

FrameSaver[®] SLV
Models 9126, 9128, and 9128-II
USER'S GUIDE

Document No. 9128-A2-GB20-40

November 2000

Copyright © 2000 Paradyne Corporation.
All rights reserved.
Printed in U.S.A.

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773.

Paradyne Corporation makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, Paradyne Corporation reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Paradyne Corporation to notify any person of such revision or changes.

Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

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

ACCULINK, COMSPHERE, FrameSaver, Hotwire, and NextEDGE are registered trademarks of Paradyne Corporation. MVL, OpenLane, Performance Wizard, and TruePut are trademarks of Paradyne Corporation. All other products and services mentioned herein are the trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

Patent Notification

FrameSaver 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 the FrameSaver SLV

■ System Overview	1-1
■ FrameSaver SLV Features	1-2
Additional FrameSaver SLV 9128 Features	1-6
FrameSaver SLV 9128-II Only Features	1-7
■ OpenLane SLM System	1-7
■ NetScout Manager Plus and NetScout Probes	1-8

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

■ Basic Configuration	3-3
Configuration Option Areas	3-4
Accessing and Displaying Configuration Options	3-5
Changing Configuration Options	3-6
Saving Configuration Options	3-7
■ Using the Easy Install Feature	3-8
■ Setting Up So the Router Can Receive RIP	3-9
■ Entering System Information and Setting the System Clock	3-9
■ Setting Up the Modem	3-10
Setting Up Call Directories for Trap Dial-Out	3-10
Setting Up to Use the Modem PassThru Feature	3-11
■ Setting Up Auto-Configuration	3-12
Selecting a Frame Relay Discovery Mode	3-13
Automatically Removing a Circuit	3-15
■ Setting Up Dial Backup	3-16
Setting Up the DBM Physical Interface	3-16
Setting Up Automatic Backup Configuration	3-17
Modifying ISDN Link Profiles	3-20
Restricting Automatic Backup and Configuring Backup Timers	3-21
Configuring the DBM Interface to Send SNMP Traps	3-22
Assigning DLCIs to a Backup Group	3-22
■ PVC Backup Over the Network Interface	3-23
■ Setting Up Back-to-Back Operation	3-23
Changing Operating Mode	3-23
■ Configuration Option Tables	3-24
■ Configuring the Overall System	3-25
Configuring Frame Relay and LMI for the System	3-25
Configuring Service Level Verification Options	3-28
Configuring General System Options	3-30
■ Configuring Physical Interfaces	3-33
Configuring the Network Interface	3-33
Configuring a User Data Port	3-37
Configuring the DSX-1 Interface	3-42
Configuring the ISDN DBM Interface	3-44
Setting Up ISDN Link Profiles	3-48

■ Assigning Time Slots/Cross Connections	3-50
Assigning Frame Relay Time Slots to the Network Interface	3-51
Assigning DSX-1 Time Slots to the Network Interface	3-52
Assigning a Synchronous Data Port to Network or DSX-1 Time Slots	3-58
Clearing Assignments	3-59
■ Configuring Frame Relay for an Interface	3-60
■ Manually Configuring DLCI Records	3-63
■ Configuring PVC Connections	3-66
■ Setting Up Management and Communication Options	3-69
Configuring Node IP Information	3-70
Configuring Management PVCs	3-72
Configuring General SNMP Management	3-76
Configuring Telnet and/or FTP Session Support	3-77
Configuring SNMP NMS Security	3-80
Configuring SNMP Traps and Trap Dial-Out	3-81
Configuring the Ethernet Port	3-86
Configuring the Communication Port	3-88
Configuring the Modem Port	3-92
■ Configuring the Criteria for Automatic Backup	3-96

4 Security and Logins

■ Limiting Access	4-2
■ Controlling Asynchronous Terminal Access	4-2
■ Limiting Dial-In Access via the Modem Port	4-4
■ Controlling ISDN Access	4-5
ISDN Call Security	4-5
Disabling ISDN Access	4-5
■ Controlling Telnet or FTP Access	4-6
Limiting Telnet Access	4-6
Limiting FTP Access	4-7
Limiting Telnet or FTP Access Over the TS Access Management Link	4-8
■ Controlling SNMP Access	4-9
Disabling SNMP Access	4-9
Assigning SNMP Community Names and Access Levels	4-10
Limiting SNMP Access Through IP Addresses	4-11
■ Creating a Login	4-12
■ Modifying a Login	4-13
■ Deleting a Login	4-13

5 Operation and Maintenance

■ Displaying System Information	5-3
■ Viewing LEDs and Control Leads	5-5
FrameSaver SLV 9126 LEDs and Control Leads	5-5
FrameSaver SLV 9128/9128-II LEDs and Control Leads	5-6
LED Descriptions	5-7
Control Lead Descriptions	5-10
■ Device Messages	5-11
■ Status Information	5-17
System and Test Status Messages	5-18
Network LMI-Reported DLCIs Status	5-28
PVC Connection Status	5-30
Time Slot Assignment Status	5-33
DBM Interface Status	5-35
■ IP Routing Table	5-45
■ Performance Statistics	5-47
Clearing Performance Statistics	5-48
Service Level Verification Performance Statistics	5-49
DLCI Performance Statistics	5-51
Frame Relay Performance Statistics	5-53
ESF Line Performance Statistics	5-57
DBM Call Performance Statistics	5-60
Ethernet Performance Statistics	5-61
■ Trap Event Log	5-62
■ Modem Operation	5-63
Activating the Modem PassThru Feature	5-63
Canceling Modem PassThru Operation	5-63
Manually Disconnecting the Modem	5-64
Verifying Modem Operation	5-64
■ ISDN DBM Operation	5-65
Forcing Backup (Disruptive)	5-65
Placing a Test Call (Nondisruptive)	5-66
Verifying ISDN Lines	5-67
Verifying That Backup Can Take Place	5-67
■ FTP File Transfers	5-68
Upgrading System Software	5-70
Upgrading ISDN BRI DBM Software	5-71
Determining Whether a Download Is Completed	5-72
Changing Software	5-72
Transferring Collected Data	5-73
■ Turning Off the System Alarm Relay	5-74

6 Troubleshooting

■ Problem Indicators	6-2
■ Resetting the Unit and Restoring Communication	6-3
Resetting the Unit from the Control Menu	6-3
Resetting the Unit By Cycling the Power	6-3
Restoring Communication with a Misconfigured Unit	6-4
■ Troubleshooting Management Link Feature	6-5
■ LMI Packet Capture Utility Feature	6-5
Viewing Captured Packets from the Menu-Driven User Interface ...	6-6
■ Alarms	6-7
■ Viewing the Trap Event Log	6-14
■ Troubleshooting Tables	6-14
Device Problems	6-14
Frame Relay PVC Problems	6-16
ISDN DBM Problems	6-17
■ Tests Available	6-18
Test Timeout Feature	6-19
DBM Tests	6-19
■ Starting and Stopping a Test	6-20
Aborting All Tests	6-21
■ PVC Tests	6-22
PVC Loopback	6-23
Send Pattern	6-24
Monitor Pattern	6-24
Connectivity	6-25
Test Call	6-25
■ Physical Tests	6-26
Line Loopback	6-27
Payload Loopback	6-28
Repeater Loopback	6-29
DTE Loopback	6-30
Send Line Loopback	6-31
Data Channel Loopbacks on a Frame Relay Link	6-32
Send Remote Line Loopback	6-33
Send and Monitor Pattern Tests	6-34
■ IP Ping Test	6-35
■ Lamp Test	6-36

7 Setting Up OpenLane for FrameSaver Devices

- OpenLane Support of FrameSaver Devices 7-1
- Setting Up the OpenLane SLM System 7-2
- Setting Up FrameSaver SLV Support 7-3

8 Setting Up NetScout Manager Plus for FrameSaver Devices

- Preparation 8-2
- Configuring NetScout Manager Plus 8-3
 - Adding FrameSaver SLV Units to the NetScout Manager Plus Network 8-4
 - Verifying Domains and Groups 8-5
 - Correcting Domains and Groups 8-6
 - Adding SLV Alarms Using a Template 8-8
 - Editing Alarms 8-9
 - Adding SLV Alarms Manually 8-11
 - Creating History Files 8-13
 - Installing the User-Defined History Files 8-15
- Monitoring a DLCI's History Data 8-16
- Monitoring the Agent Using NetScout Manager Plus 8-18
- Statistical Windows Supported 8-20

9 Setting Up Network Health for FrameSaver Devices

- Installation and Setup of Network Health 9-2
- Discovering FrameSaver Elements 9-3
- Configuring the Discovered Elements 9-4
- Grouping Elements for Reports 9-5
- Generating Reports for a Group 9-6
 - About Service Level Reports 9-6
 - About At-a-Glance Reports 9-6
 - About Trend Reports 9-7
 - Printed Reports 9-7
- Reports Applicable to SLV Devices 9-7

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-3
Paradyne Indexes to the Interface Table (ifTable)	B-3
NetScout Indexes to the Interface Table (ifTable)	B-6
■ Standards Compliance for SNMP Traps	B-8
Trap: warmStart	B-9
Trap: authenticationFailure	B-9
Traps: linkUp and linkDown	B-10
Traps: enterprise-Specific	B-13
Traps: RMON-Specific	B-16
Trap: dialControl	B-17
■ RMON Alarm and Event Defaults	B-18
Physical Interface Alarm Defaults	B-19
Frame Relay Link Alarm Defaults	B-20
DLCI Alarm Defaults – Paradyne Area	B-22
DLCI Alarm Defaults – NetScout Area	B-23
■ Object ID Cross-References (Numeric Order)	B-26

C Connectors, Cables, and Pin Assignments

■ Rear Panels	C-1
■ COM Port Connector	C-3
COM Port-to-PC Cable (Feature No. 3100-F2-550)	C-4
COM Port-to-Terminal/Printer Cable (Feature No. 3100-F2-540) ...	C-4
COM Port-to-Router Cables	C-5
Gender Adapter/Changer	C-8
LAN Adapter Converter and Cable	C-8
■ DTE Port Connector	C-9
Standard V.35 Straight-through Cable	C-10
Standard V.35 Crossover Cable	C-10
■ DSX-1 Connector	C-11
DSX-1 Adapter (Feature No. 9008-F1-560)	C-11
■ T1 Network Cable (Feature No. 3100-F1-500)	C-12
T1 Mass Termination Cable (Feature No. 9007-F1-500)	C-12
Canadian T1 Line Interface Cable (Feature No. 3100-F1-510)	C-13
■ Ethernet Port Connector	C-13
■ Modem Connector	C-14
■ ISDN DBM Connector	C-14
ISDN Modular Cable	C-14

D Technical Specifications

E Equipment List

■ Equipment	E-1
■ Cables	E-4

Index

About This Guide

Purpose and Intended Audience

This document contains information needed to properly set up, configure, and verify operation of the FrameSaver SLV (Service Level Verifier) 9126, 9128, or 9128-II, a T1 frame relay access device. It is intended for system designers, engineers, administrators, and operators.

You must be familiar with the functional operation of digital data communications equipment and frame relay networks.

Document Organization

Section	Description
Chapter 1	<i>About the FrameSaver SLV.</i> Identifies how the FrameSaver SLV 9126 and 9128/9128-II fit into Paradyne's Service Level Management (SLM) solution, and describes its features.
Chapter 2	<i>User Interface and Basic Operation.</i> Shows how to navigate the menu-driven user interface.
Chapter 3	<i>Configuration.</i> Provides configuration information for the FrameSaver SLV 9126 and 9128/9128-II.
Chapter 4	<i>Security and Logins.</i> Provides procedures for controlling access to the FrameSaver SLV and setting up logins.
Chapter 5	<i>Operation and Maintenance.</i> Provides procedures to display unit identification information and perform file transfers, as well as how to display and interpret status and statistical information.
Chapter 6	<i>Troubleshooting.</i> Provides device problem resolution, alarm, and other information, as well as troubleshooting and test procedures.

Section	Description
Chapter 7	<i>Setting Up OpenLane for FrameSaver Devices.</i> Identifies where installation and setup information is located and how FrameSaver units are supported.
Chapter 8	<i>Setting Up NetScout Manager Plus for FrameSaver Devices.</i> Describes setup of the NetScout Manager Plus application so it supports FrameSaver units, and so you can change alarm and history file defaults.
Chapter 9	<i>Setting Up Network Health for FrameSaver Devices.</i> Describes setup of Concord's Network Health application so reports can be created for FrameSaver units, and identifies those reports that apply to FrameSaver units.
Appendix A	<i>Menu Hierarchy.</i> Contains a graphical representation of how the user interface screens are organized.
Appendix B	<i>SNMP MIBs and Traps, and RMON Alarm Defaults.</i> 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	<i>Connectors, Cables, and Pin Assignments.</i> Shows the rear panel, tells what cables are needed, and provides pin assignments for interfaces and cables.
Appendix D	<i>Technical Specifications.</i>
Appendix E	<i>Equipment List.</i>
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
<i>Paradyne FrameSaver Documentation:</i>	
9000-A2-GN19	<i>FrameSaver SLV ISDN Installation Instructions</i>
9000-A2-GN1D	<i>9000 Series Access Carrier Installation Instructions</i>
9126-A2-GL10	<i>FrameSaver SLV 9126 Quick Reference</i>
9126-A2-GN10	<i>FrameSaver SLV 9126 1-Slot Unit Installation Instructions</i>
9128-A2-GL10	<i>FrameSaver SLV 9128/9128-II Quick Reference</i>
9128-A2-GN10	<i>FrameSaver SLV 9128 1-Slot Housing-to-9000 Series Access Carrier Upgrade Instructions</i>
9128-A2-GN11	<i>FrameSaver SLV 9128/9128-II Network Access Module (NAM) Installation Instructions</i>
9128-A2-GN12	<i>FrameSaver SLV 9128/9128-II 1-Slot Unit Installation Instructions</i>
<i>Paradyne OpenLane NMS Documentation:</i>	
7800-A2-GZ41	<i>OpenLane 5.x Service Level Management for UNIX Quick Start Installation Instructions</i>
7800-A2-GZ42	<i>OpenLane 5.x Service Level Management for Windows NT Quick Start Installation Instructions</i>
<i>NetScout Documentation:</i>	
2930-170	<i>NetScout Probe User Guide</i>
2930-610	<i>NetScout Manager/Plus User Guide</i>
2930-620	<i>NetScout Manager/Plus & NetScout Server Administrator Guide</i>
2930-788	<i>NetScout Manager Plus Set Up & Installation Guide</i>
<i>Concord Communications Documentation:</i>	
09-10010-005	<i>Network Health User Guide</i>
09-10020-005	<i>Network Health Installation Guide</i>
09-10050-002	<i>Network Health – Traffic Accountant Reports Guide</i>
09-10070-001	<i>Network Health Reports Guide</i>

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
<i>Italic</i>	To indicate variable information (e.g., DLCI <i>nnnn</i>).
<i>Menu sequence:</i>	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, <i>Main Menu</i> → <i>Status</i> → <i>System and Test Status</i> 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 more than one selection is available (e.g., <i>Performance Statistics</i> → <i>Status</i> → [<i>Network/Port-1</i>]).
Text highlighted in red	To indicate a hyperlink to additional information when viewing this manual online. Click on the highlighted text.

About the FrameSaver SLV

1

This chapter includes the following:

- *System Overview*
- *FrameSaver SLV Features*
 - *Additional FrameSaver SLV 9128 Features*
 - *FrameSaver SLV 9128-II Only Features*
- *OpenLane SLM System*
- *NetScout Manager Plus and NetScout Probes*

System Overview

Our system solution consists of:

- FrameSaver® SLV (Service Level Verifier) units
- OpenLane™ SLM (Service Level Management) system
- NetScout Manager Plus application
- Standalone NetScout Probes, if needed

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

FrameSaver SLV 9126, 9128, and 9128-II units operate with other FrameSaver devices, and when teamed with internationally based FrameSaver devices in multinational applications, provide a complete global frame relay management solution.

FrameSaver SLV Features

FrameSaver SLV units provide the following features:

- **Easy Installation.** Provides a straight-forward installation menu that requires minimal configuration to get the unit up and running quickly, and to set up remote configuration and management via Telnet access from the NOC (Network Operations Center). For a FrameSaver SLV 9128-II, see Easy Installation in *FrameSaver SLV 9128-II Only Features* for additional information.
- **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.
- **TruePut™ Technology.** Using Frame Delivery Ratios (FDR) and Data Delivery Ratios (DDR), throughput (within and above CIR, as well as between CIR and EIR, and above EIR) can be measured precisely, eliminating inaccuracies due to averaging.
- **Intelligent Service Level Verification.** Provides accurate throughput, latency, and availability measurements to determine network performance and whether service level agreements (SLAs) are being met, along with SLA reporting.
- **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.
- **RMON Alarms and Configurable Alarm Thresholds.** Provides the ability to change SLA parameter and RMON alarm thresholds via the OpenLane system to correct them in real-time, before the SLA is violated.
- **Security.** Provides multiple levels of security to prevent unauthorized access to the unit.

- **Auto-Configuration.** Provides the following automatic configuration features:
 - Time Slot Discovery – For automatic configuration of all network DS0 assignments.
 - 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.

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

Feature	FrameSaver SLV 9126	FrameSaver SLV 9128/9128-II
Through Connections (PVCs)	16	120
Dedicated Management PVCs	2	2

- **Multiplexed Management PVCs.** Provides a method of multiplexing management data with customer data transparently over a single PVC (Permanent Virtual Circuit) when FrameSaver devices are at each end of the circuit. This feature also makes it possible to run nondisruptive PVC tests.
- **Multiplexed Customer PVCs.** Provides a method of multiplexing customer management data and user data with network management data transparently over a single PVC when FrameSaver devices are at each end of the circuit.
- **Extensive Testing Capability.** Provides a variety of tests to identify and diagnose device and network problems, including nondisruptive PVC loopbacks and end-to-end connectivity. Tests can be commanded from the unit's menu-driven user interface or the OpenLane system.
 These tests include V.54 or FT1-ANSI data channel loopback support so the frame relay network service provider can perform a physical loopback from its own switch without having to contact the local service provider for loopback activation.
- **LMI Packet Capture.** Provides a way of uploading data that has been captured in a trace file so the data can be uploaded and transferred to a Network Associates Sniffer for analysis, or viewed via the menu-driven user interface. When viewed from the menu-driven user interface, the twelve most recent LMI messages are displayed via the LMI Trace Log.

- **Integral Modem.** Provides an internal 14.4 kbps modem to support dialing in to the unit for out-of-band management and automatic dialing out of SNMP traps.
- **Modem PassThru.** Provides access to another device's VT100-compatible user interface over a dial connection. When this feature is enabled, a logical connection between the unit's modem and COM ports is created, allowing access to a collocated device's serial port via the FrameSaver unit's internal modem. This feature is sometimes referred to as the Router Assist feature.
- **Optional ISDN Backup.** When an ISDN BRI or PRI DBM (Basic Rate Interface or Primary Rate Interface Dial Backup Module) is installed, the following ISDN backup features are provided:
 - Provides automatic dial backup through the ISDN for data when primary frame relay network or access line failures occur, then automatically restores data to the primary route when service returns to normal. Backup is supported regardless of whether or not Caller ID is provisioned on the ISDN circuit. A secondary backup phone number is also available to call when a backup link cannot be established with the primary backup site.
 - Supports simultaneous origination, answering, or origination and answering backup calls, as needed, based upon how the ISDN Link Profile is set up. This feature is also known as peer-to-peer calling.
 - Provides automatic configuration of an alternate route and DLCI for automatically created PVCs at either the remote site or central site based upon the learned far-end DLCI number. When the automatic backup feature is enabled, backup and restoration occur automatically.
 - Provides backup timers that can be configured to better control the amount of time required before backup is initiated, when a backup call will be terminated once the failure condition clears, and a delay before normal service is restored. These features are useful during periods of frequent service disruption.

In addition, round trip latency thresholds can be configured that will initiate backup when configured thresholds are exceeded.
 - Supports backup call groups, where redundant PVCs can be assigned to a specified call group. Using this feature, the unit only goes into backup when *all* PVCs in the group are down, and it returns to normal service as soon as *one* PVC in the group is operational again. This feature is useful when multiple PVCs are going to redundant central sites.
 - When the SLV Sample Interval is set to 10 seconds, provides advance detection of network problems before a DLCI Down indication is received, to minimize data loss.
 - Provides customer premises equipment (CPE) with a Backward Explicit Congestion Notification (BECN) when backup bandwidth is not sufficient for the traffic, allowing the CPE time to slow traffic to the ISDN before the network starts discarding data.
 - Supports Frame Relay Forum Multilink Frame Relay Implementation Agreement – FRF.15 so backup bandwidth can be increased by aggregating multiple B-channels over the ISDN link.

- Supports collection of call and call attempt statistical information that can be viewed from the menu-driven user interface or via SNMP, and supports alarm generation and call security, as well.
- Provides test call capability on ISDN backup links so ISDN and DBM function can be verified before there is an actual primary link failure and switched over to the backup link. Periodic tests are recommended, which can be performed from the menu-driven user interface, or through SNMP commands. Multiple Last Cause Values are also provided to assist in troubleshooting ISDN problems.

FrameSaver SLV 9126 units can be equipped with a BRI DBM, which supports up to two B-channels, which may have a different destination.

FrameSaver SLV 9128 and 9128-II 1-slot units can be equipped with a PRI DBM, which supports up to 23 B-channels, or a BRI DBM. Carrier-mounted FrameSaver SLV 9128 and 9128-II NAMs support a PRI DBM only.

- **Configurable FTP Transfer Rate.** Allows you to control the transmit rate when downloading firmware into the FrameSaver unit and uploading user history statistics to an NMS (Network Management System) via the COM port connection or a management PVC so the data can be transferred as a background task using the standard File Transfer Protocol (FTP) over extended periods of time using low bandwidth.
- **FTP User History Poller.** Provides a bulk collector using FTP through the OpenLane system that generates a file for data at the time that data is uploaded using FTP.
- **Network User History Synchronization.** Allows correlation of RMON2 User History statistics among all SLV devices in a network. Using a central clock, called the network reference time, all SLV device user history statistics are synchronized across the network, further enhancing the accuracy of OpenLane SLV reports.
- **RMON-Based User History Statistics Gathering.** Provides everything needed to monitor network service levels, plus throughput with accurate data delivery, network latency, and LMI and PVC availability. Continuous roundtrip latency testing and reporting, as well as CIR to transmitted and received data performance statistics, are included.

In addition, port bursting statistics are kept for all frame relay links for accurate calculation of utilization.

- **RMON User History Performance Statistics via SNMP Polling.** Provides access to the physical interface and basic frame relay performance statistics by polling the FrameSaver unit using SNMP (Simple Network Management Protocol). These statistics are available real-time via the Enterprise MIB and historically as an RMON2 User History object.
- **Frame Relay Traffic Policing.** Ensures proper alignment and correlation of CIR (Committed Information Rate) values between the FrameSaver unit and the network switch. When this feature is enabled, the unit can enforce CIR and EIR (Excess Information Rate), marking frames that exceed CIR as DE (Discard Eligible) using the same method used by the switch.

- **Service Provider Support.** Provides information and tools useful to network service providers, which includes the following:
 - IP Routing Table – Shows the IP routing table for the FrameSaver unit, with network as well as host routes, the number of hops to the destination, the method by which the route was added to the table, the interface used to get to the destination, and how long the route has been in existence.
 - Trap Event Log – Displays the SNMP (Simple Network Management Protocol) trap event log for the FrameSaver unit from the menu-driven user interface, with the most recent events first, keeping a running total for all trap events stored, the amount of time since the event was logged, plus a description of the trap.
 - Troubleshooting PVC – Provides a dedicated troubleshooting management link that helps service providers isolate problems within their network.
- **ATM VPI/VCI and DLCI Correlation.** For networks with both ATM and frame relay-access endpoints, allows the FrameSaver unit to report the originating Virtual Path and Channel Identifier (VPI/VCI) in the far-end ATM-access endpoint where the local DLCI is mapped so they can be correlated for OpenLane SLV reports.
- **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.
- **DSX-1 Drop/Insert Port.** Allows DTEs/PBXs that support the DS1 signal format to share the T1 network with other high-speed equipment so that voice traffic can share the same local access circuit as the frame relay data.
- **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.

Additional FrameSaver SLV 9128 Features

The following features are unique to FrameSaver SLV 9128 and 9128-II units:

- **Multiple Data Ports.** Provides two data ports instead of one, which have standard connectors so no special-order cables are required.
- **Carrier-Mounted Models.** For customers with high-density requirements, FrameSaver SLV 9128s and 9128-IIs can be ordered as multislots units, called Network Access Modules (NAMs), for insertion in the 14-slot 9000 Series Access Carrier.

FrameSaver SLV 9128-II Only Features

FrameSaver SLV 9128-II units provide a 10/100 BaseT Ethernet LAN interface for management, with automatic sensing of the operation rate of 10Mb or 100Mb, conforming to ANSI/IEEE 802.3.

