IP destination, 4-34
configuration options, 4-52
connector, C-3
Port Use, 4-52
Test
menu/branch, 2-4
Mode, 6-4, 6-6, 6-8
Status messages, DBM, 6-20
Tests, 1-4
aborting, 8-16
available, 8-14
DTE Loopback, 8-20
Duration, 4-18
IP Ping, 8-21
Lamp, 8-22
physical, 8-20
PVC, 8-17
PVC Loopback, 8-18
starting or stopping, 8-15
test pattern, 8-18
Timeout, 4-18, 8-14
through PVC connections, total number, 1-4
throughput, 1-4
time, setting, 4-4
Timeout
Inactivity, 4-42, 4-54, 4-60
Test, 8-14
TM, control lead, 6-7
trademarks, A
traffic, policing, 4-14
Training, A
transferring data, 7-6
Transmit Clock
Invert, 4-22
Source, 4-21
Trap
Dial-Out, 4-48
Disconnect, 4-48
Managers, Number of, 4-45
Traps
authentificationFailure, B-7
DLCI, 4-47
Enterprise Specific, 4-46, B-12
Event Log, 6-38
General, 4-46
Link, 4-47
Link Interfaces, 4-47
linkUp and linkDown, B-8
RMON, 4-47
RMON Specific, B-14
SNMP and dial-out, options, 4-5, 4-45
standards, B-6
supported, 8-2
warmStart, B-7
Trend, report, 11-7
troubleshooting, 8-1
creating a management link, 4-32
device problems, 8-11
frame relay PVC problems, 8-13
management link, 8-5
power supply problems, 6-10
tables, 8-11
TruePut, 1-3
TS Management Link, 4-32, 4-35
Access Level, 4-35
access level, 5-7
limiting Telnet access, 5-5, 5-7
TST, LED, 6-4, 6-6, 6-8
TXD, control lead, 6-7
Type, Access, 4-44

U

UNI, 1-3, 4-15, 4-24, 4-25
upgrading, system software, 7-4
upload/download capability, 1-5
uploading data, 7-6
user data port
connector, C-6
data rate, 4-21
LED, 6-5
rates supported, D-3
user history
adding files, 10-13
installing files, 10-15
monitoring DLCI, 10-16
statistics gathering, 1-4
user interface
cannot be accessed, 8-11
COM port, set up external modem for trap dial-out, 4-5
communication port, options, 4-52
Ethernet port, options, 4-50
external modem (on Com port), options, 4-57
Modem port, options, 4-59
resetting/restoring access, 8-4
Telnet session, 4-41
user-defined history, 10-13

V

V.35, cable kit, C-9, C-11
Value Out of Range message, 4-26, 4-27
variable-bindings, B-9, B-14
VCI, 1-5
viewing, packet capture results, 8-6
virtual path or channel identifier, 1-5
VPI, 1-5

W

warmStart
  events, General Traps, 4-46
  trap, B-7
warranty, A
Web-site
  access to documentation, xi
  glossary, x

X

X.21, cable kit, C-7, C-8