OpenLane SLM System

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

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

Some of the OpenLane system's features include:

- Real-time performance graphs provide exact performance measurement details (not averages, which can skew performance results) of service level agreement (SLA) parameters.
Port bursting and EIR (Excess Information Rate) performance monitoring graphs are available when the software release for the OpenLane SLM system is Release 5.2, or later.
- 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.
For units with ISDN backup capability, provides ISDN physical interface and PVC testing when the software release for the OpenLane SLM system is Release 5.2, or later.
- Basic configuration allows you to configure FrameSaver devices. 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.
- The maintenance scheduling feature allows for the scheduling of multiple periodic maintenance periods, and provides a record of all scheduled maintenance periods – past, present, and future.

NetScout Manager Plus and NetScout Probes

Provides complete LAN and WAN traffic analysis and monitoring functions for FrameSaver devices.

The following features are supported using this application:

- Thresholds for RMON 1 (Remote Monitoring, Version 1) alarms and events can be configured.
- Performance monitoring can be performed using collected RMON 2 (Version 2) data. NetScout Manager Plus's Protocol Directory and Distribution functionality allows FrameSaver devices 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.

User Interface and Basic Operation

2

This chapter contains information about 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.
- Direct terminal connection over the COM port.

When logging on, the User Interface Idle screen appears.

- If no security was set up or security was disabled, the Main Menu screen appears (see [Main Menu](#) on page 2-4). You can begin your session.
- If security was set up and is enabled, you are prompted for a login. Enter your login ID and password.

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

► Procedure

To log in when security is being enforced:

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

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

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

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

- If two sessions are currently active and you are attempting to access the unit through Telnet, the local Telnet client process returns a **Connection refused**: message at the bottom of the screen.
- If two sessions are currently active and you are attempting to access the unit over the COM port or modem port, not via Telnet, the User Interface Already In Use screen is redisplayed. In addition, the type of connection (Telnet Connection, Direct COM 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** (**E**xit) and press Enter.
 - For a terminal-connected to the COM port, the session is ended.
 - For a terminal-connected to the modem port, the session is ended and the modem is disconnected.
 - For a Telnet connection, the session is closed and, if no other Telnet or FTP session is occurring over the connection, the modem is disconnected.

If ending a session from the Configuration branch, see *Saving Configuration Options* in Chapter 3, *Configuration*.

Main Menu

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

```

main                               Access Level: 1                               9128-II
Device Name: Node A                               05/26/2000 23:32
Slot: 1  Type: T1 FR NAM

                                MAIN MENU

                                Status
                                Test
                                Configuration
                                Auto-Configuration
                                Control
                                Easy Install

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

```

Select ...	To ...
Status	View diagnostic tests, interfaces, PVC connections, and statistics. You can also display LEDs and FrameSaver unit identity information.
Test	Select and cancel 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 also 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.
Easy Install	Configure minimal options for a quick installation.

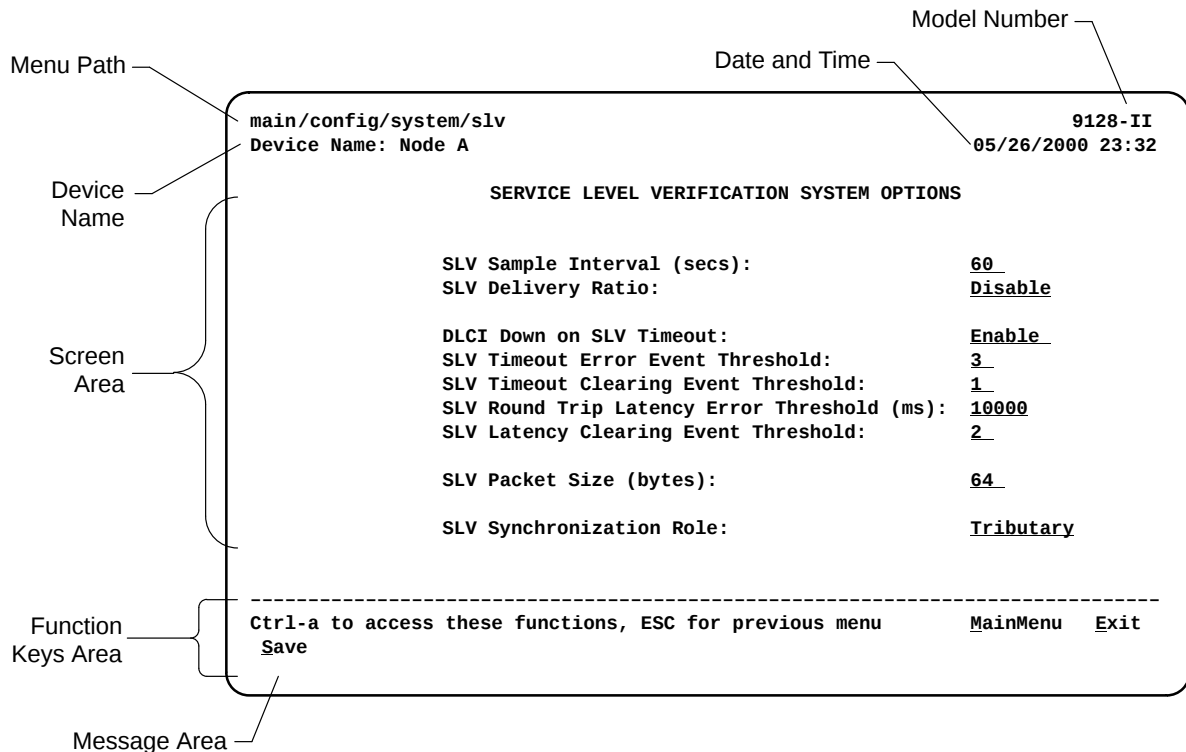
See Appendix A, *Menu Hierarchy*, for a pictorial view of the menu hierarchy, which represents the organization of the FrameSaver unit's menus and screens.

Screen Work Areas

There are two user work areas:

- **Screen area** – Where you input information into fields.
- **Function keys area** – Where you perform specific screen functions.

Below is a sample configuration screen.



Screen Format	Description
Menu Path	Menu selections made to reach the current screen.
Device Name	Customer-assigned identification of the FrameSaver unit.
9126, 9128, or 9128-II	FrameSaver unit's model number.
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 are in the lower left corner. System and Test Status messages are in the lower right corner.

Navigating the Screens

You can navigate the screens by:

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

Keyboard Keys

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

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

Function Keys

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

These keys use the following conventions:

Select . . .	For the screen function . . .	And press Enter to . . .
M or m	<u>M</u> ainMenu	Return to the Main Menu screen.
E or e	<u>E</u> xit	Terminate the asynchronous terminal session.
N or n	<u>N</u> ew	Enter new data.
O or o	<u>M</u> odify	Modify existing data.
L or l	<u>D</u> el e te	Delete data.
S or s	<u>S</u> ave	Save information.
R or r	<u>R</u> efresh	Update screen with current information.
C or c	<u>C</u> lrStats	Clear network performance statistics and refresh the screen. Variations include: ■ <u>C</u>lrSLV&DLCIStats for clearing SLV and DLCI statistics. ■ <u>C</u>lrLinkStats for clearing frame relay link statistics. ■ <u>C</u>lrDBMStats for clearing DBM call statistics.
U or u	Pg <u>U</u> p	Display the previous page.
D or d	Pg <u>D</u> n	Display the next page.

Selecting from a Menu

► Procedure

To select from a menu:

1. Tab or press the down arrow key to position the cursor on a menu selection, or press the up arrow key to move the cursor to the bottom of the menu list.
Each menu selection is highlighted as you press the key to move the cursor from position to position.
2. Press Enter. The selected menu or screen appears.

► Procedure

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

Switching Between Screen Areas

Use Ctrl-a to switch between screen areas (see the example on [page 2-5](#)).

► Procedure

To switch to the function keys area:

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

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

Selecting a Field

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

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

Entering Information

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

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

Example:

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

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

Example:

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

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

Example:

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

If a field is blank and the Message area displays valid selections, press the spacebar; the first valid setting for the field appears. Continue pressing the spacebar to scroll through other possible settings.

This chapter includes the following:

- *Basic Configuration*
 - *Configuration Option Areas*
 - *Accessing and Displaying Configuration Options*
 - *Changing Configuration Options*
 - *Saving Configuration Options*
- *Using the Easy Install Feature*
- *Setting Up So the Router Can Receive RIP*
- *Entering System Information and Setting the System Clock*
- *Setting Up the Modem*
 - *Setting Up Call Directories for Trap Dial-Out*
 - *Setting Up to Use the Modem PassThru Feature*
- *Setting Up Auto-Configuration*
 - *Selecting a Frame Relay Discovery Mode*
 - *Automatically Removing a Circuit*
- *Setting Up Dial Backup*
 - *Setting Up the DBM Physical Interface*
 - *Setting Up Automatic Backup Configuration*
 - *Modifying ISDN Link Profiles*
 - *Restricting Automatic Backup and Configuring Backup Timers*
 - *Configuring the DBM Interface to Send SNMP Traps*
 - *Assigning DLCIs to a Backup Group*
- *PVC Backup Over the Network Interface*

- *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 Physical Interfaces*
 - *Configuring the Network Interface*
 - *Configuring a User Data Port*
 - *Configuring the DSX-1 Interface*
 - *Configuring the ISDN DBM Interface*
 - *Setting Up ISDN Link Profiles*
- *Assigning Time Slots/Cross Connections*
 - *Assigning Frame Relay Time Slots to the Network Interface*
 - *Assigning DSX-1 Time Slots to the Network Interface*
 - *Assigning a Synchronous Data Port to Network or DSX-1 Time Slots*
 - *Clearing Assignments*
- *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*
 - *Configuring the Communication Port*
 - *Configuring the Modem Port*
- *Configuring the Criteria for Automatic Backup*

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 shown below is for a FrameSaver SLV 9128-II with the optional ISDN backup feature.

Configuration Menu

```
main/config                                     9128-II
Device Name: Node A                           5/26/2000 23:32

                                CONFIGURATION EDIT/DISPLAY

                                System
                                Network
                                DSX-1
                                Data Ports
                                ISDN
                                Time Slot Assignment
                                PVC Connections
                                Management and Communication
                                Auto Backup Criteria

-----
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 9126 Quick Reference* or *FrameSaver SLV 9128/9128-II 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.

Using the Easy Install Feature

The Easy Install feature provides a straight-forward installation menu that requires minimal configuration to get the FrameSaver unit up and running quickly, and to set up remote configuration and management via Telnet access from the NOC (Network Operations Center).

Main Menu → Easy Install

Easy Install Screen Example *

```

main/easy_install                                     9128-II
Device Name: Node A                                  5/26/2000 23:32

                                EASY INSTALL

Node IP Address:                                000.000.000.000 Clear
Node Subnet Mask:                               000.000.000.000 Clear
TS Access: DLCI                                980

Create a Dedicated Network Management Link
Ethernet Port Options Screen
Time Slot Assignment Screen

Network 1 Line Framing Format:                    ESF
Network 1 Line Build Out (LBO):                  0.0
Network 1 Line Coding Format:                     B8ZS

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

```

* The Ethernet Port Options Screen only applies to the Model 9128-II.
For the Model 9126 or 9128, DS0 Base Rate (Kbps) appears after the Network 1 Line Coding Format option.

Once the unit is installed and minimal configuration is completed using the Easy Install feature, the NOC can complete configuration of the unit and verify the setup.

To remotely access the FrameSaver unit, use the Dedicated Network Management Link that was created during installation, using the Node IP Address that was entered for the unit.

See the *FrameSaver SLV 9126 1-Slot Unit Installation Instructions*, the *FrameSaver SLV 9128/9128-II 1-Slot Unit Installation Instructions*, or the *FrameSaver SLV 9128/9128-II Network Access Module (NAM) Installation Instructions* for additional information and installation procedures. See *Product-Related Documents* in *About This Guide* for the document number.

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 and FLEX 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 serialx, IP RIP Receive version 1**, then **ctl-z WR**.
2. Create a Standard DLCI for the user data port.
Configuration → Data Ports → DLCI Records
3. Create a Management PVC using the user data port DLCI just configured.
Configuration → Management and Communication → Management PVCs
4. Set Primary Link RIP to Standard_Out, and Save the configuration.

Refer to Table 3-12, [DLCI Record Options](#), and Table 3-15, [Management PVC Options](#) for configuration information.

Entering System Information and Setting the System Clock

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

Main Menu → Control → System Information

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

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

NOTE:

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

See Chapter 4, [Security and Logins](#), to set up and administer logins.

Setting Up the Modem

The unit has an internal modem for dial-in access to the menu-driven user interface, as well as dial-out capability when an SNMP trap is generated. When the modem will be used to dial out, Modem Directory phone numbers need to be set up. Otherwise, simply configure or change dial-in access to the unit.

The modem port is already configured for connection to an asynchronous terminal and dial-in access, with Port Use set to Terminal. However, additional changes may be needed (see Table 3-22, [Modem Port Options](#)).

Main Menu → Configuration → Management and Communication → Modem Port

For dial-in access to the menu-driven user interface via Telnet, make sure Port Use is set to Net Link, the IP address and subnet mask are entered if they are different from the node's, and that the Link Protocol is correct.

For dial-in access to the router connected to the unit's COM port, make sure the Communication Port's Port Use option is set to Modem PassThru.

See [Setting Up Call Directories for Trap Dial-Out](#) when trap dial-out is desired. See [Setting Up to Use the Modem PassThru Feature](#), if this feature is desired. See [Limiting Dial-In Access via the Modem Port](#) in Chapter 4, *Security and Logins*, for additional information.

Setting Up Call Directories for Trap Dial-Out

► 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 to Use the Modem PassThru Feature

Dial-in access to the router is possible via the Modem PassThru feature, also known as the Router Assist feature. The FrameSaver unit's COM port must be connected to the router's auxiliary (AUX) or console port, and the COM port must be configured for this use.

When this feature is set up and active, a logical connection between the unit's modem and COM ports is made, and data received over the modem port is transmitted out the COM port to the router's AUX or console port. When an escape sequence (minus, minus, minus, with a minimum of 50 ms between each) is detected, the FrameSaver unit switches back to normal user interface operation.

See *COM Port-to-Router Cables* in Appendix C, *Connectors, Cables, and Pin Assignments*, for cable information.

► Procedure

1. Configure the COM port to use Modem PassThru.
Main Menu → Configuration → Management and Communication → Communication Port
2. Set Port Use to Modem PassThru.
3. Save the configuration.

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.

Main Menu → Auto-Configuration

Auto-Configuration Screen Example

main/auto-configuration

9128-II

Device Name: Node A

8/18/2000 23:32

AUTO-CONFIGURATION

Frame Relay Discovery Mode:

1MPort

Automatic Circuit Removal:

Enable

Automatic Backup Configuration:

Single Site Backup

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

MainMenu

Exit

Save

This feature also maintains associated DLCI option settings when Standard LMI is used on the network interface.

If an ISDN DBM is not installed, Automatic Backup Configuration does not appear (see [Setting Up Automatic Backup Configuration](#)) for additional information).

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.

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.
2MPorts (only applies to models with multiple data ports)	■ Auto-configuration is enabled on both Port-1 and Port-2. ■ A multiplexed network DLCI containing three EDLCIs is configured for Port-1 customer data, Port-2 customer data, and management data. ■ PVC connections are configured between the network and port DLCIs. ■ A management PVC is configured on the network interface.

Discovery Mode	Configuration Description
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 and when some DLCIs or PVC Connections have been configured manually, edit a selected “discovered” DLCI or PVC connection 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). In this mode, for each DLCI discovered on the network, the unit creates a multiplexed network interface DLCI (which contains two EDLCIs – one for Port-1 data and the other for management), a standard Port-1 DLCI (with the same number as the network interface DLCI), and a Management PVC, then cross-connects them. 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 selecting a 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 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.

If the model has ISDN backup capability, ISDN Link Profiles associated with the deleted records and alternate destinations will be deleted, as well.

Setting Up Dial Backup

When configuring units with ISDN backup capability, the following guidelines apply:

- **Central site** configuration guidelines:
 - Set up the ISDN DBM physical interface.
 - If a BRI DBM, change the Automatic Backup Configuration to `Multi_Site_Backup`. (A PRI DBM is already configured for multisite backup.)
 - Modify the Link Profile(s) that Automatic Backup Configuration created to add a phone number.
- **Remote site** configuration guidelines:
 - Set up the ISDN DBM physical interface.
 - If a PRI DBM, change the Automatic Backup Configuration to `Single_Site_Backup`. (A BRI DBM is already configured for single-site backup.)
 - Modify the `HQ_Site` Link Profile that Automatic Backup Configuration created to add a phone number.
 - Set the criteria by which automatic backup will take place.

Setting Up the DBM Physical Interface

► Procedure

1. Configure the DBM interface.
Main Menu → Configuration → ISDN → Physical
2. Enable the interface, and enter the Service Profile IDs (SPIDs) and local phone numbers.
3. Save the configuration.

See Table 3-7, [ISDN BRI DBM Physical Interface Options](#), or Table 3-8, [ISDN PRI DBM Physical Interface Options](#) for configuration information.

Setting Up Automatic Backup Configuration

The Automatic Backup Configuration feature is used to automatically create alternate DLCI records and PVC connections on the ISDN DBM (backup) interface for current or newly discovered PVC Connections and Management PVCs.

This feature is already set up, with `Single_Site_Backup` as the default for units with a BRI DBM and `Multi_Site_Backup` for units with a PRI DBM. If the unit at the central site has a BRI DBM, change the Automatic Backup Configuration to `Multi_Site_Backup`, if necessary.

Main Menu → Auto-Configuration → Automatic Backup Configuration

If you select . . .	Then . . .
<code>Single_Site_Backup</code> (default for a BRI DBM) <i>(Used at remote sites since only one ISDN link to the central-site is needed.)</i>	Alternate destinations are automatically configured using a single ISDN Link Profile to backup all network PVC Connections and Management PVCs over the primary destination ISDN link. Initially, PVCs with alternate destinations are configured on the first ISDN Link Profile using the same DLCI number as the network DLCI being backed up. However, primary destination PVCs on the ISDN DBM interface are automatically updated to use a different DLCI number for the alternate destination DLCI, derived from the first SLV message received on the each network DLCI.
<code>Multi_Site_Backup</code> (default for a PRI DBM) <i>(Used at central sites since multiple ISDN links are needed, one for each remote-site.)</i>	Alternate destinations are automatically configured using a separate ISDN Link Profile to backup each network PVC Connection and Management PVC over the ISDN interface. Initially, all DLCIs are configured on the ISDN links using the same DLCI number as the network DLCI being backed up. However, primary destination PVCs on the ISDN DBM interface are automatically updated to use a different DLCI number for the alternate destination DLCI, derived from the first SLV message received on the each network DLCI. Automatically created alternate destination Link Profiles appear as <code>Bkupnnnn</code>, <code>nnnn</code> being the DLCI number (e.g., <code>Bkup200</code> would be configured for network DLCI 200).
<code>Disabled</code>	No automatic configuration takes place on the DBM interface and no alternate destinations are created for PVCs.

NOTE:

Changes must be saved to take effect.

See *Setting Up Auto-Configuration* to see a screen example.

When the Automatic Backup Configuration setting is changed, the following prompts appear. No is the default for these prompts.

When the . . .	The following prompt appears . . .	If you select . . .
- Automatic Backup Configuration setting was changed, and <u>S</u>ave was selected	Saving will cause Auto-Configuration to update and Restart. Are you sure?	- No – No Auto-Configuration updates are performed and updates due to LMI response messages are performed according to the previously saved setting. - Yes – The Delete All DLCIs and PVC Connections? prompt appears.
- Response to the Delete All DLCIs and PVC Connections? prompt was <u>N</u>o, and - Automatic Backup Configuration was disabled	Delete All Alternate Destinations from PVC Connections?	- No – No previously configured DLCIs or PVC connections are removed or changed, and newly discovered DLCIs will be configured according to the new discovery mode and automatic backup setting. - Yes – All multiplexed DLCIs, ISDN Link Profiles (except for the first one), and PVC connections are deleted, except for management PVCs with the user data port as the primary destination and management PVCs designated as the TS Management Link. If an alternate destination has been configured on a retained Management PVC, the alternate destination will be deleted but the primary destination will be retained.
- Response to the Delete All DLCIs and PVC Connections? prompt was <u>N</u>o, and - Automatic Backup Configuration was set to <u>S</u>ingle_Site_Backup or <u>M</u>ulti_Site_Backup	Add Alternate Destinations to Current PVC Connections?	- Yes – DLCI records are configured on the ISDN link(s) and Alternate Destination information is added to current PVC connections and management PVCs. - No – No previously configured PVC connections are changed, and newly discovered DLCIs will be configured according to the new discovery mode and automatic backup setting.

When the . . .	The following prompt appears . . .	If you select . . .
■ Response to the Remove Alternate Destinations from PVCs and delete unused DLCI Records? prompt was <u>Yes</u>, and ■ Automatic Backup Configuration was disabled	—	■ No – No previously configured DLCIs, ISDN Link Profiles, or PVC Connections are removed or changed, but updates due to LMI responses will be performed using the new setting. ■ Yes – All Alternate Destination information will be removed from PVC Connections and Management PVCs, and all DLCIs and ISDN Link Profiles (except for the first one) used exclusively as Alternate Destinations are deleted.
■ Response to the Remove Alternate Destinations from PVCs and delete unused DLCI Records? prompt was <u>Yes</u>, and ■ Automatic Backup Configuration was set to <code>Single_Site_Backup</code> or <code>Multi_Site_Backup</code>	Add Alternate Destinations to Current PVC Connections?	■ No – No previously configured PVC Connections are removed or changed, but updates due to LMI responses will be performed using the new setting. ■ Yes – Alternate Destination information is configured for current DLCIs, ISDN Link Profiles, PVC Connections and Management PVCs on the ISDN DBM interface, except for the Management PVC designated as the TS Access Management Link.

NOTE:

When DLCIs, PVC connections, and management PVCs for the first ISDN Link Profile have been configured manually, it is recommended that specific discovered DLCIs, PVC connections, and management PVCs be deleted manually via the Configuration menus. Otherwise, the manual configurations will be deleted along with the automatically configured ones.

To specify when automatic backup is allowed or can occur, see *Setting the Criteria for Automatic Backup*.

Modifying ISDN Link Profiles

Once an ISDN Link Profile is configured using the Automatic Backup Configuration feature, phone numbers and Calling IDs need to be entered. FrameSaver units with ISDN backup capability can originate or answer calls, as needed, so both phone numbers and Calling IDs are needed.

► Procedure

1. Select Link Profiles, then Modify.

Main Menu → Configuration → ISDN → Link Profiles

2. Add a name and phone number to the ISDN Link Profile(s) created by Automatic Backup Configuration.
 - Name for the destination entered (e.g., Tampa). The default setting is HQ_Site for the first ISDN Link Profile.
 - Phone numbers entered:

For Originating a Backup Call	For Answering a Backup Call
Outbound and Alternate Outbound phone numbers Valid characters can include: ■ Numbers (0–9) ■ Special characters * and # ■ Spaces ■ Parentheses ()	Inbound Calling ID1 and ID2 These are the phone numbers of units from which calls will be accepted. Valid characters can include: ■ Numbers (0–9)

NOTES:

Remember to include local dial-out numbers (i.e., 9, then the number). For every originating (outbound) phone number entered, an answering (inbound) phone number must be entered at the far end, and vice versa.

- Maximum Link Rate (Kbps) set to the appropriate speed, if necessary.
 - Caller Identification Method set to Proprietary if call validation is not required. The setting must be the same at both ends of the circuit.
 - An Alternate Outbound Phone Number should a call using the primary Outbound Phone Number be unsuccessful, if desired.
3. Save the configuration.

See Table 3-9, [ISDN Link Profile Options](#), for configuration information.

Restricting Automatic Backup and Configuring Backup Timers

You can specify when auto backup is allowed to occur. If backup is restricted and a backup is active when the allowed time for backups is over, then the backup is terminated and the data is returned to the primary data path regardless of the primary path's condition.

You can restrict auto backup to occur only:

- On certain days of the week
- At certain times of the day

The following additional features can be configured:

- Delays can be configured to control how long the unit will wait before initiating backup when a DLCI is declared down, and how long it will wait to restore service once the DLCI is declared operational again.
- A threshold can be set to determine how many times a primary destination DLCI can transition between Active and Inactive before the unit initiates backup.

► Procedure

To set the criteria and backup timers for automatic backup:

1. Enable Auto Backup.

Main Menu → Configuration → Auto-Backup Criteria

When a failure occurs, the unit automatically enables the Alternate Link and traffic is rerouted over the backup (alternate) interface.

2. Specify the amount of delay after a DLCI is declared down before backup is initiated (DLCI Down Backup Activation Delay).
3. Set the threshold for transitions of the DLCI's status before backup is initiated (DLCI Down Backup Activation Transmission Threshold).
4. Specify the amount of delay after a DLCI is declared operation before backup is ended (Backup Restoration Delay).
5. Specify When Auto Backup Allowed – Always or Restrict. If Restrict is selected, specify the days and hours of the week during which automatic backup can take place.
6. Save the configuration.

See Table 3-23, [Auto Backup Criteria Options](#), for configuration information.

Configuring the DBM Interface to Send SNMP Traps

The ISDN DBM interface can be specified as an interface that monitors and generates SNMP traps:

Main Menu → Configuration → Management and Communications → SNMP Traps

The configuration options for doing this include:

- Link Trap Interfaces
- DLCI Traps on Interfaces
- ISDN Dial Control Traps

When DBM is selected, trap messages are generated for linkUp and linkDown events on DLCIs and frame relay links for the originating DBM interface only. For peer-to-peer backup, backing up to a neighboring node like a regional node, dial control traps can be sent to trap manager(s).

See Table 3-19, [SNMP Traps and Trap Dial-Out Options](#), for configuration information.

Assigning DLCIs to a Backup Group

DLCIs can be assigned to a Backup Group to reduce backup charges when redundant PVCs have been configured. This feature prevents backup as long as any DLCI in the group is operational.

- Backup is not initiated as long as one DLCI in the group is operational.
- Backup is terminated as soon as one DLCI in the group becomes operational.

See Table 3-12, [DLCI Record Options](#), for configuration information.

PVC Backup Over the Network Interface

Generally, backup can be performed on the network interface's frame relay link using a backup PVC, as well on an ISDN link; the unit does not have to have the ISDN DBM feature.

In this case, create a DLCI Record on the network interface that will be used for backup, then modify the PVC Connections or Management PVCs to add the alternate destination.

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 using a crossover cable.

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 each when configuring the unit.

The following configuration option tables are included:

- Table 3-1. [System Frame Relay and LMI Options](#)
- Table 3-2. [Service Level Verification Options](#)
- Table 3-3. [General System Options](#)
- Table 3-4. [Network Physical Interface Options](#)
- Table 3-5. [Data Port Physical Interface Options](#)
- Table 3-6. [DSX-1 Physical Interface Options](#)
- Table 3-7. [ISDN BRI DBM Physical Interface Options](#)
- Table 3-8. [ISDN PRI DBM Physical Interface Options](#)
- Table 3-9. [ISDN Link Profile Options](#)
- Table 3-10. [Signaling and Trunk Conditioning Values](#) (when Assigning DSX-1-to-Network Time Slots/Cross Connections)
- Table 3-11. [Interface Frame Relay Options](#)
- Table 3-12. [DLCI Record Options](#)
- Table 3-13. [PVC Connection Options](#)
- Table 3-14. [Node IP Options](#)
- Table 3-15. [Management PVC Options](#)
- Table 3-16. [General SNMP Management Options](#)
- Table 3-17. [Telnet and FTP Session Options](#)
- Table 3-18. [SNMP NMS Security Options](#)
- Table 3-19. [SNMP Traps and Trap Dial-Out Options](#)
- Table 3-20. [Ethernet Port Options](#)
- Table 3-21. [Communication Port Options](#)
- Table 3-22. [Modem Port Options](#)
- Table 3-23. [Auto Backup Criteria Options](#)

Configuring the Overall System

The System menu includes the following:

- Frame Relay and LMI
- **Service Level Verification**
- **General**

Configuring Frame Relay and LMI for the System

Select Frame Relay and LMI from the System menu to display or change the Frame Relay and LMI options for the entire system (see Table 3-1).

Main Menu → Configuration → System → Frame Relay and LMI

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

Table 3-1. System Frame Relay and LMI Options (1 of 3)

LMI Behavior
Possible Settings: Independent, Net1-FR1_Follows_Port-1, Net1-FR1_Follows_Port-2, Port-1_Follows_Net1-FR1, Port-2_Follows_Net1-FR1, All_Ports_Follow_Net1-FR1, Port-1_Codependent_with_Net1-FR1, Port-2_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. NOTE: LMI Behavior cannot be changed while Auto Backup is enabled. A warning message appears at the bottom of the screen if auto backup is enabled. First, disable Auto Backup, and then change LMI Behavior. 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. Net1-FR1_Follows_Port-2 – Reacts like the Net1-FR1_Follows_Port-1 selection, but for Port-2 instead.

Table 3-1. System Frame Relay and LMI Options (2 of 3)

LMI Behavior
(Cont'd) 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-2_Follows_Net1-FR1 – Reacts like the Port-1_Follows_Net1-FR1 selection, but for Port-2 instead. All_Ports_Follow_Net1-FR1 – Brings LMI down on all user data ports when LMI on the network interface goes down, disabling all ports and deasserting their control leads. Allows LMI to come back up and reenables the ports when LMI comes up on the network. That is, LMI on each port follows the network interface's LMI. The state of LMI on the port will not affect the state of LMI on the network interface. 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 <i>not</i> recommended since it makes fault isolation more difficult. Port-2_Codependent_with_Net1-FR1 – Reacts like the Port-1_Codependent_with_Net1-FR1 selection, but for Port-2 instead. The state of LMI on the network interface will not affect the state of LMI on Port-1.
Traffic Policing
Possible Settings: Enable, Disable Default Setting: Disable Determines whether or not CIR (Committed Information Rate) and EIR (Excess Information Rate) will be enforced by the unit on frames being sent on network frame relay links. Enable – CIR and EIR are enforced. ■ Frames that exceed CIR will be marked Discard Eligible (DE). These frames are counted in the Above CIR but within EIR category until this category is full. Once full, additional frames are counted as being in the Within CIR category. ■ Frames in excess of EIR will be discarded. Disable – CIR and EIR are not enforced.
LMI Error Event (N2)
Possible Settings: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Default Setting: 3 Configures the LMI-defined N2 parameter, which sets the number of errors that can occur on the LMI link before an error is reported. Applies to both the user and network sides of a UNI. 1 – 10 – Specifies the maximum number of errors.

Table 3-1. System Frame Relay and LMI Options (3 of 3)

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 3-2).

Main Menu → Configuration → System → Service Level Verification

Table 3-2. 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 missed SLV packets will be monitored along with the LMI status to determine the status of PVC connections to remote FrameSaver units. NOTE: This option does not apply to multiplexed DLCIs connected to a far-end unit with hardware bypass capability. Enable – After the configured threshold for missed SLV packets has been exceeded, causing the DLCI's status to turn Inactive, an alarm and SNMP trap are generated, and a Health and Status message created. Disable – Missed SLV packets are monitored, but the DLCI is not declared down.
SLV Timeout Error Event Threshold
Available Settings: 1, 2, 3, 4 . . . 20 Default Setting: 3
Specifies the number of consecutive missed SLV communications that must be detected before a DLCI Inactive status is declared. 1–20 – Sets the limit for these error events.

Table 3-2. 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 Round Trip Latency Error Threshold (ms)
Available Settings: 50, 51, 52, . . . 10000 Default Setting: 10000
Specifies the number of milliseconds that must be exceeded before an SLV Latency Threshold alarm event is declared and backup, if configured, is initiated for a DLCI. 50–10000 – Sets the limit for these error events.
SLV Round Trip Latency Clearing Event Threshold
Available Settings: 1, 2, 3, 4 . . . 20 Default Setting: 2
Specifies the number of consecutive SLV latency measurements that must be received before it is determined that a DLCI is suitable for normal multiplexed PVC operation, and the alarm is cleared. 1 – 20 – Sets the limit for the clearing event.
SLV Packet Size (bytes)
Available Settings: 64 – 2048 Default Setting: 64
Sets the size of packets, in bytes, that will be used for SLV communications. SLV packets are used to track latency and other SLV-related variables. When the packet size is changed, a new round trip and average latency calculation must be performed, so these measurements will not appear on the SLV Performance Statistics screen until a new sampling interval has occurred. 64 – 2048 – Sets the packet size for SLV communications.
SLV Synchronization Role
Available Settings: Tributary, Controller, None Default Setting: Tributary
Determines the role the unit plays in maintaining synchronization of user history data collection and storage between FrameSaver SLV and/or FLEX 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 3-3).

Main Menu → Configuration → System → General

Table 3-3. General System Options (1 of 3)

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 accidentally 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. <i>Display Conditions</i> – This option only appears when Test Timeout is set to Enable. 1 – 120 – Sets the Test Timeout period in minutes (inclusive).
Primary Clock Source
Possible Settings: Net1, DSX, Internal, DBM Default Setting: Net1
Allows you to select the primary clock source for the unit. The source selected provides all of the timing within the FrameSaver unit and the clocks for all of the external interfaces. Failure of the clock specified by this configuration option results in automatic fallback to the Secondary Clock Source configuration option setting. NOTE: For the Primary and Secondary Clock Source options, only Internal can be selected for both options. All other selections must have different settings (e.g., if Primary Clock Source is set to Net1, Secondary Clock Source cannot be set to Net1). Net1 – The primary clock is derived from the Network1 T1 interface. DSX – The primary clock for the unit is derived from the DSX-1 interface. This setting only appears if the DSX-1 interface is enabled (see Configuring the DSX-1 Interface). Internal – The primary clock is the internal clock. DBM – The primary clock is derived from the DBM. This selection only appears if the DBM is installed and enabled.

Table 3-3. General System Options (2 of 3)

Secondary Clock Source
Possible Settings: Net1, DSX, Internal, DBM Default Setting: Internal
Provides a secondary clock source when the primary clock source fails. The source selected for this configuration option provides all of the timing within the unit and the clocks for all of the external interfaces. The clock source will switch back to primary when the primary clock source returns and is stable for 10 seconds. If the secondary clock source fails, the clock source will switch to internal. The clock source will switch back to primary when the primary clock source returns and is stable for 10 seconds. NOTE: For the Primary and Secondary Clock Source options, only Internal can be selected for both options. All other selections must have different settings (e.g., if Primary Clock Source is set to Net1, Secondary Clock Source cannot be set to Net1). Net1 – The secondary clock is derived from the Network1 T1 interface. DSX – The secondary clock for the unit is derived from the DSX-1 interface. This setting only appears if the DSX-1 interface is enabled. Internal – The secondary clock is the internal clock. DBM – The secondary clock is derived from the DBM. This selection only appears if the DBM is installed and enabled.

Table 3-3. General System Options (3 of 3)

System Alarm Relay
Possible Settings: Enable, Disable Default Setting: Disable
Specifies whether an alarm condition for the unit will activate the system alarm relay. The alarm relay is deactivated when the condition causing the alarm is corrected. If more than one alarm condition is present, the alarm relay remains active until all alarm conditions are cleared. You can also deactivate an alarm via the System Alarm Relay Cut-Off selection from the Control menu; however, the alarm itself is not cleared. When another alarm condition is detected, the alarm is reactivated again, requiring another manual deactivation of the alarm relay. <i>Display Conditions</i> – This option only appears for a FrameSaver SLV 9128 or 9128-II installed in the 9000 Series Access Carrier. Alarm conditions are: ■ Alarm Indication Signal (AIS) received at the Network, DSX-1, or PRI interface ■ Continuous Loss of Signal (LOS) condition at the Network, DSX-1, or PRI interface ■ CTS Down ■ DBM Download Required ■ DBM BRI Card Failed ■ Device Fail ■ DLCI Down ■ DTR Down ■ Ethernet Link Down ■ Excessive Error Rate (EER) detected at the Network or PRI interface ■ Internal Modem Failed ■ ISDN Network Failure ■ LMI Down ■ Network Communication Link Down ■ Out of Frame (OOF) at Network, DSX-1, or PRI ■ Primary or Secondary Clock Failure ■ Power Supply/Fan Failure ■ RTS Down ■ Self-Test Failure ■ SLV Latency Exceeded ■ SLV Timeout ■ Suboptimal (Maximum) Link Rate Cannot be Achieved ■ Two Level-1 Users Accessing Device ■ Yellow Alarm Signal on the Network, DSX-1, or PRI interface Enable – Activates alarm conditions on the system alarm relay when an alarm condition occurs. Disable – Does not activate the system alarm relay when an alarm condition occurs.

Configuring Physical Interfaces

Characteristics for the following physical interfaces can be configured:

- Network Interface
- User Data Port(s)
- DSX-1 Interface
- ISDN

Configuring the Network Interface

When configuring the physical characteristics for the network interface, select Physical from the Network menu (see Table 3-4).

Main Menu → Configuration → Network → Physical

Table 3-4. Network Physical Interface Options (1 of 4)

Line Framing Format
Possible Settings: D4 , ESF Default Setting: ESF
Specifies the framing format for transmitted and received signals on the T1 network interface. D4 – Uses D4 framing format. NOTE: This setting is not recommended by network carriers. False yellow alarms may occur after traffic has been running and the channel returns to idle, or when there is light traffic when other settings are selected. ESF format does not create this problem. ESF – Uses Extended Superframe framing format.
Line Coding Format
Possible Settings: AMI , B8ZS Default Setting: B8ZS
Specifies the line coding format for the network interface. AMI – Uses Alternate Mark Inversion (AMI) line coding format. B8ZS – Uses Bipolar 8 Zero Substitution (B8ZS) line coding format.

Table 3-4. Network Physical Interface Options (2 of 4)

Line Build Out (LBO)
Possible Settings: 0.0, -7.5, -15, -22.5 Default Setting: 0.0
Specifies the line build out for the signal transmitted to the network. 0.0, -7.5, -15, -22.5 – Specifies line build out in dB.
Bit Stuffing
Possible Settings: 62411, Disable Default Setting: 62411
Determines the type of bit insertion to provide ones density requirements for data transmitted to the network. <i>Display Conditions</i> – This option does not appear when Line Coding Format is set to B8ZS. 62411 – Inserts a one in the data after 15 consecutive zeros are received or the density of ones falls below 12.5%. This setting complies with AT&T TR 62411, but is not recommended for frame relay data because it inserts errors in the data traffic. Disable – Disables bit stuffing. Ones density is not enforced on data sent to the network.
Transmit Timing
Possible Settings: System, Interface Default Setting: System
Allows transmit timing to be selected from either the system master clock source or from the currently selected interface. System – Transmit timing is derived from the current system clock source (see Table 3-3, General System Options). Interface – Transmit timing is derived from this interface. NOTE: When Interface is configured, the clock must be synchronized to the system clock source.
Network Initiated LLB
Possible Settings: Enable, Disable Default Setting: Enable
Allows the initiation and termination of the line loopback (LLB) to be controlled by the receipt of LLB-Actuate and LLB-Release commands from the network. Enable – LLB is controlled by LLB-Actuate and LLB-Release commands. Receiving a LLB-Actuate command causes the FrameSaver unit to enter a line loopback (provided an LLB can be performed in the FrameSaver unit's current state). Receiving an LLB-Release command terminates the LLB. Disable – The FrameSaver unit ignores the LLB-Actuate and LLB-Release commands. NOTE: When disabled, the system is not in compliance with ANSI T1.403 or AT&T TR 62411.

Table 3-4. Network Physical Interface Options (3 of 4)

Network Initiated PLB
Possible Settings: Enable, Disable Default Setting: Enable
Allows the initiation and termination of the payload loopback (PLB) to be controlled by the receipt of PLB-Actuate and PLB-Release commands from the network. <i>Display Conditions</i> – This option only appears when Line Framing Format is set to ESF. Enable – PLB is controlled by PLB-Actuate and PLB-Release commands. Receiving a PLB-Actuate command causes the system to enter a payload loopback (provided a PLB can be performed in the unit's current state). Receiving a PLB-Release command terminates the PLB. Disable – The FrameSaver unit ignores the PLB-Actuate and PLB-Release commands. NOTE: When disabled, the unit is not in compliance with ANSI T1.403 or AT&T TR 54016.
Network Initiated DCLB
Possible Settings: Disable, V.54 & ANSI Default Setting: V.54 & ANSI
Allows the initiation and termination of the Data Channel Loopback (DCLB V.54 Loop 2) to be controlled by the receipt of a DCLB-actuate or DCLB-release sequence (either V.54 or FT1-ANSI compliant) from the network on the DS0s used for the network frame relay link. When enabled and a DCLB-activate sequence is received, the unit initiates a DCLB on the network interface. When a DCLB-release sequence is received, the DCLB is stopped. Disable – DCLB-actuate and DCLB-release sequences are ignored. V.54 & ANSI – DCLB-actuate and DCLB-release sequences that comply with either V.54 or ANSI T1.403, Annex B standard will be recognized and will control initiation and termination of a DCLB for the network frame relay link. The actuate and release sequences do not need to match (for example, a DCLB started with a V.54 actuate sequence can be stopped with an FT1 release sequence).
ANSI Performance Report Messages
Possible Settings: Enable, Disable Default Setting: Disable
Specifies whether ANSI T1.403 compliance performance report messages (PRMs) are generated and sent to the network over the ESF facility data link every second. <i>Display Conditions</i> – This option only appears when Line Framing Format is set to ESF. Enable – Generates and sends PRMs. Disable – Does not generate and send PRMs.

Table 3-4. Network Physical Interface Options (4 of 4)

Excessive Error Rate Threshold
Possible Settings: 10E-4, 10E-5, 10E-6, 10E-7, 10E-8, 10E-9 Default Setting: 10E-4
Sets the error rate threshold that determines when an EER condition is declared. The excessive error rate is determined by the ratio of the number of CRC6 errors to the total number of bits received over a set period of time. <i>Display Conditions</i> – This option only appears when Line Framing Format is set to ESF. 10E-4 – Declares an EER if more than 1,535 CRC6 errors are detected in a 10 second period. Clears when fewer than 1,536 CRC6 errors are detected within the same time period. 10E-5 – Declares an EER if more than 921 CRC6 errors are detected in a 60 second period or a 10^{-4} condition occurs. Clears when fewer than 922 CRC6 errors are detected within the same time period. 10E-6 – Declares an EER if more than 92 CRC6 errors are detected in a 60 second period or a 10^{-5} or 10^{-4} condition occurs. Clears when fewer than 93 CRC6 errors are detected within the same time period. 10E-7 – Declares an EER if more than 9 CRC6 errors are detected in a 60 second period or a 10^{-6}, or 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 10 CRC6 errors are detected within the same time period. 10E-8 – Declares an EER if more than 41 CRC6 errors are detected in three 15 minute intervals or a 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4} condition occurs. Clears when fewer than 42 CRC6 errors are detected within the same time period. 10E-9 – Declares an EER if more than 4 CRC6 errors are detected in three 15 minute intervals or a 10^{-8}, 10^{-7}, 10^{-6}, 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 5 CRC6 errors are detected within the same time period.
Circuit Identifier
Possible Settings: ASCII Text Entry, Clear Default Setting: blank
Identifies the transmission vendor's circuit information to facilitate troubleshooting. ASCII Text Entry – Edit or display circuit identifier information (maximum 255 characters). Clear – Removes the circuit identifier information.

Configuring a User Data Port

Select Physical from the Data Ports menu to display or change the physical characteristics of the data port connected to the DTE (see Table 3-5).

Main Menu → Configuration → Data Ports → Physical

Table 3-5. Data Port Physical Interface Options (1 of 5)

Port Status
Possible Settings: Enable, Disable Default Setting: Enable
Determines whether the data port is being used and can be configured. Enable – The port is active, and can be used to transmit and receive data. Disable – The port is not active. When the port is disabled, the following will occur: ■ No alarms or traps configured for the port will be generated. ■ LED for the port will be held in an Off state. No – The operation is cancelled. (Pressing either the Esc or Ctrl-a key also acts as a No.) Yes – Port status is disabled.
Port Use
Possible Settings: Frame Relay, Synchronous Data Default Setting: Frame Relay when the port supports frame relay. Synchronous Data when the port only supports synchronous data.
Determines how the data port will be used. <i>Display Conditions</i> – This option only appears for user data on Port-2. Frame Relay – The port is configured for frame relay traffic. Frame relay links, DLCIs, and PVC connections can be configured on this port. Synchronous Data – The port is configured for standard TDM data, and can be cross-connected to a time slot on a T1 interface. ■ No alarms or traps configured for the port will be generated. ■ The LED for the port will be held in an Off state. ■ Existing cross-connect assignments associated with the port are cleared.

Table 3-5. Data Port Physical Interface Options (2 of 5)

Max Port Rate (Kbps)
Possible Settings: 1536, 2048 Default Setting: 1536
Specifies the maximum clock rate for a user data port. The data rate for this port is limited to the rate specified by this option so that the maximum rate supported by an attached DTE is not exceeded. <i>Display Conditions</i> – This option only appears when the Port Use is set to Frame Relay and, if the unit has multiple data ports, the selected port is Port-2. 1536 – The maximum port rate for the port is 1536 kbps. 2048 – The maximum port rate for the port is 2048 kbps.
Port Base Rate (Kbps)
Possible Settings: Nx64, Nx56 Default Setting: Nx64
Specifies the base rate for the data port, which is a multiple (from 1 to 24) of the base rate specified by this option. N is a number from 1 to 24. <i>Display Conditions</i> – This option only appears when Port Use is set to Synchronous Data. This option does not appear for a FrameSaver SLV 9128-II. Nx64 – The base rate for the port is 64 kbps. Nx56 – The base rate for the port is 56 kbps.
Invert Transmit Clock
Possible Settings: Auto, Enable, Disable Default Setting: Auto
Determines whether the clock supplied by the FrameSaver unit on interchange circuit DB (ITU 114) – Transmit Signal Element Timing (DCE Source) TXC is phase inverted with respect to the clock used to time the incoming Transmitted Data (TD). Auto – The port checks the clock supplied by the DCE on TXC on this port. 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.

Table 3-5. Data Port Physical Interface Options (3 of 5)

Transmit Clock Source
Possible Settings: Internal, External Default Setting: Internal
Determines whether the DTE's transmitted data is clocked into the FrameSaver unit by its internal transmit clock or by the external clock provided by the DTE. NOTE: Changing settings for this configuration option causes the FrameSaver unit to abort any physical port tests, including any DTE-initiated loopback tests. Internal – The FrameSaver unit uses the interchange circuit DB (ITU 114) – Transmit Signal Element Timing (TXC) (DCE source) for timing the incoming data. External – The DTE provides the clock for the transmitted data, and the FrameSaver unit uses the interchange circuit DA (ITU 113) – Transmit Signal Element Timing (XTXC) (DTE source) for timing the incoming data.
Monitor RTS (Control)
Possible Settings: Enable, Disable Default Setting: Enable
Specifies whether the state of the Request To Send (RTS) circuits on the user data port will be used to determine when valid data communication is possible with the DTE. When this condition is detected, CTS is deasserted, LMI is declared down, and no further transfer of frame relay data can occur on this interface. Enable – Interchange circuit CA (ITU 105) – RTS is monitored to determine when valid data communication is possible with the DTE. Disable – RTS is not monitored. RTS is assumed to be asserted and data is being transmitted, regardless of the state of the lead.
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 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. Enable – Interchange circuit CD (ITU 108/1/2) – DTR is monitored to determine whether data should be transmitted to 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.

Table 3-5. Data Port Physical Interface Options (4 of 5)

Port (DTE) Initiated Loopbacks
Possible Settings: <i>When Port-1 or Port Use is set to Frame Relay:</i> Disable, Local <i>When Port-2 or Port Use is set to Synchronous Data:</i> Disable, DTPLB, DCLB, Both Default Setting: Disable
Possible Settings: Local, Disable Default Setting: Disable
<i>When Port-1 or Port Use is set to Frame Relay:</i> Allows a local external DTE Loopback to be started or stopped via the data terminal equipment attached to the port's interchange lead LL (ITU 141), as specified by V.54. Disable – The DTE attached to the port cannot control the local external DTE Loopback. Local – The DTE attached to the port controls the local external DTE Loopback. <i>When Port-2 or Port Use is set to Synchronous Data:</i> Allows local Data Terminal Loopbacks (DTPLBs) and remote Data Channel Loopbacks (DCLBs) to be controlled by the DTE connected to this port. <i>Display Conditions</i> – This option does not appear when Port Type is set to X.21. Disable – The DTE attached to the port cannot control Local Data Terminal Loopbacks (DTPLBs) and remote Data Channel Loopbacks (DCLBs). DTPLB – The DTE attached to the port controls DTPLBs via circuit LL – CCITT 141, as specified by V.54. The port remains in loopback as long as the circuit stays on. DCLB – The DTE attached to the port controls DCLBs via circuit RL – CCITT 140, as specified by V.54. The far-end equipment must support inband V.54 loopbacks. Both – The DTE attached to the port controls both local DTPLBs and remote DCLBs.
Invert Transmit and Receive Data
Possible Settings: Enable, Disable Default Setting: Disable
Specifies whether transmitted and received data for the synchronous data port is logically inverted before being transmitted or after being received from the network. Use this configuration option for applications where data is being transported using HDLC protocol, whereby inverting the data ensures that the ones density requirements for the network are met. <i>Display Conditions</i> – This option only appears for Port-2 on a FrameSaver SLV 9128 or 9128-II, when Port Use is set to Synchronous Data. Enable – Inverts the transmitted and received data for the port. Disable – Does not invert the transmitted and received data for the port.

Table 3-5. Data Port Physical Interface Options (5 of 5)

Action on Network Yellow Alarm
Possible Settings: None, Halt Default Setting: Halt
Specifies the action to take on the synchronous data port when a yellow alarm is received on the network interface. (A yellow alarm indicates a problem with the signal being transmitted to the network.) <i>Display Conditions</i> – This option only appears for Port-2 on a FrameSaver SLV 9128 or 9128-II, when Port Use is set to Synchronous Data. None – No action taken when a yellow alarm is received. Halt – Halts the transmission of data received on the synchronous data port and all ones are sent on circuit BB (ITU 104) – Receive Data (RD) and circuit CB (ITU 106) – Clear-to-Send (CTS) is deasserted to the port when a yellow alarm is received.
Network Initiated Data Channel Loopback
Possible Settings: Disable, V.54, ANSI_FT1, V.54_&_ANSI Default Setting: Disable
Allows the initiation and termination of the Data Channel Loopback (V.54 Loop 2) to be controlled by the receipt of a DCLB-actuate and DCLB-release sequence (either V.54, or FT1 [ANSI] compliant sequences) from the network or far end unit. When this configuration is enabled (V.54, FT1, or Both), receiving a DCLB-actuate sequence on a particular port causes the unit to initiate a DCLB on that port (provided that a DCLB can be performed based on the current state of the port and unit). Receiving a DCLB-release sequence terminates the DCLB. <i>Display Conditions</i> – This option only appears for Port-2 on a FrameSaver SLV 9128 or 9128-II, when Port Use is set to Synchronous Data. Disable – Ignores the DCLB-actuate and DCLB-release for the port. V.54 – DCLB-actuate and DCLB-release sequences that comply with the V.54 standard for “inter-DCE signaling for point-to-point circuits” are recognized and will control the initiation and termination of a DCLB (V.54 Loop 2) for the port. ANSI_FT1 – DCLB-actuate and DCLB-release sequences that comply with either the ANSI.403, Annex B standard for “in-band signaling for fractional T1 (FT1) channel loopbacks” are recognized and will control the initiation and termination of a DCLB for the port. V.54_&_ANSI – DCLB-actuate and DCLB-release sequences that comply with either the ANSI or V.54 standard are recognized and will control the initiation and termination of a DCLB for the port.

Configuring the DSX-1 Interface

Select DSX-1 to display or change the physical configuration options when a DSX-1 interface is installed (see Table 3-6).

Main Menu → Configuration → DSX-1

Table 3-6. DSX-1 Physical Interface Options (1 of 2)

Interface Status
Possible Settings: Enable, Disable Default Setting: Disable
Specifies whether the DSX-1 interface selected is available for use. Enable – The interface is available. Disable – The interface is not available for use. If there are time slots assigned to the DSX-1 interface when you attempt to disable it, the message This action will clear all DSX-1 Cross Connections. Are You Sure? No appears. If you select: No – The operation is cancelled. Yes – The following occurs: ■ All existing DSX-1 interface cross-connect assignments are cleared. ■ Alarms or traps associated with the DSX-1 interface are not generated. ■ LEDs associated with the DSX-1 interface are held in an “off” state.
Line Framing Format
Possible Settings: D4, ESF Default Setting: ESF
Specifies the framing format for transmitted and received signals on the DSX-1 interface. D4 – Uses D4 framing format. ESF – Uses Extended Superframe (ESF) framing format.
Line Coding Format
Possible Settings: AMI, B8ZS Default Setting: B8ZS
Specifies the line coding format for the DSX-1 interface. AMI – Uses Alternate Mark Inversion (AMI) line coding format. B8ZS – Uses Bipolar 8 Zero Substitution (B8ZS) line coding format.

Table 3-6. DSX-1 Physical Interface Options (2 of 2)

Line Equalization
Possible Settings: 0–133, 133–266, 266–399, 399–533, 533–655 Default Setting: 0–133
Permits a standard DSX signal to be delivered over a distance of up to 655 feet. 0–133 – Equalization on the DSX-1 side allows up to 133 feet of cable between the FrameSaver unit and the DTE. 133–266 – Equalization on the DSX-1 side allows up to 266 feet of cable between the FrameSaver unit and the DTE. 266–399 – Equalization on the DSX-1 side allows up to 399 feet of cable between the FrameSaver unit and the DTE. 399–533 – Equalization on the DSX-1 side allows up to 533 feet of cable between the FrameSaver unit and the DTE. 533–655 – Equalization on the DSX-1 side allows up to 655 feet of cable between the FrameSaver unit and the DTE.
Send All Ones on DSX-1 Failure
Possible Settings: Enable, Disable Default Setting: Enable
Determines whether action is taken when a valid signal cannot be recovered for the DSX-1 (LOS, continuous OOF, or AIS). Enable – Sends all ones on the DS0 channels allocated to the DSX-1 interface in the event of an LOS, AIS, or continuous OOS condition on the DSX-1 interface. Disable – No action is taken when a signal fails on the DSX-1 interface. The data received is passed through the network interface channels unchanged.

Configuring the ISDN DBM Interface

For models with ISDN backup capability, select Physical from the ISDN menu to configure the physical characteristics for DBM Interface.

Main Menu → Configuration → ISDN → Physical

When configuring a **BRI DBM**, refer to Table 3-7.

When configuring a **PRI DBM**, refer to Table 3-8.

Table 3-7. ISDN BRI DBM Physical Interface Options

Interface Status
Possible Settings: Enable, Disable Default Setting: Disable
Determines whether the ISDN interface is available for use. Enable – The ISDN interface is enabled. Disable – The ISDN interface cannot be configured, nor can it transmit or receive data. No PVC connections or frame relay DLCIs will be deleted. Disabling the ISDN interface results in the following: ■ All currently connected ISDN calls are terminated. ■ Alarms or traps associated with this interface are not generated or displayed.
Service Profile ID (SPID) 1 or 2
Possible Settings: 3 – 20 digits Default Setting: Clear
Specifies the SPID number assigned by the ISDN service provider for Bearer channel 1 (B1) and Bearer channel 2 (B2). SPID numbers are used by the switch to identify which ISDN services the DBM can access. All blanks is a valid setting. 3 – 20 digits – You can enter a SPID number, or you can leave blanks. If a nondigit/numeric is entered, an Invalid Character (x) message appears at the bottom of the screen. If fewer than three digits/numerics are entered, an Invalid – SPID must be at least 3 digits message appears at the bottom of the screen. Clear – Clears the SPID field so it can be reentered.
Local Phone Number 1 or 2
Possible Settings: 10 digits Default Setting: Clear
Provides the telephone number associated with Bearer channel 1 (B1) and 2 (B2). All blanks is a valid setting. 10 digits – Enter the telephone number, up to 10 digits. If a nondigit/numeric is entered, an Invalid Character (x) message appears at the bottom of the screen. Clear – Clears the phone number field so it can be reentered.

Refer to the following table when configuring a PRI DBM.

Table 3-8. ISDN PRI DBM Physical Interface Options (1 of 3)

Interface Status
Possible Settings: Enable, Disable Default Setting: Disable
Determines whether the ISDN interface is available for use. Enable – The ISDN interface is enabled. Disable – The ISDN interface cannot be configured, nor can it transmit or receive data. No PVC connections or frame relay DLCIs will be deleted. Disabling the ISDN interface results in the following: ■ All currently connected ISDN calls are terminated. ■ Alarms or traps associated with this interface are not generated or displayed. ■ LEDs associated with this interface are held in an “off” state. Specifically, the DSX/PRI LEDs are held off if they represent the PRI status.
Switch Type
Possible Settings: NI-2, ATT_4ESS, ATT_5ESS Default Setting: NI-2
Specifies type of ISDN switch provided by the server. NI-2 – The DBM will communicate with a service provider supporting the National ISDN-2 switching standard. ATT_4ESS – The DBM will communicate with a service provider supporting the ATT 4ESS switching standard. ATT_5ESS – The DBM will communicate with a service provider supporting the ATT 5ESS switching standard.
Local Phone Number
Possible Settings: 10 digits Default Setting: Clear
Provides the telephone number associated with all Bearer channels. All blanks is a valid setting. 10 digits – Where you enter the telephone number, up to 10 digits. If a nondigit/numeric is entered, an Invalid Character (x) message appears at the bottom of the screen. Clear – Clears the phone number field so it can be reentered.
Line Framing Format
Possible Settings: D4, ESF Default Setting: ESF
Specifies the framing format for transmitted and received signals on the ISDN interface. D4 – Uses D4 framing format. NOTE: This setting is not recommended by network carriers. False yellow alarms may occur after traffic has been running and the channel returns to idle, or when there is light traffic when other settings are selected. ESF format does not create this problem. ESF – Uses Extended Superframe framing format.

Table 3-8. ISDN PRI DBM Physical Interface Options (2 of 3)

Line Build Out (LBO)
Possible Settings: 0.0, -7.5, -15, -22.5 Default Setting: 0.0
Specifies the line build out for the signal transmitted to the ISDN. 0.0, -7.5, -15, -22.5 – Specifies line build out in dB.
Network Initiated LLB
Possible Settings: Enable, Disable Default Setting: Enable
Allows the initiation and termination of the line loopback (LLB) to be controlled by the receipt of LLB-Actuate and LLB-Release commands from the ISDN. Enable – LLB is controlled by LLB-Actuate and LLB-Release commands. Receiving a LLB-Actuate command causes the system to enter a line loopback (provided an LLB can be performed in the system's current state). Receiving an LLB-Release command terminates the LLB. Disable – The system ignores the LLB-Actuate and LLB-Release commands. NOTE: When disabled, the system is not in compliance with ANSI T1.403 or AT&T TR 62411.
Network Initiated PLB
Possible Settings: Enable, Disable Default Setting: Enable
Allows the initiation and termination of the payload loopback (PLB) to be controlled by the receipt of PLB-Actuate and PLB-Release commands from the ISDN. <i>Display Conditions</i> – This option only appears when Line Framing Format is set to ESF. Enable – PLB is controlled by PLB-Actuate and PLB-Release commands. Receiving a PLB-Actuate command causes the system to enter a payload loopback (provided a PLB can be performed in the system's current state). Receiving a PLB-Release command terminates the PLB. Disable – The system ignores the PLB-Actuate and PLB-Release commands. NOTE: When disabled, the unit is not in compliance with ANSI T1.403 or AT&T TR 54016.
ANSI Performance Report Messages
Possible Settings: Enable, Disable Default Setting: Disable
Specifies whether ANSI T1.403 compliance performance report messages (PRMs) are generated and sent to the ISDN over the ESF facility data link every second. <i>Display Conditions</i> – This option only appears when Line Framing Format is set to ESF. Enable – Generates and sends PRMs. Disable – Does not generate and send PRMs.

Table 3-8. ISDN PRI DBM Physical Interface Options (3 of 3)

Excessive Error Rate Threshold
Possible Settings: 10E-4, 10E-5, 10E-6, 10E-7, 10E-8, 10E-9 Default Setting: 10E-4
Sets the error rate threshold that determines when an EER condition is declared. The excessive error rate is determined by the ratio of the number of CRC6 errors to the total number of bits received over a set period of time. <i>Display Conditions</i> – This option only appears when Line Framing Format is set to ESF. 10E-4 – Declares an EER if more than 1,535 CRC6 errors are detected in a 10 second period. Clears when fewer than 1,536 CRC6 errors are detected within the same time period. 10E-5 – Declares an EER if more than 921 CRC6 errors are detected in a 60 second period or a 10^{-4} condition occurs. Clears when fewer than 922 CRC6 errors are detected within the same time period. 10E-6 – Declares an EER if more than 92 CRC6 errors are detected in a 60 second period or a 10^{-5} or 10^{-4} condition occurs. Clears when fewer than 93 CRC6 errors are detected within the same time period. 10E-7 – Declares an EER if more than 9 CRC6 errors are detected in a 60 second period or a 10^{-6}, or 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 10 CRC6 errors are detected within the same time period. 10E-8 – Declares an EER if more than 41 CRC6 errors are detected in three 15 minute intervals or a 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4} condition occurs. Clears when fewer than 42 CRC6 errors are detected within the same time period. 10E-9 – Declares an EER if more than 4 CRC6 errors are detected in three 15 minute intervals or a 10^{-8}, 10^{-7}, 10^{-6}, 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 5 CRC6 errors are detected within the same time period.
Circuit Identifier
Possible Settings: ASCII Text Entry, Clear Default Setting: blank
Identifies the transmission vendor's circuit information to facilitate troubleshooting. ASCII Text Entry – Assigns a name to identify the circuit (maximum 255 characters). Clear – Removes the circuit identifier information.

Setting Up ISDN Link Profiles

For models with ISDN backup capability, select ISDN Link Profiles from the ISDN menu to set up the ISDN Link Profiles (see Table 3-9).

Main Menu → Configuration → ISDN → ISDN Link Profiles

Table 3-9. ISDN Link Profile Options (1 of 3)

Link Name
Possible Settings: ASCII Text Entry , HQ_Site Default Setting: HQ_Site for first link; blank for all others
Assigns the name to the ISDN link profile. It is generally the backup destination for a frame relay link. Each profile must have a unique link name. If the link name field is blank, the link profile will be deleted. Use ASCII text, 8 characters maximum. ASCII Text Entry – Assigns a name to identify the ISDN link (maximum 255 characters). NOTE: To prevent confusion, do not use the following link names: Network, Net1-FR1, Port-1, or Port-2. These names will be treated as nonunique and the Link Name Not Unique message appears and you must enter another name. HQ_Site – The link name configured in the remote site unit (originating a backup call) for the central site unit (answering a backup call). One link has a default value of HQ_Site to allow for Automatic Backup Configuration.
Link Status
Possible Settings: Auto , Disable Default Setting: Auto
Determines whether the ISDN frame relay link is in or out of service. Auto – The link is configured to be in service when needed. Packets will be transmitted and received on the interface, and the LMI for a PVC connection will become active when the link is required. If this profile is configured as the alternate link and the primary link or DLCI fails, the unit dials the Outbound Phone Number, or the Alternate Outbound Phone Number if the first call was unsuccessful. The unit also answers calls from Inbound Call IDs associated with this link. This link profile becomes active when: ■ This profile is configured as the alternate link and there is a failure of a primary link or DLCI. ■ Source or Primary Destination DLCIs are configured on this link. When the primary link recovers, the call is automatically disconnected. Disable – The frame relay link is out of service. No data will be transmitted or received on the interface. If there is any active calls when disabled, the calls are ended and no calls will be answered or originated using this profile.

Table 3-9. ISDN Link Profile Options (2 of 3)

Outbound Phone Number
Possible Settings: 0 – 9, *, #, space, _ , -, (, or) Default Setting: none Specifies the primary phone number to call (the ISDN Called Party Identifier) for the Link Profile. Up to 18 valid characters can be entered. Each Outbound Phone Number must be unique. If not, the Outbound Phone Number is Not Unique message appears and you must enter another phone number. NOTE: For every originating (outbound) phone number entered, an answering (inbound) phone number must be entered at the far end, and vice versa. Currently active calls are not effected when this number is changed.
Inbound Calling ID 1 or 2
Possible Settings: 0 – 9 Default Setting: none Specifies the local phone number of a remote device from which that the unit will accept calls (the ISDN Calling Party Identifier). Up to 18 digits can be entered. Each Inbound Calling ID must be unique. If not, the Inbound Calling ID n is Not Unique message appears and you must enter another phone number. For remote devices with a PRI DBM, only one Inbound Calling ID is required. Inbound Calling ID 2 is provided to identify incoming calls from a second phone number assigned to a remote device with a BRI DBM. NOTES: Inbound Calling ID 2 is only useful when multiple local phone numbers are programmed at the originating site (e.g., a 2B+D BRI location). For every originating (outbound) phone number entered, an answering (inbound) phone number must be entered at the far end, and vice versa. Currently active calls are not effected when this number is changed. 0 – 9 – Specifies the numbers in the remote device's local phone number.
Maximum Link Rate (Kbps)
Possible Settings: <i>For a BRI DBM: 64, 128</i> <i>For a PRI DBM: 64 – 1472</i> Default Setting: 64 Specifies the maximum rate that will be attempted for the frame relay link when it is activated. The actual rate achieved on the link depends upon the number of successful calls placed or answered, and the negotiated rate on each call. NOTE: This option takes effect as soon as a change is saved. If the rate is increased, additional calls will be placed. If the rate is decreased, calls will be dropped. For extra calls to be successful, the Maximum Link Rate must be increased at the originating device before it is increased at the answering device. 64 – An individual frame relay link is formed and a single call is placed using a B-channel when the link is activated. 128 . . . 1472 – A constituent link is configured for each multiple of 64 kbps in the specified bandwidth. This bundle of constituent links will function as a single frame relay multilink. When the multilink aggregate link is activated, calls will be placed or answered on as many constituent links as possible based upon available B-channels.

Table 3-9. ISDN Link Profile Options (3 of 3)

Caller Identification Method
Possible Settings: Caller ID, Proprietary Default Setting: Caller ID
Specifies the method used to identify callers. NOTE: The Caller Identification Method setting must be the same at both ends of the circuit. Caller ID – Incoming calls will only be answered and the frame relay link on this Link Profile will only be activated when the Caller ID received from the switch matches one of the configured Inbound Calling IDs. Proprietary – Incoming calls will always be answered, even when no Caller ID is provided by the switch, provided the following conditions are met: ■ Link Status is set to Auto (the default). ■ At least one ISDN Link Profile is enabled. When using the Proprietary method, the unit queries the originating unit for its Local Phone Number. If the returned phone number matches one of the configured Inbound Calling IDs, the call is accepted. If the queried unit does not respond with its phone number within five seconds, the unit drops the call.
Alternate Outbound Phone Number
Possible Settings: 0 – 9, *, #, space, _ , - , (, or) Default Setting: none
Specifies an alternate phone number to call (the ISDN Called Party Identifier) when a call using the primary Outbound Phone Number was unsuccessful. Up to 18 valid characters can be entered. Each Outbound Phone Number must be unique. If not, the Alt Outbound Phone Number is Not Unique message appears and you must enter another phone number. NOTE: For every originating (alternate outbound) phone number entered, an answering (inbound) phone number must be entered at the far end, and vice versa. Currently active calls are not effected when this number is changed.

Assigning Time Slots/Cross Connections

The Time Slot Assignment/Cross Connect feature provides an easy method of assigning time slots for frame relay data and creating cross-connections to the synchronous data interface. The system allows you to assign DS0s on the T1 network interface and between the user data port and network interface in order to share the T1 network.

You can also clear cross-connection assignments for the system, or for a selected slot or interface.

NOTE:

Although it is not required, it is suggested that you progress through each screen in order, from top to bottom.

Assigning Frame Relay Time Slots to the Network Interface

Before assigning network time slots for use by frame relay traffic, configure the Network physical and Frame Relay options (if needed), then allow Time Slot Discovery to autodetect and assign the appropriate time slots to frame relay.

If there are multiple Frame Relay data links on the network interface, or if Time Slot Discovery is not currently active, you can manually assign time slots on the network interface for frame relay traffic using the Frame Relay Network Assignments screen. This screen is read-only when Time Slot Discovery is set to Enable for the network interface.

Frame Relay Network Time Slot Assignment Screen Example

```

main/config/tslot_assign/frame_relay                               9128-II
Device Name: Node A                                              5/26/2000 23:32

                                FRAME RELAY NETWORK 1 ASSIGNMENT

                                Time Slot Discovery: Disable

      N01      N02      N03      N04      N05      N06      N07      N08
Available Available Available Available Available Available Available Available

      N09      N10      N11      N12      N13      N14      N15      N16
Available Available FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1

      N17      N18      N19      N20      N21      N22      N23      N24
FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1

-----
Ctrl-a to access these functions, ESC for previous menu      MainMenu  Exit
Save  PgDn  PgUp  ClearAll          DSXAssign

```

Value	Meaning
Time Slot Discovery	Specifies whether the time slots used for frame relay traffic should be discovered from the network interface upon detection of an LMI failure. This option allows additional time slots to be added without manually reconfiguring the device.
N <i>tt</i>	This field represents time slot <i>tt</i> of the selected network interface.
Assigned	The time slot is already assigned to something other than frame relay, so it is unavailable. Assigned time slots cannot be modified from this screen.
Available	The time slot is currently unassigned.
FrameRly1	The time slot is assigned to frame relay service, link 1.

For easy movement between screens, select the DSXAssign function key to go directly to the DSX-1 to Network Assignments screen.

Time Slot Assignment Rule:

Valid network time slots are either **Available** or contain a Frame Relay Link 1 assignment.

► Procedure

1. Follow this menu selection sequence:

*Main Menu → Configuration → Time Slot Assignment →
Frame Relay Network Assignments*

The Frame Relay Network Assignments screen appears. This screen contains a matrix of the current assignment status of all time slots on the network interface.

2. Enable or disable Time Slot Discovery.
 - When enabled, the unit examines all time slots not cross-connected to other ports to determine which time slots are being used by the network for frame relay traffic. These time slots are set to **FrameRly1**. This is the factory default.
 - When disabled, time slot assignments must be manually configured.
3. If Time Slot Discovery is disabled, assign network time slots for use by frame relay service, link 1, by typing **FrameRly1** in the selected Network field.
4. Repeat Step 3 until all desired time slots are assigned.
5. Save the configuration.

Assigning DSX-1 Time Slots to the Network Interface

DSX-1 time slots are assigned by channel allocation, where you specify individual time slots. The DSX-1 interface must be enabled to assign DSX-1 time slots to the network interface (see Table 3-6, **DSX-1 Physical Interface Options**).

Value	Meaning
<i>Ntt</i>	It represents time slot <i>tt</i> of the selected network interface.
Assigned	The time slot is already assigned to something other than a DSX-1 time slot, so it is unavailable. Assigned time slots cannot be modified from this screen.
Available	The time slot is currently unassigned.
DSX-1/ <i>tt</i>	Slot <i>tt</i> of the DSX-1 interface is assigned to the network interface time slot identified right above it (<i>Ntt</i>).

DSX-1 to Network Time Slot Assignment Screen Example (Page 1)

```

main/config/tslot_assign/dsx                      9128-II
Device Name: Node A                             5/26/1999 23:32

                                DSX-1 TO NETWORK 1 ASSIGNMENTS                                Page 1 of 2

    N01      N02      N03      N04      N05      N06      N07      N08
DSX-1/01 DSX-1/02 DSX-1/03 DSX-1/04 Assigned Assigned Assigned Assigned

    N09      N10      N11      N12      N13      N14      N15      N16
DSX-1/09 DSX-1/01 Available Available Available Available Available Available

    N17      N18      N19      N20      N21      N22      N23      N24
Available Available Available Available Available Available Available Available

-----
Ctrl-a to access these functions, ESC for previous menu      MainMenu Exit
Save      PgDn PgUp  ClearAll      _____      FrAssign

```

Page 2 of 2 is for defining signaling assignments and trunk conditioning for each DSX-1 interface time slot. See DSX-1 Signaling Assignments and Trunk Conditioning for an example of this screen.

For easy movement between screens, select the FrAssign function key to go directly to the Frame Relay Network Assignments screen.

Time Slot Assignment Rules:

- Valid Network time slots are either **Available** or contain a DSX-1 time slot assignment.
- Valid DSX-1 time slots are those that are unassigned, including the currently assigned time slot.
- Order of display is as follows:
 - **Available** is the first selection.
 - Then, from the lowest DSX-1 interface to the highest DSX-1 interface.
 - Then the lowest available time slot number to the highest available time slot number.

For example, if the cursor is on a field with the **Available** value under assigned time slot *Ntt*, pressing the Spacebar causes this field's values to cycle through all valid DSX-1 time slots, starting with *Ds-p/yy*, assuming it is unassigned. If *Ds-p/tt* is already assigned, the next valid time slot in the order described above is displayed.

► Procedure

1. Follow this menu selection sequence:

Configuration → Time Slot Assignment → DSX-to-Network Assignments

The DSX-1 to Network Assignments screen appears. This screen contains a matrix of the current cross-connect status of all time slots on the network interface.

2. Move the cursor to the next time slot that can be edited (underlined). Use the spacebar or type in the desired time slot to display its time slot assignment.
3. Repeat Step 2 until all desired time slots are assigned.
4. Save the configuration.

DSX-1 Signaling Assignments and Trunk Conditioning (Page 2)

The second page of the DSX-1 to Network Assignments screen allows you to define the signaling assignments and trunk conditioning for each time slot on the DSX-1 interface. You can specify whether robbed bit signaling information is being passed within a given DS0, and the value of the signaling bits that will be transmitted for that DS0 to the other cross-connected T1 network interface if a Carrier Group Alarm (CGA) occurs on a T1 network interface.

DSX-1 to Network Time Slot Assignment Screen Example (Page 2)

```

main/config/tslot_assign/dsx                               9128-II
Device Name: Node A                                       5/26/2000 23:32

                                DSX-1 TO NETWORK 1 ASSIGNMENTS
                                SIGNALING AND TRUNK CONDITIONING
                                Page 2 of 2

Network 1 Side      DSX-1 Side      Network 1 Side      DSX-1 Side
Net1/01 E&M-busy - DSX-1/01 E&M-busy   Net1/02 E&M-busy - DSX-1/01 E&M-busy
Net1/03 E&M-busy - DSX-1/03 E&M-busy   Net1/04 E&M-busy - DSX-1/04 E&M-busy
Net1/09 None       - DSX-1/09 None      Net1/10 None       - DSX-1/10 None

-----
Ctrl-a to access these functions, ESC for previous menu   MainMenu  Exit
Save      PgDn  PgUp  ClearAll      ____VocAssign  ErAssign

```

For easy movement between screens, select the ErAssign function key to go directly to the Frame Relay Network Assignments screen or the DSXAssign function key to go to the DSX-1 to Network Assignments screen.

Only those DSX-1-to-Network assignments from page 1 are displayed on this page, from left to right and top to bottom in ascending order, by network and time slot.

When a CGA condition (LOS, OOF, or AIS) is declared for a T1 interface, the signaling bits being transmitted to the other T1 interface for the DS0 are forced to idle for two seconds (except for user-defined patterns which are transmitted immediately). This drops any call in progress. The signaling bits are then forced to the selected state (Busy or Idle), and remain in this state until the CGA condition clears. At this point, the received signaling bits from the T1 interface which formerly had the CGA condition are passed through to the other T1 interface.

NOTE:

Trunk conditioning will only occur on DS0s that are cross-connected to another T1 interface. All other DS0s remain unaffected by trunk conditioning.

Enter one of the values shown in Table 3-10 in each of the fields on both the Network side and the DSX-1 side. Although you can choose any value for the DSX-1 side, the default value displayed is based on a typical setting that would be used with the corresponding Network side value. Typical pairs of values are shown in the table below. If you change the Network side value, the DSX side value is changed to the corresponding default value.

Table 3-10. Signaling and Trunk Conditioning Values (1 of 3)

Network Side	Meaning	DSX-1 Side
None	No signaling used on this DS0. Use this setting if there is no voice signaling information being passed on this DS0 (clear channel).	None
RBS (default)	Robbed Bit Signaling is used on this DS0, but no trunk conditioning. Signaling bits will be passed to the T1 interface to which this DS0 is cross-connected when this T1 interface is not in CGA, but the signaling bits will be all ones when CGA is present.	RBS
The following values configure the cross-connect for RBS, as well as perform the trunk conditioning. Although ABCD signaling bits for each setting are described, only AB bits are transmitted when the cross-connected T1 network interface is using D4 framing.		

Table 3-10. Signaling and Trunk Conditioning Values (2 of 3)

Network Side	Meaning	DSX-1 Side
E&M-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an E&M interface (ABCD = 0000).	E&M idle
E&M-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an E&M interface (ABCD = 1111).	E&M busy
FXOg-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXO Ground-Start interface (ABCD = 1111).	FXSg-idle
FXOg-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXO Ground-Start interface (ABCD = 0101).	FXSg-busy
FXOI-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXO Loop-Start interface (ABCD = 0101).	FXSI-idle
FXOI-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXO Loop-Start interface (ABCD = 0101).	FXSI-busy
FXSg-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXS Ground-Start interface (ABCD = 0101).	FXOg-idle
FXSg-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXS Ground-Start interface (ABCD = 1111).	FXOg-busy
FXSI-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXS Loop-Start interface (ABCD = 0101).	FXOI-idle
FXSI-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXS Loop-Start interface (ABCD = 1111).	FXOI-busy
FXOD-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXODN interface (ABCD = 0000).	FXSD-idle
FXOD-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXODN interface (ABCD = 1111).	FXSD-busy
FXSD-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXSDN interface (ABCD = 0000).	FXOD-idle

Table 3-10. Signaling and Trunk Conditioning Values (3 of 3)

Network Side	Meaning	DSX-1 Side
FXSD-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXSDN interface (ABCD = 1111).	FXOD-busy
PLAR3idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for a PLAR D3 interface (ABCD = 0000).	PLAR3idle
PLAR3busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an PLAR D3 interface (ABCD = 1111).	PLAR3busy
PLAR4idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for a PLAR D4 interface (ABCD = 1111).	PLAR4idle
PLAR4busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an PLAR D4 interface (ABCD = 0000).	PLAR4busy
DPO-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for a DPO interface (ABCD = 0000).	DPT-idle
DPO-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for a DPO interface (ABCD = 1111).	DPT-busy
DPT-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for a DPT interface (ABCD = 0000).	DPO-idle
DPT-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for a DPT interface (ABCD = 1111).	DPO-busy
USER-xxxx	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent a user-defined pattern of ABCD = xxxx.	USER-xxxx ¹
¹ xxxx is the same value on both the Network and the DSX-1 sides.		

Assigning a Synchronous Data Port to Network or DSX-1 Time Slots

For a FrameSaver SLV 9128 or 9128-II, which has two data ports, another assignment screen is available. Use the Sync Data Port Assignment screen to view the status of:

- All DS0 assignments on the Network interface
- All DS0 assignments on the DSX-1 interface

Then, you can assign synchronous data port to:

- Network interface time slots
- DSX-1 interface time slots

Synchronous Data Port Assignment Screen Example

```

main/config/tslot_assign/sync_data/net                                     9128-II
Device Name: Node A                                                         5/26/2000 23:32

                                SYNC DATA PORT ASSIGNMENT

                                Assign To: Net1

    N01      N02      N03      N04      N05      N06      N07      N08
Assigned Assigned Assigned Assigned Assigned Port-2 Port-1 Assigned

    N09      N10      N11      N12      N13      N14      N15      N16
Assigned Assigned Assigned Assigned Assigned Port-2 Port-1 Available

    N17      N18      N19      N20      N21      N22      N23      N24
Available Available Available Available Available Available Available Available1

-----
Ctrl-a to access these functions, ESC for previous menu      MainMenu Exit
Save                  ClearAll                  DSXAssign      FrAssign

```

Value	Meaning
Assign To	Specifies either Net1 (network) or DSX1-1 (DSX-1) time slots.
N <i>tt</i>	This field represents time slot <i>tt</i> of the network interface.
D <i>tt</i>	This field represents time slot <i>tt</i> of the DSX-1 interface.
Assigned	The time slot is already assigned to a network or DSX-1 time slot. Assigned time slots cannot be modified from this screen.
Available	The time slot is currently unassigned.
Port-2	For a FrameSaver SLV 9128 or 9128-II, synchronous data Port-2 is assigned to the time slot.

For easy movement between screens, select the ErAssign function key to go directly to the Frame Relay Network Assignments screen or the DSXAssign function key to go to the DSX-1 to Network Assignments screen.

Time Slot Assignment Rules:

- To assign a synchronous data port to network or DSX-1 time slots, Port-2's Port Use option must be set for Synchronous Data (see Table 3-5, **Data Port Physical Interface Options**).
- If the DSX-1 interface is disabled, only Net1 is available for synchronous data port assignment (see the Interface Status option in Table 3-6, **DSX-1 Physical Interface Options**).

► Procedure

1. Select one of the following menu selection sequences:
Main Menu → Configuration → Time Slot Assignment → Sync Data Port Assignments or
Main Menu → Easy Install → Time Slot Assignment Screen
2. Select an interface in the Assign To field. A matrix of the current cross-connect status of all time slots on the selected interface appears.
3. Move the cursor to the next time slot that can be edited (underlined). Use the spacebar or type in the desired time slot to display its time slot assignment.
4. Repeat Step 3 until the synchronous data port is assigned to all desired time slots.
5. Save the configuration.

Clearing Assignments

Clearing assignments sets all time slots to **Unassgn** (unassigned).

Main Menu → Configuration → Time Slot Assignment → Clear Assignments

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 3-11).

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

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

Table 3-11. 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: <i>For a user data port link: Initialize_From_Interface</i> <i>For a network link: Auto_On_LMI_Fail</i>
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 <i>not</i> be updated based on changes to Net1FR1 after being set initially. <i>Display Conditions</i> – 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 <i>not</i> be updated after being initially discovered. Frame relay links on user data ports discover the LMI protocol from an attached device via LMI status polls. Frame relay links on the network interface discover LMI protocol by sending polls to an attached Network line and “listening” for correct poll response messages. Auto_On_LMI_Fail – The LMI type supported on this frame relay link will be configured to match the LMI protocol discovered from the attached Network line or the DTE device whenever an LMI Link Down failure occurs. This option is available for frame relay links on the Port and network interfaces. Frame relay links on user data ports discover the LMI protocol from LMI status polls by attached DTE devices. Frame relay links on the network interface 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 3-11. 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 3-1, System Frame Relay and LMI Options). Custom – Use the following options in this table to configure LMI parameters.
Frame Relay DS0s Base Rate
Possible Settings: Nx64, Nx56 Default Setting: Nx64
Selects the base rate for the DS0s allocated to frame relay on the network interface. <i>Display Conditions</i> – This option only appears on the network interface of the FrameSaver SLV 9128, not the 9128-II. Nx64 – The base rate is 64 kbps. Nx56 – The base rate is 56 kbps.
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 3-11. 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 3-12).

Main Menu → Configuration → [Network/Data Port/ISDN] → DLCI Records

ISDN is only available when the FrameSaver unit has an ISDN DBM installed.

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 3-12. 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 (inclusive).
DLCI Type
Possible Settings: Standard, Multiplexed Default Setting: <i>For user data port DLCIs: Standard</i> <i>For network interface DLCIs: Multiplexed</i>
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.
<i>Display Conditions</i> – This option does not appear for a user data port, and it cannot be changed if the DLCI is specified as the TS Access Management Link.
Standard – Supports standard DLCIs as specified by the Frame Relay Standards. Use this setting when a non-FrameSaver unit is at the other end.
Multiplexed – Enables multiplexing of multiple connections into a single DLCI. Allows a single PVC through the frame relay network to carry multiple DLCIs as long as these connections are between the same two endpoints (proprietary). Do not select Multiplexed unless there are FrameSaver units at both ends of the connection.

Table 3-12. DLCI Record Options (2 of 3)

CIR (bps)
Possible Settings: 0 – 1536000 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 – 1536000 – Specifies the network-committed data rate.
Tc
Possible Settings: 1 – 65535 Default Setting: Read Only
Displays the DLCI's calculated value of its committed rate measurement interval (Tc) in milliseconds. This value is calculated based upon the settings for the Committed Burst Size Bc (Bits) and CIR (bps) options.
Committed Burst Size Bc (Bits)
Possible Settings: CIR, Other Default Setting: CIR
Specifies whether the DLCI's committed burst size will follow the CIR, or whether it will be entered independently. This value is the maximum amount of data that the service provider has agreed to accept during the committed rate measurement interval (Tc). CIR – Uses the value in the CIR (bps) option as the committed burst size (Bc). The Bc and excess burst size (Be) options are updated when a CIR update is received from the network switch. Other – Allows you to specify the committed burst size for the DLCI. When Other is selected, the Bc and Be values must be manually entered and maintained, as well.
Bc
Possible Settings: 0 – 1536000 Default Setting: 64000
Allows you to display or change the DLCI's committed burst size. <i>Display Conditions</i> – This option only appears when Committed Burst Size is set to Other. 0 – 1536000 – Specifies the DLCI's committed burst size.
Excess Burst Size (Bits)
Specifies the maximum amount of data in bits that the network may accept beyond the CIR without discarding frames.
Be
Possible Settings: 0 – 1536000 Default Setting: 1472000
Allows you to display or change the DLCI's excess burst size. 0 – 1536000 – Specifies the DLCI's excess burst size.

Table 3-12. DLCI Record Options (3 of 3)

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 <i>quality of service</i>). All data on Port 1 is cut-through, as long as there is no higher-priority data queued from another user port. The DLCI priority set for an interface applies to data coming into that interface. For example, the priority set for DLCIs on Port 1 applies to data coming into Port 1 from the attached equipment (such as a router). NOTE: For units with multiple user data ports, since pipelining occurs on Port-1, it is recommended that higher priority data be connected to Port-1 . <i>Display Conditions</i> – This option is not available for the network interface or, if the model has ISDN backup capability, an ISDN DBM interface. Low – Data configured for the DLCI has low priority. Medium – Data configured for the DLCI has medium priority. High – Data configured for the DLCI has high priority.
Outbound Management Priority
Possible Settings: Low, Medium, High Default Setting: Medium
Specifies the relative priority for management traffic sent on management PVCs on this DLCI to the network. <i>Display Conditions</i> – This option is not available on a user data port. Low – Management data configured for the DLCI has low priority. Medium – Management data configured for the DLCI has medium priority. High – Management data configured for the DLCI has high priority.
Backup Group
Possible Settings: A, B, C, . . . Z, None Default Setting: None
Assigns DLCIs to a backup group so backup does not take place unless all DLCIs in the group are no longer operational or latency has been exceeded. Backup is terminated when one DLCI in the group is operational again. This feature reduces backup charges when redundant PVCs have been configured. <i>Display Conditions</i> – This option is not available on a user data port or ISDN DBM interface. A – Z – Specifies the designation for this group of DLCIs. Only DLCIs in a PVC will be considered part of a Backup Group. None – No Backup Groups have been set up.

Configuring PVC Connections

The Auto-Configuration feature automatically configures PVC Connections and their DLCI Records. PVC Connections can also be created manually (see [Table 3-13](#)).

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 (and ISDN Link Profiles, except for HQ_Site, if the model has an ISDN DBM installed) included in an existing PVC Connection 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 3-13. PVC Connection Options (1 of 3)

Source Link
Possible Settings: Port-n, ISDN Link Name, 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. Net1-FR1 – Specifies that the network interface be used in the connection. ISDN Link Name – For units with ISDN backup capability, specifies the ISDN link of the DBM as the source link. This can be any nonnull link name configured on an ISDN frame relay link. Port-n – Specifies that the frame relay link on the user data port be used in the connection. 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. <i>Display Conditions</i> – This option only appears when Source DLCI contains a multiplexed DLCI record number. 0 – 62 – Specifies the EDLCI number.

Table 3-13. PVC Connection Options (2 of 3)

Primary Destination Link
Possible Settings: Net1-FR1, ISDN Link Name 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 interface has no DLCIs defined, Net1-FR1 would not appear as a valid setting. Net1-FR1 – Specifies the Network interface as the destination link. ISDN Link Name – For units with ISDN backup capability, specifies the ISDN link of the DBM as the destination of the connection. This can be any nonnull link name configured on an ISDN frame relay 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. NOTES: – Primary Destination DLCI has no value if Primary Destination Link contains no value. – When an ISDN DBM is installed and the DLCI assigned to the PVC is in a Backup Group (see Table 3-12, DLCI Record Options), the letter designation assigned to the group of DLCIs appears next to the primary destination DLCI number on the Management PVCs Options screen. 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. <i>Display Conditions</i> – This option only appears when the Primary Destination DLCI contains a multiplexed DLCI record number. 0 – 62 – Specifies the EDLCI number.

Table 3-13. PVC Connection Options (3 of 3)

Alternate Destination Link
Possible Settings: Net1-FR1, ISDN Link Name Default Setting: Initially blank; no default. Specifies the frame relay interface used as the alternate destination link; the <i>to</i> end of a from-to link that is used for backup when the primary destination link or DLCI is out of service. 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 <i>ISDN Link Name</i> has no DLCIs defined, the ISDN link name would not appear as a valid setting. Net1-FR1 – Specifies the Network interface as the destination link. ISDN Link Name – Specifies the ISDN link of the DBM as the destination of the connection. This can be any non-null link name configured on an ISDN frame relay link on an installed DBM. Clear Alternate – Clears the Alternate Destination Link and Alternate Destination DLCI settings, and suppresses Alternate Destination EDLCI.
Alternate Destination DLCI
Possible Settings: 16 – 1007 Default Setting: Initially blank; no default. Specifies the alternate destination Data Link Connection Identifier (DLCI) for a frame relay interface used for backup. 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. <i>Display Conditions</i> – This option does not appear when the Alternate Destination Link contains no value. 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 backup connection. <i>Display Conditions</i> – This option only appears 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
- Communication Port Options
- Modem Port Options
- Auto Backup Criteria Options

Configuring Node IP Information

Select Node IP to display, add, or change the information necessary to support general IP communications for the node (see [Table 3-14](#)). 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 Access 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_Access_Management_Link is initially disabled in most models, but the link can be enabled at any time. Any valid network Management PVC created on a standard DLCI can be used. When enabled, a troubleshooting link can be accessed any time the service provider requests access. An assigned security level can also control access.

When a DLCI has been defined as the troubleshooting management link, the link is identified in the status field at the bottom of the Management PVC Entry screen with the **Note: This PVC has been designated as the TS Access Management Link** message.

NOTE:

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

Table 3-14. Node IP Options (1 of 3)

Node IP Address
Possible Settings: 001.000.000.000 – 223.255.255.255, Clear Default Setting: Clear (000.000.000.000)
Specifies the IP address needed to access the node. Since an IP address is not bound to a particular port, it can be used for remote access via a management PVC.
001.000.000.000 – 223.255.255.255 – Shows the IP address for the node, which can be viewed or edited.
Clear – Fills the node IP address with zeros.
Node Subnet Mask
Possible Settings: 000.000.000.000 – 255.255.255.255, Clear Default Setting: 000.000.000.000
Specifies the subnet mask 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 3-14. Node IP Options (2 of 3)

Default IP Destination
Possible Settings: None, Modem, COM, Ethernet, PVCname Default Setting: None Specifies an IP destination to route data that does not have a specifically defined route. Examples: ■ If the default IP network is connected to the communications port, select COM. ■ If the default IP network is connected to a far-end device over the management PVC named London for the remote device located in the London office, select the PVC name London (as defined by the Name configuration option, Table 3-15, Management PVC Options). NOTE: If the link to the IP destination selected as the default route becomes disabled or down, the unroutable 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 the modem port Use option is set to Net Link. COM – Specifies that the default destination is connected to the COM port. Only appears when Port Use is set to Net Link (see Table 3-21, Communication Port Options). Ethernet – For the FrameSaver SLV 9128-II only, specifies that the default destination is connected to the Ethernet port. Only appears when the Ethernet port's Interface Status option is enabled. When selected, the Default Gateway Address must also be configured (see Table 3-20, Ethernet Port Options). PVCname – Specifies a name for the management PVC. Only appears when a management PVC name is defined for the node. For example, when the network is connected to a remote device located in the London office, London can be specified as the PVC name, which is the link between the local FrameSaver unit and the one located in London. London would appear as one of the available selections.
TS Access Management Link
Available Settings: None, PVCname Default Setting: None Specifies a troubleshooting management link for the special needs of network service providers. If the setting is changed from the management PVC name to None, the Delete the Management PVC PVCname and the associated DLCI 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 Access Management Link. PVCname – Specifies the name of the TS Management PVC. <i>Display Conditions</i> – 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.

Table 3-14. Node IP Options (3 of 3)

TS Management Link Access Level
Available Settings: Level-1, Level-2, Level-3 Default Setting: Level-1
Specifies the highest access level allowed when accessing the unit via a Telnet or FTP session when the service provider is using the TS Access Management Link. <i>Display Conditions</i> – This option only appears when TS Access Management Link is set to None. NOTES: Telnet and FTP sessions on this link <i>are not</i> affected by the access level set by the Session Access Level, Login Required, or FTP Login Required option settings (see Table 3-17, Telnet and FTP Session Options). Telnet and FTP sessions on this link <i>are</i> 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 3-15](#)). 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.

These options do not apply when the Management PVC is designated as a TS Management Link (see [Configuring Node IP Information](#) for additional information).

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

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

Table 3-15. 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., Tampa for Tampa, Florida). ASCII Text Entry – Enter a unique name for the management PVC (maximum length 8 characters).
Intf IP Address
Possible Settings: Node-IP-Address, Special (<i>nnn.nnn.nnn.nnn</i>) 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 3-14, Node IP Options). Special (001.000.000.000 – 223.255.255.255) – Allows you to display/edit an IP address for the unit's management PVC when the IP address for this interface is different from the node's IP address.
Intf Subnet Mask
Possible Settings: Node-Subnet-Mask, Calculate, Special (<i>nnn.nnn.nnn.nnn</i>) 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 <i>Interface</i> IP Subnet contained in the Node-Subnet Mask configuration option (see Table 3-14, 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.

Table 3-15. Management PVC Options (2 of 4)

Primary Link
Possible Settings: Net1-FR1, Port-n, ISDN Link Name, 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 the network interface as the source link for the connection. Port-n – Specifies the frame relay link on the user data port as the destination link for the connection. ISDN Link Name – For units with ISDN backup capability, specifies the ISDN link on the DBM to be used in the connection. This can be any nonnull link name configured on an ISDN frame relay link on an installed DBM. Clear – Clears the link and the DLCI field, and suppresses the EDLCI field if the DLCI was multiplexed.
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. – When an ISDN DBM is installed and the DLCI assigned to the PVC is in a Backup Group (see Table 3-12, DLCI Record Options), the letter designation assigned to the group of DLCIs appears next to the primary destination DLCI number on the Management PVCs Options screen. 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. <i>Display Conditions</i> – 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).

Table 3-15. Management PVC Options (3 of 4)

Primary Link RIP
Possible Settings: None, Proprietary, Standard_out Default Setting: For multiplexed DLCIs: Proprietary For nonmultiplexed DLCIs: Standard_out
Specifies which Routing Information Protocol (RIP) is used to enable routing of management between FrameSaver units and attached equipment. None – Does not use a routing protocol. Proprietary – Uses a proprietary variant of RIP version 1 to communicate routing information between FrameSaver units. A FrameSaver unit must be on the other end of the link. This is the factory default for management PVCs configured on multiplexed DLCIs (see Table 3-12, DLCI Record Options). Standard_out – The device will send standard RIP messages to communicate routing information only about FrameSaver SLV and FLEX devices 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 serialx, IP RIP Receive version 1, ct1-z WR). See Setting Up So the Router Can Receive RIP.
Alternate Link
Possible Settings: Net1-FR1, Port-n, ISDN Link Name, Clear Default Setting: Initially blank; no default.
Specifies the frame relay interface to use for this management PVC as the alternate link. 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. <i>Display Conditions</i> – This option does not appear unless ISDN backup is available. Net1-FR1 – Specifies the Network interface as the frame relay link. Port-n – Specifies the frame relay link on the user data port as the alternate destination link for the connection. ISDN Link Name – For units with ISDN backup capability, specifies the ISDN link of the DBM to be used in the connection. This can be any nonnull link name configured on an ISDN frame relay link on an installed DBM. Clear – Clears the link and the DLCI field, and suppresses the EDLCI field if the DLCI was multiplexed.
Alternate DLCI
Possible Settings: 16 – 1007 Default Setting: Initially blank; no default.
Specifies the alternate DLCI number to be 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. <i>Display Conditions</i> – The DLCI cannot be entered if the Link field is blank. NOTE: Clearing Link also clears the DLCI. 16 – 1007 – Specifies the DLCI number (inclusive).

Table 3-15. Management PVC Options (4 of 4)

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 for the frame relay link. 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. <i>Display Conditions</i> – This option does not appear unless ISDN backup is available and the DLCI field does not reference a multiplexed DLCI. NOTE: Clearing the DLCI or changing it to a standard DLCI suppresses the 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 3-16).

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

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

Table 3-16. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: Enable, Disable Default Setting: Enable
Determines whether the FrameSaver unit can be managed as an SNMP agent by an SNMP-compatible NMS. Enable – Can be managed as an SNMP agent. Disable – Cannot be managed as an SNMP agent. The FrameSaver unit will not respond to SNMP messages nor send SNMP traps.
Community Name 1
Possible Settings: ASCII text entry, Clear Default Setting: Public in ASCII text field
Specifies the first of two names that are allowed to access the objects in the FrameSaver unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB. ASCII text entry – Adds to or changes Community Name 1 (maximum 255 characters). Clear – Clears Community Name 1.

Table 3-16. General SNMP Management Options (2 of 2)

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 3-17).

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

When a TS Access 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 3-17. Telnet and FTP Session Options (1 of 2)

Telnet Session
Possible Settings: Enable, Disable Default Setting: Enable
Specifies whether the FrameSaver unit will respond to a session request from a Telnet client on an interconnected IP network. Enable – Allows Telnet sessions between the FrameSaver unit and Telnet client. Disable – Does not allow Telnet sessions.
Telnet Login Required
Possible Settings: Enable, Disable Default Setting: Disable
Specifies whether a user ID and password (referred to as the login) are required to access the menu-driven user interface via a Telnet session. If required, the login used is the same login used for an menu-driven user interface session. This option does not affect the TS Access Management Link. Enable – Requires a login to access a Telnet session. Disable – Does not require a login.
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 <i>not</i> required, the effective access level is determined by this option. This option does not affect the TS Access Management Link. NOTE: The effective access level is always the lowest one assigned to either the session or the user. For example, if the assigned Session Access Level is Level-2, but the User Access Level is Level-3, then only level-3 access is allowed for the session. Level-1 – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information, change configuration options, and run tests. This is the highest access level allowed. CAUTION: Before changing the session access level to Level-2 or 3, make sure that the COM port's Port Access Level is set to Level-1 and that at least one Login ID is set to Level-1. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. A reset is required if the Communication Port's Port Use option is set to Net Link (see Table 3-3, 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.

Table 3-17. Telnet and FTP Session Options (2 of 2)

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. <i>Display Conditions</i> – This option does not appear when Inactivity Timeout is disabled. 1 – 60 – Up to an hour can be set.
FTP Session
Possible Settings: Enable, Disable Default Setting: Enable
Determines whether the system responds as a server when an FTP (file transfer protocol) client on an interconnected IP network requests an FTP session. This option must be enabled when downloading files. Enable – Allows an FTP session between the system and an FTP client. Disable – Does not allow FTP sessions.
FTP Login Required
Possible Settings: Enable, Disable Default Setting: Disable
Specifies whether a login ID and password are required for an FTP session. If required, the login used is the same login used for a menu-driven user interface session. This option does not affect the TS Access Management Link. Enable – User is prompted for a login ID and password. Disable – No login is required for an FTP session.
FTP Max Transfer Rate (kbps)
Possible Settings: 1 – 1536 Default Setting: 1536
Sets the maximum receive (or send) rate of file transfer to the system via management PVCs. This option allows new software and configuration files to be downloaded using selected bandwidth without interfering with normal operation. Using this option, new software and configuration files can be downloaded quickly using the default settings, or at a slower rate over an extended period of time by selecting a slower speed. Based upon TCP flow control, the FTP server in the system throttles bandwidth to match this setting. 1 – 1536 – 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 3-18).

*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 3-18. SNMP NMS Security Options (1 of 2)

NMS IP Validation
Possible Settings: Enable, Disable Default Setting: Disable
Specifies whether security checks are performed on the IP address of SNMP management systems attempting to access the node. Only allows access when the sending manager's IP address is listed on the SNMP NMS Security Options screen. Enable – Performs security checks. Disable – Does not perform security checks.
Number of Managers
Possible Settings: 1 – 10 Default Setting: 1
Specifies the number of SNMP management systems that are authorized to send SNMP messages to the FrameSaver unit. An IP address must be configured for each management system allowed to send messages. Configure IP addresses in the NMS <i>n</i> IP Address configuration option. 1 – 10 – Specifies the number of authorized SNMP managers.
NMS <i>n</i> 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. <i>Display Conditions</i> – 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.

Table 3-18. SNMP NMS Security Options (2 of 2)

Access Type
Possible Settings: Read, Read/Write Default Setting: Read
Specifies the type of access allowed for an authorized NMS when IP address validation is performed. <i>Display Conditions</i> – 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 3-19).

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 3-19. 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 <i>n</i> IP Address configuration option for each trap manager to receive trap messages. 1 – 6 – Specifies the number of trap managers (inclusive).

Table 3-19. SNMP Traps and Trap Dial-Out Options (2 of 5)

NMS <i>n</i> 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. <i>Display Conditions</i> – 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.
Initial Route Destination
Possible Settings: AutoRoute, Modem, COM, Ethernet, 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. <i>Display Conditions</i> – 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 3-14, Node IP Options). Modem – Uses the Modem port. This selection only appears if the Modem Port Use configuration option is set to Net Link (see Table 3-22, Modem Port Options). COM – Uses the COM port. This selection is only available when Port Use is set to Net Link (see Table 3-21, Communication Port Options). Ethernet – For the FrameSaver SLV 9128-II only, uses the Ethernet port. Only appears when the Ethernet port's Interface Status option is enabled (see Table 3-20, Ethernet Port Options). PVCname – Uses the defined management <i>linkname</i> (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). An authenticationFailure trap indicates that the unit is the addressee of an SNMP protocol message, or an incoming ISDN call is not properly authenticated. 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.

Table 3-19. SNMP Traps and Trap Dial-Out Options (3 of 5)

Enterprise Specific Traps
Possible Settings: Enable, Disable Default Setting: Enable
Determines whether trap messages for enterpriseSpecific events are sent to the currently configured trap manager(s). Enable – Sends trap messages for enterpriseSpecific events. Disable – Does not send trap messages for enterpriseSpecific events.
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, DSX-1, T1s, Ports, DBM, All Default Setting: All
Specifies which interfaces will generate linkUp, linkDown, and enterpriseSpecific trap messages. These traps are not supported on the COM port or Modem port. Network – Generates these trap messages on the network interface only. DSX-1 – For applicable T1 FrameSaver units, generates these trap messages on the DSX-1 interface only. T1s – For applicable T1 FrameSaver units, generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on both the T1 network and DSX-1 interfaces. Ports – Generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on a user data port only. DBM – For units with an ISDN DBM installed, generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on the DBM only. All – Generates these trap messages for linkUp and enterpriseSpecific events on all interfaces, except for the COM port or modem port, that are applicable to the FrameSaver model.

Table 3-19. SNMP Traps and Trap Dial-Out Options (4 of 5)

DLCI Traps on Interfaces
Possible Settings: Network, Ports, DBM, 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. DBM – For units with an ISDN DBM installed, generates trap messages on DLCIs for the DBM only. All – Generates these trap messages on all frame relay interfaces. None – No DLCI trap messages are generated.
RMON Traps
Possible Settings: Enable, Disable Default Setting: Enable
Specifies whether remote monitoring traps are sent to the currently configured trap manager(s). RMON traps are typically sent as a result of the Alarms and Events Groups of RMON1 when a selected variable's configured threshold is exceeded. Enable – Sends trap messages when set thresholds are exceeded. Disable – Does not send trap messages when set thresholds are exceeded.
ISDN Dial Control Traps
Possible Settings: Enable, Disable Default Setting: Disable
Controls whether dialCtlPeerCallSetup and dialCtlPeerCallInformation events send trap messages to the currently configured SNMP trap manager(s). Use this feature when peer-to-peer (nearest neighbor) calling is desired. <i>Display Conditions</i> – This option only appears when an ISDN DBM is installed. Enable – Sends trap messages. Disable – Does not send trap messages.
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. NOTE: When the modem port is configured as a network communication link, up to 10 SNMP trap messages are held at the port. 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.

Table 3-19. SNMP Traps and Trap Dial-Out Options (5 of 5)

Trap Disconnect
Possible Settings: Enable, Disable Default Setting: Enable
Determines whether the internal 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. 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
Controls whether an incomplete call (busy, no answer, etc.) is retried when an SNMP trap message is sent to the modem port. If an Alternate Dial-Out Directory is specified, 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). 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 the Call Retry option). 1 – 10 – Sets the number of minutes for the delay between call retry attempts.
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. 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

For the FrameSaver SLV 9128-II only, select Ethernet Port from the Management and Communication menu, or Ethernet Port Options Screen from the Easy Install screen, to configure the Ethernet port (see Table 3-20).

Main Menu → Configuration → Management and Communication → Ethernet Port

Main Menu → Easy Install → Ethernet Port Options Screen

Table 3-20. Ethernet Port Options (1 of 2)

Interface Status
Possible Settings: Enable, Disable Default Setting: Disable
Determines whether the Ethernet port is being used and can be configured. Enable – The port is active. It can receive Version 2 or IEEE 802.3 MAC frames and transmit Version 2 MAC frames only. When the Ethernet port is enabled, the would you like to set the Node's IP Destination to Ethernet? prompt is displayed. ■ If you select Yes, the Default IP Destination (see Table 3-14, Node IP Options) is automatically changed to Ethernet, so the Ethernet port's Default Gateway Address is used for packets that do not have a route. This is required when the NMS is on a different subnet than the unit. ■ If you select No, the COM port or a PVC will be used for packets without a route. Disable – The port is not active. When the port is disabled, the following will occur: ■ No alarms or traps configured for the port will be generated. ■ All port uses that refer to the Ethernet port, like the Default IP Destination and Initial Route Destination, will be reset to their default values (see Table 3-14, Node IP Options, and Table 3-19, SNMP Traps Options).
IP Address
Possible Settings: 001.000.000.000 – 223.255.255.255, Clear Default Setting: Clear (000.000.000.000)
Specifies the IP address needed to access the Ethernet port. 001.000.000.000 – 223.255.255.255 – Shows the IP address for the port, which can be viewed or edited. Clear – Fills the IP address with zeros.
Subnet Mask
Possible Settings: 000.000.000.000 – 255.255.255.255, Clear Default Setting: 000.000.000.000
Specifies the subnet mask associated with the IP address that is needed to access the Ethernet port. 000.000.000.000 – 255.255.255.255 – Set the Ethernet port's subnet mask. The range for each byte is 000 to 255. Clear – Fills the subnet mask associated with the IP address with zeros.

Table 3-20. Ethernet Port Options (2 of 2)

Default Gateway Address
Possible Settings: 001.000.000.000 – 223.255.255.255, Clear Default Setting: Clear (000.000.000.000) Specifies the IP address for the port's default gateway. It is used for packets that do not have a route. 001.000.000.000 – 223.255.255.255 – Shows the IP address for the port, which can be viewed or edited (i.e., a router on the LAN). Clear – Fills the default gateway's IP address with zeros.
Proxy ARP
Possible Settings: Enable, Disable Default Setting: Disable Determines whether the FrameSaver unit will use the Proxy ARP (Address Resolution Protocol) technique, acting as the gateway to other FrameSaver devices in its management network when there is an ARP request for a device not on the Ethernet. Enable – Proxy ARP is enabled on the port so the FrameSaver unit will act as an agent for or gateway to other units in its management network. Using this technique, the FrameSaver unit returns its own MAC (Media Access Control) address in response to ARP requests when it recognizes that the destination IP address is in its subnet, but the device sending the ARP request is in another network. Packets sent to the FrameSaver unit's gateway address are forwarded to the appropriate device. Disable – The Proxy ARP technique will not be used by the unit; it will not act as an agent for other devices in its network.

Configuring the Communication Port

Select Communication Port from the Management and Communication menu to display or change the communication port configuration options (see Table 3-21).

Main Menu → Configuration → Management and Communication → Communication Port

Table 3-21. Communication Port Options (1 of 5)

Port Use
Possible Settings: Terminal, Net Link, Modem PassThru Default Setting: Terminal
Assigns a specific use to the COM port. NOTE: If the Default IP Destination is set to COM (see Table 3-14, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. Terminal – The COM port is used for the asynchronous terminal connection. Net Link – The COM port is the network communications link to the IP network or IP device port. You cannot change Port Use to Net Link when the Modem PassThru feature is enabled. When you try, the Cannot change Port Use – Modem PassThru is enabled message is displayed. Modem PassThru – Available to the FrameSaver SLV 9626 only, the COM port is connected to the router's auxiliary (AUX) or console port so the router can be accessed via a dial-up connection to the unit. When this feature is active, a logical connection between the unit's modem and COM ports is made, and data received over the modem port is transmitted out the COM port to the router's AUX or console port. When an escape sequence (minus, minus, minus, with a minimum of 50 ms between each) is detected, the FrameSaver unit switches back to normal user interface operation.
Data Rate (Kbps)
Possible Settings: 9.6, 14.4, 19.2, 28.8, 38.4, 57.6, 115.2 Default Setting: 19.2
Specifies the rate for the COM port in kilobits per second. 9.6 – 115.2 kbps – Sets the communication port speed.
Character Length
Possible Settings: 7, 8 Default Setting: 8
Specifies the number of bits needed to represent one character. NOTE: Character length defaults to 8 and cannot be changed if Port Use is set to Net Link. 7 – Sets the character length to seven bits. 8 – Sets the character length to eight bits. Use this setting if using the COM port as the network communication link.

Table 3-21. 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 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 port. 1 – Provides one stop bit. 2 – Provides two stop bits.
Ignore Control Leads
Possible Settings: Disable, DTR Default Setting: Disable
Specifies whether DTR is used. Disable – Treats control leads as standard operation. DTR – Ignores DTR. This may be necessary when connecting to some PAD devices.
Login Required
Possible Settings: Enable, Disable Default Setting: Disable
Determines whether a user ID and password (referred to as the login) is required in order to log on to the asynchronous terminal connected to the COM port. <i>Display Conditions</i> – 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 3-21. 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 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 <i>not</i> 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. <i>Display Conditions</i> – 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 either Telnet Session Access Level or the Modem Port's Port 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). <i>Display Conditions</i> – 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. <i>Display Conditions</i> – This option only appears when Port Use is set to Terminal. 1 – 60 – Sets the time from 1 to 60 minutes (inclusive).

Table 3-21. 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 port. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). <i>Display Conditions</i> – This option only appears when Port Use is set to Net Link. 001.000.000.000 – 223.255.255.255 – Shows the IP address for the COM port, which you can view or edit. Clear – Clears the IP address for the COM port and fills the address with zeros. When the IP Address is all zeros, the COM port uses the Node IP Address if one has been configured.
Subnet Mask
Possible Settings: 000.000.000.000 – 255.255.255.255, Clear Default Setting: 000.000.000.000
Specifies the subnet mask needed to access the unit. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). <i>Display Conditions</i> – This option only appears when Port Use is set to Net Link. 000.000.000.000 – 255.255.255.255 – Shows the subnet mask for the COM port, which you can view or edit. Clear – Clears the subnet mask for the COM port and fills the address with zeros. When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.
RIP
Possible Settings: None, Standard_out Default Setting: None
Specifies which Routing Information Protocol (RIP) is used to enable routing of management data between devices. <i>Display Conditions</i> – This option only appears when Port Use is set to Net Link. None – No routing is used. Standard_out – The device will send standard RIP messages to communicate routing information about other FrameSaver units in the network. Standard RIP messages received on this link are ignored. NOTE: The router must be configured to receive RIP on the port connected to the COM port, configured as the management interface (e.g., Cisco: config-t, router RIP, int serialx, IP RIP Receive version 1, ctl-z WR). To create this management interface, make sure that Node or COM port IP Information has been set up (see <i>Configuring Node IP Information</i>).

Table 3-21. Communication Port Options (5 of 5)

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). <i>Display Conditions</i> – This option only appears when Port Use is set to Net Link. PPP – Point-to-Point Protocol. SLIP – Serial-Line Internet Protocol.

Configuring the Modem Port

Select Modem Port from the Management and Communication menu to configure the modem port (see Table 3-22).

Main Menu → Configuration → Management and Communication → Modem Port

Table 3-22. Modem Port Options (1 of 4)

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 3-14, 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 a network communications link to the IP network. You cannot change Port Use to Net Link when the Modem PassThru feature is enabled. When you try, the Cannot change Port Use – Modem PassThru is enabled message is displayed. See <i>Modem Operation</i> in Chapter 5, <i>Operation and Maintenance</i> , for more information about Modem PassThru operation.
Dial-In Access
Possible Settings: Enable, Disable Default Setting: Enable
Controls whether external devices can dial-in to the system through the internal modem. This allows dial-in access by a remote terminal when Port Use is set to Terminal. When Port Use is set to Net Link, Dial-In Access must be set to Enable to allow an external NMS to dial in to the device. Enable – Dial-in access is allowed. Incoming calls are answered. Disable – Dial-in access is not allowed. Incoming calls are not answered. You cannot disable Dial-In Access when the Modem PassThru feature is enabled. When you try, the Cannot change Dial-In Access when Modem PassThru is enabled message is displayed. See <i>Modem Operation</i> in Chapter 5, <i>Operation and Maintenance</i> , for more information about Modem PassThru operation.

Table 3-22. Modem Port Options (2 of 4)

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 modem port. <i>Display Conditions</i> – 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 require a login.
Port Access Level
Possible Settings: Level-1, Level-2, Level-3 Default Setting: Level-1
Specifies the level of user access privilege for an asynchronous terminal connected to the modem port. 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 modem port. <i>Display Conditions</i> – 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, save, and perform device testing. If Login Required is set to Enable, the effective access level is determined by the user's access level. Otherwise, the access level is 1. CAUTION: Before changing the modem port's access level to Level-2 or 3, make sure that either Telnet Session Access Level or the communications port's Port Access Level is set to Level-1 and at least one Login ID are 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. If Login Required is set to Enable, the effective access level is 2 for User ID access levels of 1 or 2. User IDs set to access Level-3 have only Level-3 access. Level-3 – Allows limited access with monitoring control only. The user can only display and monitor status and configuration screens. If Login Required is set to Enable, the effective access level is 3 for all user IDs.
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). <i>Display Conditions</i> – This option only appears when Port Use is set to Terminal. Enable – Disconnects the user session after the specified time of inactivity. Disable – Does not disconnect the user session.

Table 3-22. Modem Port Options (3 of 4)

Disconnect Time (Minutes)
Possible Settings: 1 – 60 Default Setting: 10
Determines the amount of lapsed time before disconnecting a user session in minutes. <i>Display Conditions</i> – This option only appears when: ■ Port Use is set to Terminal. ■ Inactivity Timeout is set to Enable. 1 – 60 – Sets the number of minutes allowed before the modem disconnects.
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 system via the modem port. This option is only in effect when the modem port is configured as a network communication link. <i>Display Conditions</i> – 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. Clear – Clears the IP address for the modem port and fills the address with zeros (i.e., 000.000.000.000). When the IP Address is all zeros, the modem 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 system. This option is only in effect when the modem port is configured as a network communication link. <i>Display Conditions</i> – 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 modem port, which you can view or edit. Clear – Clears the subnet mask for the COM port and fills the address with zeros. When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.
Link Protocol
Possible Settings: PPP, SLIP Default Setting: PPP
Specifies the link-layer protocol to be used. This option is only in effect when the modem port is configured as a network communication link. <i>Display Conditions</i> – This option only appears when Port Use is set to Net Link. PPP – Point-to-Point Protocol. SLIP – Serial-Line Internet Protocol.

Table 3-22. Modem Port Options (4 of 4)

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 modem port. If this configuration option is not configured (i.e., it is zero), the modem port's primary IP address is used when the alternate telephone directory is used for dial-out traps. <i>Display Conditions</i> – This option only appears when Port Use is set to Net Link. 001.000.000.000 – 223.255.255.255 – Shows the modem's alternate IP address, which you can view or edit. Clear – Clears the alternate IP address for the modem port and fills the address with zeros.
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 needed to access the unit. Only in effect when the modem port is configured as a network communication link. <i>Display Conditions</i> – 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 modem port, which you can view or edit. Clear – Clears the subnet mask for the modem 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.

Configuring the Criteria for Automatic Backup

For units with an ISDN DBM, follow this menu selection sequence to specify whether and when automatic backup is allowed, and to configure timers that will control and terminate backup, or set delays (see Table 3-23).

Main Menu → Configuration → Auto Backup Criteria

Table 3-23. Auto Backup Criteria Options (1 of 2)

Auto Backup
Possible Settings: Enable, Disable Default Setting: Disable
Determines whether backup for the access unit is automatically performed when the primary physical link or LMI, or a DLCI on a PVC connection fails, or when latency is exceeded. When enabled, the access unit automatically enables the Alternate Link configuration option, and establishes an alternate DLCI and EDLCI, rerouting traffic over the backup interface. (See Table 3-15, Management PVC Options, to configure the alternate DLCI and alternate EDLCI.) NOTE: Auto Backup cannot be enabled unless LMI Behavior is set to Independent (see Table 3-1, System Frame Relay and LMI Options). Enable – Reroutes traffic over the backup (alternate) interface. Disable – Does not reroute traffic over the backup interface.
DLCI Down Backup Activation Delay (sec)
Possible Settings: 0 – 3600 Default Setting: 0
Specifies the number of seconds the unit will wait once a DLCI is declared down before it initiates backup. A DLCI is declared down when the DLCI changes to Inactive status in an LMI response, or when there is an LMI or physical link failure. When a delay is configured, the unit is more tolerant of network glitches, or repeated short outages, before going into backup, minimizing bouncing between network and backup services. 0 – 3600 – Specifies the amount of time for the delay.
DLCI Down Backup Activation Transition Threshold
Possible Settings: 1 – 10 Default Setting: 1
Specifies how many times a primary destination DLCI transitions up or down during the DLCI Down Backup Activation Delay period before the unit initiates backup, provided the DLCI is active when the delay period ends. 1 – 10 – Specifies the number of transitions allowed between Active and Inactive status.
Backup Restoration Delay (sec)
Possible Settings: 0 – 3600 Default Setting: 0
Specifies the number of seconds the unit will wait after all backup alarm conditions have cleared for a primary destination DLCI before the backup connection is terminated. 0 – 3600 – Specifies the amount of time for the delay.

Table 3-23. Auto Backup Criteria Options (2 of 2)

When Auto Backup Allowed
Possible Settings: Always, Restrict Default Setting: Always
Determines when backup for the access unit is allowed to occur. Always – No restrictions on backup. Restrict – Backup is restricted to the day and time selected in the following configuration options. Use this selection when the importance of the data that you are backing up is day/time dependent.
Backup Allowed: Day From nn:nn
Possible Settings: 00:00 – 23:00, None Default Setting: 00:00
Specifies the time that Auto Backup can begin for a selected day of the week in increments of 1 hour. <i>Day</i> is Monday through Sunday. 00:00 – 23:00 – Specifies the time of day that Auto Backup will start for this particular day. None – Auto Backup cannot occur on this day.
Backup Allowed: Day To nn:nn
Possible Settings: 00:00 – 24:00 Default Setting: 24:00
Specifies the time that Auto Backup must end occurring for the selected day of the week in increments of 1 hour. <i>Display Conditions</i> – This option only appears if a start time was specified. 00:00 – 24:00 – Specifies the time of day that Auto Backup will stop for this particular day.

This chapter includes the following:

- *Limiting Access*
- *Controlling Asynchronous Terminal Access*
- *Limiting Dial-In Access via the Modem Port*
- *Controlling ISDN Access*
 - *ISDN Call Security*
 - *Disabling ISDN Access*
- *Controlling Telnet or FTP Access*
 - *Limiting Telnet Access*
 - *Limiting FTP Access*
 - *Limiting Telnet or FTP Access Over the TS Access 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 terminal
- Telnet
- FTP
- SNMP

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

Controlling Asynchronous Terminal Access

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

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

An asynchronous terminal can be connected to the unit's COM (communications) port or its modem port.

► Procedure

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

1. Select the appropriate port options.

Main Menu → Configuration → Management and Communication → Communication Port

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

NOTE:

See *Resetting the Unit and Restoring Communication* in Chapter 6, *Troubleshooting*, should you be locked out inadvertently.

3. Save your changes.

If connecting an asynchronous terminal to the unit's:

- COM port – See *Configuring the Communication Port* in Chapter 3, *Configuration*, for more information about the communication (COM) port.
- Modem port – See *Setting Up Call Directories for Trap Dial-Out* and *Configuring the Modem Port* in Chapter 3, *Configuration*, for additional information.

Limiting Dial-In Access via the Modem Port

The modem port is already configured for dial-in and asynchronous terminal access; these are the default settings.

To limit dial-in access via the modem port, disable the Dial-In Access configuration option.

Main Menu → Configuration → Management and Communication → Modem Port

See *Configuring the Modem Port* in Chapter 3, *Configuration*, for more information about modem port options.

Controlling ISDN Access

FrameSaver units with the built-in DBM limit access through the following methods:

- ISDN call security.
- Disabling ISDN access.

ISDN Call Security

The FrameSaver unit uses the Caller Identification Method to screen calls and avoid accidental or intentional disruption of network traffic. The answering DBM only accepts calls with valid calling number identifiers or phone numbers.

When the ISDN DBM interface is enabled and Caller Identification Method is set to Caller ID, the DBM takes advantage of ISDN services for network backup and Calling Number Identification Service (CNIS) to provide backup security. ISDN assures the integrity of calling party identifiers. The DBM uses the calling party identifier to identify the calling unit and switches PVC connections as specified by the user. No additional security is required.

When the ISDN DBM interface is enabled and Caller Identification Method is set to Proprietary, the DBM queries the originating unit for its Local Phone Number to identify the calling unit. If the returned number is in one of the unit's Inbound Calling IDs, the call is accepted. If not, or if the queried unit does not respond within five seconds, the unit drops the call.

See [Caller Identification Method](#) in Table 3-9, ISDN Link Profile Options, for additional information.

Disabling ISDN Access

► Procedure

To disable ISDN access:

1. Select the ISDN Physical options.
Main Menu → Configuration → ISDN → Physical
2. Set Interface Status to Disable.
3. Save your change.

See [Configuring the ISDN DBM Interface](#) in Chapter 3, *Configuration*, for more information about ISDN BRI or PRI DBM 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 Access Management Link.
- Assigning an access level for Telnet sessions.
- Disabling TS Access Management Link access.

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

► Procedure

To limit Telnet access when the session is **not on** the TS Access 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 <i>Creating a Login</i> .
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 3, *Configuration*, for more information about setting Telnet configuration options.

Limiting FTP Access

FTP access can be limited by:

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

► Procedure

To limit FTP access when the session is **not on** the TS Access 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 <i>Creating a Login</i>. If you want to allow users to configure the unit or perform file transfers, including downloads, keep the access at Level-1. Level-1 access is required to download software to the unit, or to upload or download configuration files. Level-3 is sufficient for NMS access for SLV historical information.
Limit bandwidth for FTP	FTP Max Transfer Rate to a rate less than the network line speed, typically less than or equal to the CIR. This method is not recommended if SLV reports are desired since FTP is required to generate the reports.

3. Save your changes.

See *Configuring Telnet and/or FTP Session Support* in Chapter 3, *Configuration*, for more information about setting FTP configuration options.

Limiting Telnet or FTP Access Over the TS Access Management Link

► Procedure

To limit Telnet or FTP access when the session is **on** the TS Access 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 the TS Access Management Link	TS Access Management Link to None.
Assign an access level to the TS Access Management Link	TS Access Management Link's 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 3, *Configuration*, 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 3, *Configuration*, 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 3, *Configuration*, 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 3, *Configuration*, 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 <i>n</i> IP Address to the appropriate IP address.
Specify the access allowed for an authorized NMS when IP address validates is performed	Access Level to Read or Read/Write.

3. Save your changes.

See *Configuring SNMP NMS Security* in Chapter 3, *Configuration*, for more information about SNMP NMS Security configuration options.

Creating a Login

A login is required if security is enabled. Security is enabled by the configuration options Login Required for the communication port, modem port, and Telnet Login Required or FTP Login Required for a Telnet or FTP Session.

Up to six login ID/password combinations can be created using ASCII text, and each login must have a specified access level. Logins must be unique and they are case-sensitive.

► Procedure

To create a login record:

1. Select Administer Logins.

Main Menu → Control → Administer Logins

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

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

NOTE:

See *Resetting the Unit and Restoring Communication* in Chapter 6, *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 3, *Configuration*, for more information about security configuration options.

Modifying a Login

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

Deleting a Login

► Procedure

To delete a login record:

1. Select Administer Logins.

Main Menu → Control → Administer Logins

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

3. Select Delete.

4. Save your deletion.

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

Example:

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

Operation and Maintenance

5

This chapter includes the following:

- *Displaying System Information*
- *Viewing LEDs and Control Leads*
 - *FrameSaver SLV 9126 LEDs and Control Leads*
 - *FrameSaver SLV 9128/9128-II LEDs and Control Leads*
 - *LED Descriptions*
 - *Control Lead Descriptions*
- *Device Messages*
- *Status Information*
 - *System and Test Status Message*
 - *Network LMI-Reported DLCIs Status*
 - *PVC Connection Status*
 - *Time Slot Assignment Status*
 - *DBM Interface Status*
- *IP Routing Table*
- *Performance Statistics*
 - *Clearing Performance Statistics*
 - *Service Level Verification Performance Statistics*
 - *DLCI Performance Statistics*
 - *Frame Relay Performance Statistics*
 - *ESF Line Performance Statistics*
 - *DBM Call Performance Statistics*
 - *Ethernet Performance Statistics*

- *Trap Event Log*
- *Modem Operation*
 - *Activating the Modem PassThru Feature*
 - *Canceling Modem PassThru Operation*
 - *Manually Disconnecting the Modem*
 - *Verifying Modem Operation*
- *ISDN DBM Operation*
 - *Forcing Backup (Disruptive)*
 - *Placing a Test Call (Nondisruptive)*
 - *Verifying ISDN Lines*
 - *Verifying That Backup Can Take Place*
- *FTP File Transfers*
 - *Upgrading System Software*
 - *Upgrading ISDN BRI DBM Software*
 - *Determining Whether a Download is Completed*
 - *Changing Software*
 - *Transferring Collected Data*
- *Turning Off the System Alarm Relay*

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., T1 FR NAM). This card type is supported by the SNMP SysDescr Object.
Hardware Revision	Unit's hardware version. Format <i>nnnn-nnx</i> consists of a 4-digit number, followed by two digits and one alphabetic character.
Current Software Revision	Software version currently being used by the unit. Format <i>nn.nn.nn</i> 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
Serial Number	Unit's 7-character serial number.
Ethernet MAC Address	Media Access Control (MAC) address assigned to the Ethernet port during manufacturing.

View this field . . .	To find the . . .
ISDN DBM	
Card Type	The type of dial backup module installed, ISDN-BRI or ISDN-PRI, if applicable. ■ If an unsupported DBM is installed, Unsupport displays. ■ If the DBM has failed, Failed displays.
Software Revision	Software version currently being used by the FrameSaver unit's DBM. Format <i>nn.nn.nn</i> consists of a 6-digit number that represents the major and minor revision levels. For an ISDN-PRI DBM, None displays because the DBM does not have loaded software; it runs from the NAM's software.
Hardware Revision	FrameSaver DBM's hardware version. Format <i>nnnn-nnx</i> consists of a 4-digit number, followed by 2 digits and 1 alphabetic character.

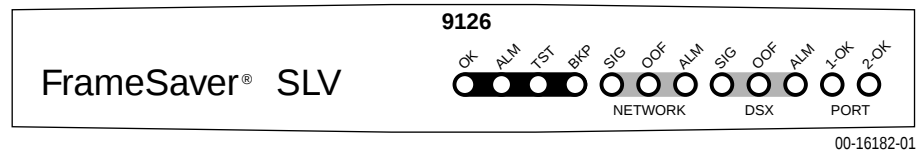
Viewing LEDs and Control Leads

FrameSaver SLV 9126 or 9128 faceplates include LEDs (light-emitting diodes) that provide status on the unit and its interfaces. These faceplates are shown in the following sections.

The Display LEDs and Control Leads feature allows you to monitor a remote unit; it is useful when troubleshooting control lead problems. The Display LEDs and Control Leads screen shows the appropriate interfaces for the unit, with the appropriate status highlighted.

FrameSaver SLV 9126 LEDs and Control Leads

The FrameSaver SLV 9126 unit's faceplate includes 12 LEDs (light-emitting diodes) that provide status on the FrameSaver unit, its network interface, DSX-1, and DTE interface.



To access the Display LEDs and Control Leads screen:

Main Menu → Status → Display LEDs and Control Leads

Display LEDs & Control Leads Screen for a FrameSaver SLV 9126

```

main/status/leds                                     9126
Device Name: Node A                                  5/26/2000 23:32

DISPLAY LEDS & Control Leads

T1 FR NAM

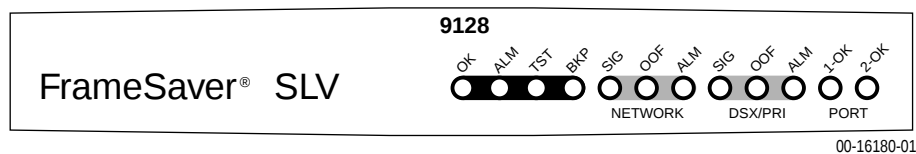
GENERAL      NETWORK 1    DSX-1    Port-1
OK           Sig         Sig      OK
Alarm       OOF         OOF      TXD
Test        Alm         Alm      RXD
Backup      LMI OK
                                DTR
                                RTS

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

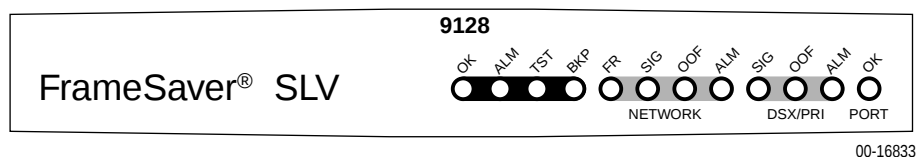
Refresh the screen to view control lead transitions. LED and control lead descriptions are in the sections that follow.

FrameSaver SLV 9128/9128-II LEDs and Control Leads

The FrameSaver SLV 9128 faceplate includes 12 LEDs (light-emitting diodes) that provide status on the FrameSaver unit, its network interface, DSX/PRI, and DTE interface. The faceplate below is for the Model 9128, without an Ethernet port.



The FrameSaver SLV 9128-II, with an Ethernet port, faceplate is shown below.

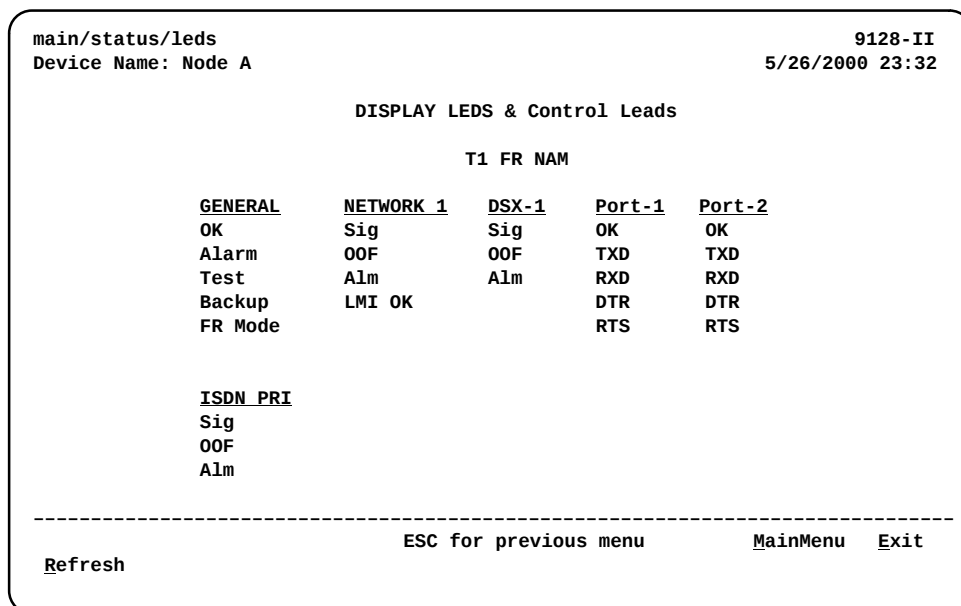


To access the Display LEDs and Control Leads screen:

Main Menu → Status → Display LEDs and Control Leads

The following example shows the screen for a FrameSaver SLV 9128-II with an ISDN PRI DBM installed. FR Mode only appears for a FrameSaver SLV 9128-II.

Display LEDs & Control Leads Screen for a FrameSaver SLV 9128-II



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

LED Descriptions

Table 5-1 identifies the alarms that cause the Alarm LED to light. See [Table 5-2](#) for network, DSX-1, or PRI interface LED and [Table 5-3](#) for user data port interface LED information.

Table 5-1. General Status LEDs (1 of 2)

Label	Indication	Color	What It Means
OK ¹	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: ■ Alarm Indication Signal (AIS) ■ CTS Down ■ DBM BRI Card Failure ■ DBM Download Failed ■ DLCI Down ■ DTR Down ■ Ethernet Link Down ■ Exceeded Error Rate (EER) ■ Internal Modem Failed ■ ISDN Network Failed ■ LMI Down ■ Loss of Signal (LOS) ■ Network Communication Link Down ■ Out of Frame (OOF) ■ Power Supply/Fan Failure ■ Primary or Secondary Clock Failed ■ Self-Test Failed ■ SLV Latency Exceeded ■ SLV Timeout ■ Suboptimal Link Rate ■ Two Level-1 Users Accessing Device ■ Yellow Alarm Signal
¹ When an ISDN BRI DBM is installed, if the OK LED comes on then goes off during power recycling, the ISDN BRI DBM may have failed.			

Table 5-1. General Status LEDs (2 of 2)

Label	Indication	Color	What It Means
ALM <i>(cont'd)</i>	Operational Alarm (Fail)	Red	ON – FrameSaver unit has just been reset, or an error or fault has been detected. Alarms appear on the System and Test Status screen. See Table 5-7, Health and Status Messages , for additional information. OFF – No failures have been detected.
TST	Test Mode	Yellow	ON – Loopback or test pattern is in progress, initiated locally, remotely, or from the network. OFF – No tests are active.
BKP	Backup	Yellow	ON – FrameSaver unit is in Backup mode; that is, the backup link has been established, and backup is in progress through the specified Alternate Destination Link. OFF – FrameSaver unit is not in Backup mode. Blinking ON and OFF – Alternate Destination Link is being established, but no data has been passed.
FR Mode ² <i>(Model 9128-II only)</i>	Frame Relay Mode	Multi-colored	Yellow – LMI is down on the FrameSaver SLV 9128-II.
			Green – LMI is up on the FrameSaver SLV 9128-II.
² On the Display LEDs & Control Leads screen for the Model 9128-II only, FR Mode is On or Off. When On (highlighted), the FrameSaver unit is in Frame Relay mode.			

Table 5-2. Network, DSX, or PRI Interface LEDs

Label	Indication	Color	What It Means
SIG	Signal	Green	ON – A recoverable signal is present on the Network/DSX/PRI interface. OFF – The signal cannot be recovered from the Network/DSX/PRI interface. An LOS condition exists.
OOF	Out of Frame	Yellow	ON – At least one OOF was detected during the sampling period. OFF – No OOFs were detected during the sampling period.
ALM	Alarm	Yellow	ON – An alarm condition is present on the network/DSX/PRI interface. Current alarm conditions: ■ Loss of Signal (LOS) ■ Loss of Frame (LOF) ■ Out of Frame (OOF) ■ Excessive Error Rate (EER) ■ Yellow Alarm Signal ■ Alarm Indication Signal (AIS) OFF – No alarm condition is present on the Network/DSX/PRI interface.

Table 5-3. User Data Port LED

Label	Indication	Color	What It Means
OK ¹	Operational Status	Green	ON – The interchange circuits for the port are in the correct state to transmit and receive data. OFF – The port is idle. Occurs if the port is disabled, or if the port is configured to monitor DTR and/or RTS and the lead(s) is not asserted.
¹ The FrameSaver SLV 9128-II only has one OK LED even though it has two user data ports. If either port is enabled and active, the LED is on. If both ports are enabled and one of the ports is inactive, the LED is off.			

Control Lead Descriptions

See Table 5-2, **Network, DSX-1, or PRI Interface LEDs**, for descriptions of these leads. See Table 5-3, **User Data Port LED**, to interpret the user data port OK control lead. The LED descriptions and control lead descriptions are the same.

In addition to these LEDs, additional control leads can be monitored through the Display LEDs and Control Leads screen. These indicators show the current state of each control lead and what they indicate when they are highlighted; that is, in the On state. They are described in Table 5-4.

Table 5-4. Additional Control Leads

Label	Indication	What It Means
Network Interface		
LMI OK	LMI Operational Status	LMI is operating successfully on the first frame relay link on the network interface.
User Data Port		
TXD	Transmit Data	Data is being sent to the far-end device.
RXD	Receive Data	Data is being received from the far-end device.
DTR	Data Terminal Ready	Shows the current state of the DTR control lead. This indicator should always be on.
RTS	Request to Send	Shows the current state of the RTS control lead. This indicator should always be on.

Device Messages

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

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

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

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

Message	What It Indicates	What To Do
DLCI Number Reserved	User tried to designate a special troubleshooting DLCI.	No action is needed.
Duplicate DLCI Number	DLCI number entered is not unique for the frame relay link.	No action needed; previous contents of the DLCI number field is restored.
File Transfer Complete (Seen at an FTP terminal.)	A file transfer was performed successfully.	Switch to the newly downloaded software. See <i>Changing Software</i> .
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 <i>Changing Software</i> .
Invalid – Already Active	A test was already in progress when it was selected.	No action needed.
Invalid Character (x)	A non-valid printable ASCII character has been entered.	Reenter information using valid characters.
Invalid date: must be mm/dd/yyyy	A non-valid date was entered on the System Information screen.	Reenter the date in the month/day/4-digit year format.
Invalid date and/or time	A non-valid date or time was entered on the System Information screen. The date does not exist (e.g., February 30th).	Reenter the date in the month/day/4-digit year format and/or time in the hour:minutes:seconds format.
Invalid – Link Already Active	Start was selected for a Test Call, but the selected frame relay link is currently in use.	Wait until the link is available and try again.
Invalid – No ISDN Channels Available	Start was selected for a Test Call, but all supported ISDN channels are currently in use.	Wait until a channel is available and try again.
Invalid – No Test Call Active	Stop was selected for a Test Call and no test call is active on the selected link. This can occur when the test is ended because the link is needed for an active connection, but the PVC Test screen has not yet been updated to Start.	Start the Test Call again when the connection is Inactive again.

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

Message	What It Indicates	What To Do
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 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.
Limit of six Login IDs reached	An attempt to enter a new login ID was made, and the limit of six login/password combinations has been reached.	■ Delete another login/password combination. ■ Reenter the new login ID.
Limit of Mgmt PVCs reached	New was selected from the PVC Connection Table and the maximum number of management PVCs has already been created.	■ Do not create the management PVC. ■ Delete another management PVC, and try again.
Limit of PVC Connections reached	New was selected from the PVC Connection Table and the maximum number of PVCs has already been created.	■ Do not create the PVC connection. ■ Delete another PVC connection, and try again.
Name Must be Unique	Name entered for a management PVC has been used previously.	Enter another 4-character name for the logical/management link.
No Destination Link DLCIs Available	New was selected from the PVC Connection Table, but even though DLCIs are available to form a connection, no DLCIs are available on the network link, which is a suitable PVC Destination.	Configure additional DLCIs for the network link and try again.
No DLCIs available for connection	New was selected from the PVC Connection Table, but all configured DLCIs have been connected.	No action needed, or configure more DLCIs and try again.

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

Message	What It Indicates	What To Do
No DLCIs available for connection	<u>N</u> ew was selected from the Management PVCs option screen, but all Link/DLCI pairs have been connected.	Configure more network and/or Port-1 Links/DLCIs pairs and try again.
No DLCIs Available for Mgmt PVC	<u>N</u> ew was selected from the Management PVCs option screen, but all configured DLCIs have been connected.	Configure more network and/or Port-1 DLCIs and try again.
No DLCIs Defined	DLCI Records was selected from an interface's Configuration Edit/Display menu, and no DLCI Records have been created for this interface.	Select <u>N</u> ew and create a DLCI record.
No more DLCIs allowed	<u>N</u> ew or <u>C</u> opyFrom was selected from an interface's DLCI Records configuration screen, and the maximum number of DLCI Records had already been reached.	Delete a DLCI, then create the new DLCI Record.
No Primary Destination Link DLCIs Available	<u>N</u> ew or <u>M</u> odify was selected from the PVC Connection Table, but even though DLCIs are available to form a connection, no DLCIs are available on the network link, which is a suitable Primary PVC Destination.	Configure additional DLCIs for the network link and try again. If a network DLCI has been entered as a Source DLCI: 1. Change the Source DLCI to a user data port DLCI. 2. Enter the network DLCI as the PVC's Primary Destination.
No Security Records to Delete	Delete was selected from the Administer Login screen, and no security records had been defined.	■ No action needed. ■ Enter a security record.
Password Matching Error – Re-enter Password	Password entered in the Re-enter Password field of the Administer Logins screen does not match what was entered in the Password field.	■ Try again. ■ Contact your system administrator to verify your password.

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

Message	What It Indicates	What To Do
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 <i>Upgrading System Software</i>.
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Port Inactive (FrameSaver SLV 9128-II only)	The port is disabled, or it supports synchronous data when a DTE Loopback was started.	No action is needed.
Resetting Device, Please Wait ...	Yes (or y) was entered in the <i>Reset COM Port usage</i> field of the System Paused menu.	No action needed.
Save Cancelled (FrameSaver SLV 9128-II only)	Changes were made on the Easy Install screen, but when it came to saving the changes, the Esc key was pressed or No was entered in response to the Save Changes? prompt.	No action is needed.
Test Active	No higher priority System and Test 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.

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

Message	What It Indicates	What To Do
User Interface Already in Use	Two Telnet sessions are already in use when an attempt to access the menu-driven user interface through the COM port is made. IP addresses and logins of the users currently accessing the interface are also provided.	■ Wait and try again. ■ Contact one of the IP address user and request that they log off.
User Interface Idle	Previously active session is now closed/ended, and access via the COM port is now available.	Log on to the FrameSaver unit.
	Session has been ended due to timeout.	No action needed.
Value Out of Range	CIR entered for the DLCI is a number greater than the maximum allowed.	Enter a valid CIR (0 – 64000).
	Excess Burst Size entered for the DLCI is a number greater than the maximum allowed.	Enter a valid Excess Burst Size (0 – 1536000).
	DLCI Number entered is less than 16 or greater than 1007.	Enter a valid number (16 – 1007).

Status Information

Status information is useful when monitoring the FrameSaver unit. The following illustration shows the Status menu for a FrameSaver SLV 9128-II with the ISDN DBM feature installed.

Status Menu Example

```
main/status                                     9128-II
Device Name: Node A                           5/26/2000 23:32

                                STATUS

                                System and Test Status
                                LMI Reported DLCIs
                                PVC Connection Status
                                Timeslot Assignment Status
                                DBM Interface Status
                                IP Routing Table
                                Performance Statistics
                                Trap Event Log
                                Display LEDs and Control Leads
                                Identity

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

DBM Interface Status will not appear on the menu if the unit does not have the optional ISDN DBM feature.

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 (see Table 5-6)
- Last System Reset Date and Time
- **Health and Status Messages** (see Table 5-7)
- **Test Status Messages** (see Table 5-8)

Self-Test Results Messages

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

Table 5-6. Self-Test Results Messages

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

Last System Reset Date and Time

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

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

Health and Status Messages

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

Table 5-7. Health and Status Messages (1 of 7)

Message	What It Indicates
AIS at DSX-1	An Alarm Indication Signal (AIS) is received by the DSX-1 interface. AIS is an unframed, all ones signal.
AIS at ISDN PRI (Active/Idle) (ISDN PRI DBM only)	An Alarm Indication Signal (AIS) is received by the ISDN PRI interface. AIS is an unframed, all ones signal. Only appears when a PRI dial backup module (DBM) is installed. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. The ISDN network is transmitting an AIS.
AIS at Network 1	An Alarm Indication Signal (AIS) is received by the network interface. AIS is an unframed, all ones signal. Possible reasons include: ■ Upstream FrameSaver unit is transmitting AIS (keep-alive signal). ■ The network is transmitting an AIS.
Auto-Configuration Active	Auto-Configuration feature is active, which allows automatic configuration and cross-connection of DLCIs as they are reported by the network LMI.
Back-to-Back Mode Active	The operating mode has been configured for back-to-back operation (<i>Main Menu → Control → Change Operating Mode</i>). 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	Backup has been established and data is flowing over the alternate DLCI.
CTS down to Port-1 Device	The user data port CTS control lead on the FrameSaver unit is off.
DBM BRI Card Failed (ISDN BRI DBM only)	One or more of the access unit's integrated circuit chips has failed to internally loop data through the dial backup unit BRI circuit.

Table 5-7. Health and Status Messages (2 of 7)

Message	What It Indicates
DBM Download Required (<i>ISDN BRI DBM only</i>)	A download attempt was interrupted and failed to complete. The NAM software and DBM software are incompatible.
DCLB Active, [<i>Interface</i>]	A V.54 Loopback is active on the specified interface.
DLCI <i>nnnn</i> Down, <i>frame relay link</i> ^{1,2}	The DLCI for the specified frame relay link is down.
DTE External LB Active, Port- <i>n</i>	A Data Terminal Loopback is running on the specified user data port.
DTE Init. Ext LB Active, Port- <i>n</i>	The DTE has initiated an external DTE Loopback on the specified user data port.
DTPLB Active, Port-2	A Data Terminal Payload Loopback (DTPLB) is active on the synchronous user data port.
DTR Down from Port-1 Device	The DTR control lead from the device connected to the user data port is deasserted.
EER at ISDN PRI (Active/Idle) (<i>ISDN PRI DBM only</i>)	The error rate of the received ISDN network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing and a PRI dial backup module (DBM) is installed. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.
EER at Network 1	The error rate of the received network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.
Ethernet Link Down (<i>FrameSaver SLV 9128-II only</i>)	The Ethernet port is enabled, but communication between the management system and the unit is not currently possible on the port.
Internal Modem Failed	The unit's internal modem failed to pass the self-test.
¹ <i>nnnn</i> indicates a DLCI number of 16 through 1007. ² <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i>. The frame relay link associated with the user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface.	

Table 5-7. Health and Status Messages (3 of 7)

Message	What It Indicates
ISDN Active	An ISDN call is active.
ISDN Link Profile Disabled <i>ISDN Link Name</i>	An ISDN backup call could not be made because the ISDN link profile specified Link Name is disabled (<i>Main Menu</i> → <i>Configuration</i> → <i>ISDN</i> → <i>Link Profiles</i>).
ISDN Link Profile Invalid, <i>ISDN Link Name</i>	No phone numbers have been specified in the ISDN link profile (specified by <i>ISDN Link Name</i>).
ISDN Network Failed (Active/Idle)	An ISDN network failure was detected when: ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode.
Link Down Administratively, <i>frame relay link</i> 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.
Link Profile Disabled, <i>ISDN Link Name</i>	An ISDN backup call could not be made because the specified link profile was disabled.
LLB Active, [<i>Interface</i>]	A network Line Loopback (LLB) is active on the specified interface.
LMI Discovery in Progress, <i>frame relay link</i> ²	Local Management Interface protocol discovery is in progress to determine which protocol will be used on the specified frame relay link.
LMI Down, <i>frame relay link</i> ²	The Local Management Interface(s) has been declared down for the specified frame relay link. ■ For an individual ISDN link, the message appears when LMI has been declared down on the link. ■ For a multilink aggregate link, the message appears when LMI has been declared down on all constituent links of the frame relay multilink.
LOS at DSX-1	A Loss of Signal (LOS) condition is detected on the DSX-1 interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. Possible reasons include: ■ DSX-1 cable problem. ■ No signal being transmitted from the DTE.
² <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i>. The frame relay link associated with the user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface.	

Table 5-7. Health and Status Messages (4 of 7)

Message	What It Indicates
LOS at ISDN PRI (Active/Idle) (ISDN PRI DBM only)	A Loss of Signal (LOS) condition is detected on the ISDN PRI interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. Only appears when a dial backup module (DBM) is installed. Possible reasons include: ■ DBM cable problem. ■ T1 facility problem.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. Possible reasons include: ■ Network cable problem. ■ No signal is being transmitted at the far-end FrameSaver unit. ■ T1 facility problem.
Monitor Ptn. Active, DLCI <i>nnnn</i> , <i>frame_relay_link</i> ^{1,2}	The unit is monitoring a test pattern on the specified DLCI on the specified frame relay link.
Monitor <i>Ptn</i> Active, [<i>Interface</i>]	A Monitor Pattern test is active on the specified interface using a selected pattern. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
Network Com Link Down	The communication link for the COM port is down, and the COM port is configured for Net Link.
Network Initiated ISDN BRI Test Active (ISDN BRI DBM only)	An ISDN test has been initiated by the ISDN BRI network and it is currently active.
OOF at DSX-1	An Out of Frame (OOF) condition is detected on the DSX-1 interface. Possible reasons include: ■ Incompatible framing format between the DTE and the FrameSaver unit. ■ DSX-1 cabling problem.
¹ <i>nnnn</i> indicates a DLCI number of 16 through 1007. ² <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i>. The frame relay link associated with the user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface.	

Table 5-7. Health and Status Messages (5 of 7)

Message	What It Indicates
OOF at ISDN PRI (Active/Idle) (<i>ISDN PRI DBM only</i>)	An Out of Frame (OOF) condition is detected on the ISDN PRI interface. An OOF is declared when two out of four frame synchronization bits are in error. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. Possible reasons include: ■ Incompatible framing format between the ISDN network and the FrameSaver unit. ■ ISDN network cabling problem. ■ ISDN network problem.
OOF at Network 1	An Out of Frame (OOF) condition is detected on the network interface. Possible reasons include: ■ Incompatible framing format between the network and the FrameSaver unit. ■ Network cabling problem. ■ T1 facility problem.
PLB Active, [<i>Interface</i>]	A Payload Loopback (PLB) is active on the specified interface.
Power Supply/Fan Alarm (<i>9000 Series Access Carrier only</i>)	The power supply output voltage has dropped below the specified tolerance level required for the system. Or the fan tray is not operating properly.
Primary Clock Failed	A failure of the primary clock source configured for the unit is detected and the secondary clock is providing the timing for the unit. This condition clears when the configured primary clock is restored.
Primary & Secondary Clocks Failed	A failure of the primary and secondary clock sources configured for the unit are detected and the internal clock is providing timing for the unit. The clock source will not automatically switch from internal until the primary clock source returns.
PVC Loopback Active, DLCI <i>nnnn</i> , <i>frame_relay_link</i> ^{1,2}	A PVC Loopback is active on the specified DLCI on the frame relay link.
RLB Active, [<i>Interface</i>]	A network Repeater Loopback (RLB) is active on the specified interface.
¹ <i>nnnn</i> indicates a DLCI number of 16 through 1007. ² <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i>. The frame relay link associated with the user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface.	

Table 5-7. Health and Status Messages (6 of 7)

Message	What It Indicates
Secondary Clock Failed	A failure of the secondary clock source configured for the unit is detected and the internal clock is providing the timing for the unit. The clock source will not automatically switch from internal until the primary clock source returns.
Send Pattern Active, DLCI <i>nnnn</i> , <i>frame_relay_link</i> ^{1,2}	A Send Pattern test is currently active on the specified DLCI on the specified frame relay link.
Send <i>Pttn</i> Active, [<i>Interface</i>]	A Send Pattern test is active on the specified interface using a selected test pattern. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
SLV Latency Exceeded, DLCI <i>nnnn</i> , <i>frame relay link</i> ^{1,2,3}	The measured latency of SLV communication responses from the remote unit on this DLCI is excessive, so the DLCI has been declared unsuitable for normal multiplexed PVC operation (DLCI Type is set to Multiplexed).
SLV Timeout, DLCI <i>nnnn</i> , <i>frame relay link</i> ^{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. When an ISDN DBM is present, this message only appears for individual and aggregate multilink frame relay links, not constituent links of a frame relay multilink.
Suboptimal Link Rate, <i>frame relay link</i> ² (<i>ISDN DBM only</i>)	The specified frame relay multilink has failed to achieve the configured Maximum Link Rate for the link. This message appears for multilink aggregate frame relay links if LMI is down on any of its constituent links.
¹ <i>nnnn</i> indicates a DLCI number of 16 through 1007. ² <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i>. The frame relay link associated with the user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface. ³ Does not apply to a TS Management Link DLCI.	

Table 5-7. Health and Status Messages (7 of 7)

Message	What It Indicates
Timeslot Discovery in Progress, Network 1	Time slot discovery is currently taking place to determine the time slots that will be used for frame relay traffic on the network interface. This message only appears when the Time Slot Discovery option is enabled (<i>Main Menu → Configuration → Time Slot Assignment → Frame Relay Network Assignments</i>) and an LMI failure is detected on the network interface's frame relay link.
Two Level-1 Users Accessing Device	Two Level 1 users are already using the menu-driven user interface; only two sessions can be active at one time.
Test Call Active, <i>ISDN Link Name</i>	A test call is active on the specified frame relay link, the link being the ISDN Link Name assigned in the ISDN Link Profile. This message would only appear for models with the built-in DBM.
Yellow at DSX-1	A yellow alarm signal is received on the DSX-1 interface. DTE has detected a LOS or OOF condition.
Yellow at ISDN PRI (Active/Idle) (<i>ISDN PRI DBM only</i>)	A yellow alarm signal is received on the ISDN network interface. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. Indicates a possible cable problem.
Yellow at Network 1	A yellow alarm signal is received on the network interface. Possible reasons include: ■ Network cable problem. ■ T1 facility problem.

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 6, *Troubleshooting*, for more information on tests, including how to start and stop them.

Table 5-8. Test Status Messages (1 of 2)

Message	What It Indicates
DCLB Active, <i>frame_relay_link</i> ¹ or DCLB Active, Port-2	A Data Channel V.54 Loopback (DCLB) is active on the specified frame relay link, or Port-2.
DTE External LB Active, Port- <i>n</i>	An external DTE Loopback is active on the user data port.
DTE Init. Ext LB Active, Port- <i>n</i>	An external DTE Loopback is active on the user data port.
DTPLB Active, Port- <i>n</i>	A Data Terminal Payload Loopback (DTPLB) is active on the user data port.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the faceplate to flash on and off.
LLB Active, <i>Interface</i> ²	A network Line Loopback (LLB) is active on the specified network, DSX-1, or ISDN PRI interface.
No Test Active	No tests are currently running.
PLB Active, <i>Interface</i> ²	A Payload Loopback (PLB) is active on the specified network, DSX-1, or ISDN PRI interface.
PVC Loopback Active, DLCI <i>nnnn</i> , <i>frame_relay_link</i> ^{1,3}	A PVC Loopback is active on the specified DLCI for the frame relay link.
RLB Active, <i>Interface</i> ²	A network Repeater Loopback (RLB) is active on the specified network or DSX-1 interface.
¹ <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i> for a 1-slot unit, or SsPort-<i>n</i> for a NAM in a multislot housing (the frame relay link associated with the specified user data port in the specified slot). – <i>ISDN Link Name</i> on a non-network ISDN DBM interface. ² <i>Interface</i> is one of the following: – Network 1 – DSX-1 – Port-<i>n</i> – ISDN, BRI or PRI ³ <i>nnnn</i> indicates a DLCI number of 16 through 1007.	

Table 5-8. Test Status Messages (2 of 2)

Message	What It Indicates
Send <i>Pttn</i> Active, <i>Interface</i> ²	A Send Pattern test is active on the specified interface. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
Monitor <i>Pttn</i> Active, <i>Interface</i> ²	A Monitor Pattern test is active on the specified interface. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
Network Initiated ISDN BRI Test Active	An ISDN test has been started by the ISDN BRI network and it is currently active.
Send <i>Pttn</i> Active, DLCI <i>nnnn</i> , <i>frame_relay_link</i> ^{1,3}	A selected Send Pattern test is active on the specified DLCI for the specified frame relay link.
Monitor <i>Pttn</i> Active, DLCI <i>nnnn</i> , <i>frame_relay_link</i> ^{1,3}	A selected Monitor Pattern test is active on the specified DLCI for the specified frame relay link.
Test Call Active, <i>ISDN Link Name</i>	A test call is active on the specified frame relay link, the link being the ISDN Link Name assigned in the ISDN Link Profile. This message would only appear for units with the ISDN DBM feature.
¹ <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i> for a 1-slot unit, or SsPort-<i>n</i> for a NAM in a multislot housing (the frame relay link associated with the specified user data port in the specified slot). – <i>ISDN Link Name</i> on a non-network ISDN DBM interface. ² <i>Interface</i> is one of the following: – Network 1 – DSX-1 – Port-<i>n</i> – ISDN, BRI or PRI ³ <i>nnnn</i> indicates a DLCI number of 16 through 1007.	

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			9128-II		
Device Name: Node A			5/26/2000 23:32		
<u>frame relay link</u> 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.					
Refresh PgUp PgDn			ESC for previous menu NextLink PrevLink		
			MainMenu Exit		

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 5-9. 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)	0–1536000	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

The PVC Connection Status screen shows all PVC connections and management links configured for the unit. The source and primary destination are shown, along with an alternate destination for backup. When a primary destination DLCI was assigned to a Backup Group, the Backup Group designation appears next to the DLCI number. In the example below, DLCIs 502 and 504 had been assigned to Backup Group A.

PVC Connection Status Screen Example

main/status/connections										9128-II	
Device Name: Node A										5/26/2000 23:32	
Page 1 of 2											
PVC CONNECTION STATUS											
Source			Primary Destination			Status	Alternate Destination				
Link	DLCI	EDLCI	Link	DLCI	EDLCI		Link	DLCI	EDLCI	Status	
Port-1	201		Net1-FR1	300		Active					
Port-2	202		Net1-FR1	1001	1	Active					
Port-1	100		Net1-FR1	1001	4	Active					
Port-2	204		Net1-FR1	1001	2	Active					
Mgmt PVC	Tampa		Net1-FR1	1001	5	Active					
Port-2	206		Net1-FR1	1001	3	Active					
Port-1	207		Net1-FR1	1001		Active					
Port-1	208		Net1-FR1	502A		Active	Colorado	400		Inactive	
Port-1	209		Net1-FR1	504A		Inactive	Colorado	302		Active	
Port-1	210		Net1-FR1	505		Inactive	Tampa	304		Active	
Port-1	214		Net1-FR1	506		Active					

ESC for previous menu						MainMenu		Exit			
Refresh	PgUp	PgDn									

For units with ISDN backup capability, the DBM provides backup support through the unit's ISDN DBM interface. For units without ISDN backup capability, an alternate network DLCI can be used to backup user data. For additional information about the Alternate Destination fields, see *Configuring PVC Connections* in Chapter 3, *Configuration*.

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

Table 5-10. PVC Connection Status (1 of 2)

Field	Status	What It Indicates
Link	Net1-FR1 Port-1, or Port-2 Mgmt <i>PVCName</i>	Identifies the cross-connection of DLCIs configured for the unit. ■ Source/destination is frame relay link 1 on Network 1 ■ User data port – Port-1, or Port-2 if a FrameSaver SLV 9128/9128-II ■ Virtual circuit is a management link that terminates in the unit, where <i>Name</i> is the link name
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.

Table 5-10. PVC Connection Status (2 of 2)

Field	Status	What It Indicates
Status	Active ¹ Inactive Disabled Invalid	Identifies whether the physical interfaces, LMIs, and DLCIs are all enabled and active for this PVC connection. ■ The PVC is currently active. ■ 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. ■ 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. ■ 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.		

Time Slot Assignment Status

Time slot assignments are made using the Time Slot Assignment configuration option. See *Assigning Time Slots/Cross Connections* in Chapter 3, *Configuration*, for making time slot assignments. Use the Timeslot Assignment Status screen to display time slot assignments for the network channels and the DSX-1 channels.

Displaying Network Time Slot Assignments

Use the Network Timeslot Assignment Status screen to display DS0 assignments for each DS0 on the network interface.

Main Menu → Status → Timeslot Assignment Status → Network

The Network Timeslot Assignment Status screen displays 24 two-field entries in three rows. Together, each two-field entry defines the assignment for one network interface time slot. The top field represents the timeslot of the network interface. The bottom field represents the cross-connect status of the associated (top field) network time slot.

Network Timeslot Assignment Status Screen Example

main/status/timeslot/net_display							9128-II
Device Name: Node A							5/26/2000 23:32
NETWORK 1 TIMESLOT ASSIGNMENT STATUS							
N01	N02	N03	N04	N05	N06	N07	N08
D5-1/01r	D5-1/02r	D5-1/03r	S1P01	S1P01	S1P01	S1P01	S1P01
N09	N10	N11	N12	N13	N14	N15	N16
FrameRly1	FrameRly1	FrameRly1	FrameRly1	FrameRly1	FrameRly1	FrameRly1	FrameRly1
N17	N118	N19	N20	N21	N22	N23	N24
Unassign	Unassign	Unassign	Unassign	Unassign	Unassign	Unassign	Unassign
Slot 1 - T1 FR NAM							

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

The following information is available for network interface time slots (N01– N24).

The Cross Connect Status Field (bottom) . . .	Indicates . . .
Unassgn	The time slot is unassigned.
FrameRly1	The time slot is assigned to the network frame relay link.
Port-2	The synchronous data port (Port-2) is assigned to the network interface time slot (01 to 24).
Ds-pltt	The DSX-1 time slot <i>tt</i> is assigned to the network interface time slot (01 to 24).
Ds-pltr	The DSX-1 time slot <i>tt</i> is assigned to the network interface time slot (01 to 24), using Robbed Bit Signaling (r).

Displaying DSX-1 Time Slot Assignments

Use the DSX-1 Timeslot Assignments Status screen to display all of the DS0 assignments for each DS0 on the DSX-1 interface.

Main Menu → Status → Timeslot Assignment Status → DSX-1

The DSX-1 Timeslot Assignment Status screen displays 24 two-field entries in three rows. Together, each two-field entry defines the assignment for one DSX-1 interface time slot. The top field represents the time slot of the DSX-1 Interface. The bottom field represents the cross-connect status of the associated (top field) DSX-1 time slot.

DSX-1 Timeslot Assignment Status Screen Example

main/status/timeslot/dsx_display							9128-II
Device Name: Node A							5/26/2000 23:32
DSX-1 TIMESLOT ASSIGNMENT STATUS							
D01	D02	D03	D04	D05	D06	D07	D08
D05-1/01r	D05-1/02r	D05-1/03r	S1P01	S1P01	S1P01	S1P01	S1P01
D09	D10	D11	D12	D13	D14	D15	D16
FrameRly1	FrameRly1	FrameRly1	FrameRly1	FrameRly1	FrameRly1	FrameRly1	FrameRly1
D17	D118	D19	D20	D21	D22	D23	D24
Unassign	Unassign	Unassign	Unassign	Unassign	Unassign	Unassign	Unassign
Slot 1 - T1 FR NAM							

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

The following information is available for DSX-1 interface time slots (D01– D24):

The Cross Connect Status Field (bottom) . . .	Indicates the . . .
blank	The time slot is unassigned.
Net1/ <i>tt</i>	Network interface 1, time slot (<i>tt</i>) is assigned to DSX-1 time slot (01 to 24) using Clear Channel.
Net1/ <i>ttr</i>	Network interface 1, time slot (<i>tt</i>) is assigned to DSX-1 time slot (01 to 24) using Robbed Bit Signaling (<i>r</i>).

DBM Interface Status

When an ISDN DBM is installed, these interface statuses appear when DBM Interface Status is selected from the Status menu.

Main Menu → Status → DBM Interface Status

DBM Interface Status Screen Example

```

main/status/dbm                                     9128-II
Device Name: Node A                                5/26/2000 23:32

                                DBM INTERFACE STATUS

Line Status:                Call Rejected - HQ_Site: Disabled

Link:                        Colorado
Multilink Constituent Link: Colorado-1
Link Operating Mode:        Active
Call Status:                Connected
Most Recent Cause Value:    Call Awarded and Being Delivered In Est Chnl-7
Previous Cause Value 1:     None
                             2:     None
                             3:     None
                             4:     None
Maximum Link Rate (Kbps):   64K      (Configured)
Negotiated Rate (Kbps):     64K
ISDN Channel:               B1
Remote Call ID:             8135302000

-----
Ctrl-a to access these functions, ESC for previous menu      MainMenu  Exit
Refresh                                                    NextLink  PrevLink  ConstLinkStatus

```

Select the NextLink and PrevLink function keys to move forward or backward through the frame relay links that can be selected. If the selected frame relay link is a multilink aggregate link, select the ConstLinkStatus function key to see the status for selected constituent links.

For a multilink aggregate link, Multilink Constituent Link appears under Link so a specific constituent link can be selected. Otherwise, the line is blank. In addition, the Most Recent Cause Value, Previous Cause Values, and Remote Call ID do not appear for a multilink aggregate frame relay link.

Table 5-11. DBM Interface Status (1 of 3)

Field	Status	What It Indicates
Line Status	Active	The overall status of the ISDN line. ■ The ISDN line is active and no error conditions exist.
	Disabled	■ The ISDN interface has been disabled. <i>Main Menu → Configuration → ISDN → Physical</i>
	Inactive	■ The ISDN line is disconnected or an ISDN network alarm condition exists.
	Invalid SPID	■ The switch has rejected one of the configured SPIDs (<i>ISDN BRI DBM only</i>).
	Invalid Local Number	■ The phone number configured for a B-channel is an invalid local number.
	Call Rejected – Invalid ID: <i>Caller ID</i>	■ The incoming call was rejected because the Caller ID or local phone number received from the switch did not match any configured Link Profiles. If provided by the switch, the rejected Caller ID is displayed after the status. Otherwise, Invalid Call ID is displayed.
	Call Rejected – No Far-End ID	■ The incoming call was rejected because no Caller ID was received from the switch (COM port's Port Use option is set to Caller ID). ■ No local phone number was received from the far-end device during the call validation process (COM port's Port Use option is set to Proprietary).
	Call Rejected – <i>ISDN Link Name: Busy</i>	■ The incoming call was rejected because the enabled ISDN Link Name associated with the incoming Caller1 ID or local phone number was busy. The ISDN Link Name associated with the incoming call is displayed.

Table 5-11. DBM Interface Status (2 of 3)

Field	Status	What It Indicates
Line Status <i>(cont'd)</i>	Call Rejected – <i>ISDN Link Name: Disabled</i>	The incoming call was rejected because the enabled ISDN Link Name associated with the incoming Caller1 ID or local phone number was disabled. The ISDN Link Name associated with the incoming call is displayed.
Link	<i>ISDN Link Name</i>	The selected ISDN backup link for which status will be displayed.
Multilink Constituent Link ¹	<i>ISDN Link Name</i>	The selected multilink constituent link for which status will be displayed.
Link Operating Mode	Disabled ² Idle ² Active	The status of the ISDN DBM. - The ISDN Link Profile is disabled. - An ISDN link is not currently needed, so there is no ISDN connection. - The ISDN link is required for frame relay traffic and needs an active ISDN connection.
Call Status	Not Connected – Invalid Link Profile Not Connected Connected Connected – Incoming Call ¹	The overall status of the ISDN frame relay link. - No calls are currently connected on the selected link because the ISDN Link Profile is incomplete. - No calls are currently connected on the selected link. - At least one call is actively connected and available for data transfer on the selected ISDN frame relay link (when the Most Recent Cause Value is Call Awarded and Being Delivered In Est Chnl-7). - An incoming call has been answered and is actively connected and available for data transfer on the selected multilink constituent link (when the Most Recent Cause Value is Call Awarded and Being Delivered In Est Chnl-7).
¹ Only appears for a constituent frame relay link. ² If Link Operating Mode is Disabled or Idle, the Remote Call ID, ISDN Channel, and Negotiated Rate fields will not appear.		

Table 5-11. DBM Interface Status (3 of 3)

Field	Status	What It Indicates
Call Status <i>(cont'd)</i>	Connected – Outbound Call ¹	An outbound call has been placed and is actively connected and available for data transfer on the selected multilink constituent link (when the Most Recent Cause Value is Call Awarded and Being Delivered In Est Chnl-7).
Most Recent Cause Value ³	Various ITU cause messages	Refer to Table 5-12, Most Recent and Previous Cause Value Messages , for additional information.
Previous Cause Values ³		
Maximum Link Rate (Kbps)	BRI DBM: 64K, 128K PRI DBM: 64K, 128K, . . . 1472	The maximum link rate that was configured for the selected link. This is the maximum rate the link will attempt to achieve when activated.
Negotiated Rate (Kbps)	64K per B-channel 56K per B-channel	The negotiated rate of the connection/link. For a multilink aggregate frame relay link, the negotiated rate will be the sum of the negotiated rates on all connected constituent links.
ISDN Channel	BRI DBM: B1, B2 PRI DBM: B1, B2, . . . B23	The ISDN B-channel being used for the call on this link.
Remote Call ID ³	None	Backup has never been active on the link.
	Remote device's ID	Remote call origination – Last Calling ID of the remote backup device received for the B-channel. If the remote device initiated the call, this is the Inbound Call ID. If this device originated the call, this is the Outbound Phone Number.
¹ Only appears for a constituent frame relay link. ³ Appears for frame relay links with only one constituent and for all constituent frame relay links.		

Most Recent and Previous Cause Value Messages

The following Cause Value Messages are presented in alphabetical order. The Cause Number is also provided if you need to convert the message to its corresponding ITU number for your service provider.

Table 5-12. Most Recent and Previous Cause Value Messages (1 of 6)

Message	Cause No.	What It Indicates	What To Do
Bearer Capability Not Authorized	57	User has requested a bearer capability that the user is not authorized to use.	Arrange for the desired capability.
Bearer Capability not Implemented	65	Device sending this cause does not support the bearer capability (i.e., channel type) requested.	Arrange for the desired capability.
Bearer Capability Presently Not Available	58	Bearer capability requested is supported by the device generating the cause, but it is not available at this time.	Arrange for the desired capability.
Call Awarded and Being Delivered in Est Chnl-7	7	An incoming call is being connected to an already established channel that is used for similar calls.	No action is needed.
Call Rejected	21	Equipment sending the cause does not want to receive the call at this time.	No action is needed.
Call Terminated by Remote End	130	Remote DBM rejected or terminated the call.	1. Retry the call. 2. Verify that the remote DBM's link profile is correct.
Call With Requested Call ID Has Been Cleared	86	Network has received a call resume request, but the call had been cleared after it was suspended.	No action is needed.
Channel Type Not Implemented	66	Device sending this cause does not support the requested channel type.	Arrange for the desired capability.
Channel Unacceptable	6	Channel identified for the call is not acceptable to the receiving device.	Arrange for the desired capability.

Table 5-12. Most Recent and Previous Cause Value Messages (2 of 6)

Message	Cause No.	What It Indicates	What To Do
Destination Out of Order	27	Destination interface specified is not functioning correctly so the signalling message could not be delivered (e.g., physical or data-link layer failure at the remote end, user equipment is offline).	Verify that the remote DBM's link profile is correct.
Facility Rejected	29	Requested facility is not provided by the network.	No action is needed.
Incoming Calls Barred	54	Called user is not permitted to accept the call.	Turn off network call screening.
Incompatible Destination	88	Request to establish a call has been received, but low-layer, high-layer, or another compatibility attribute (e.g., data rate) cannot be provided. Incorrect format of the destination link.	Arrange for the desired capability.
Identified Channel Does Not Exist	82	Channel requested for a call is not activated on the interface.	Make sure the network is configured for 2B service, if a BRI DBM. Contact your service provider to verify that your service is provisioned for two B-channels.
Info Element Nonexistent or Nonimplemented	99	Device sending this cause has received a message it does not recognize. This cause will not prevent the message from being precessed.	1. Verify that the Inbound Calling ID has been defined. 2. Verify that the Inbound Calling ID is part of your service.
Interworking, Unspecified	127	Precise cause of a message cannot be determined because the interworking network does not provide causes.	No action is needed.
Invalid Call Reference Value	81	Call reference used is not currently in use on the user-network interface.	Contact your service representative.

Table 5-12. Most Recent and Previous Cause Value Messages (3 of 6)

Message	Cause No.	What It Indicates	What To Do
Invalid Info Element Contents	100	Device sending this cause has received and implemented an information element, but one or more fields in the element cannot be processed.	Contact your service representative.
Invalid Message, Unspecified	95	No other cause in the invalid message class applies for this invalid message event.	Contact your service representative.
Invalid Number Format – Incomplete Address	28	Call cannot be completed because the phone number is incorrect or incomplete.	Check your ISDN link profile, and correct the number.
Invalid Transit Network Selection	91	Incorrect format of transit network identification.	Contact your service representative.
Mandatory Information Element Missing	96	Required data is missing from a mandatory information element.	Contact your service representative.
Message Not Compatible with Call State	101	Device sending this cause has received a message that is not permissible while in the call state.	Contact your service representative.
Msg Nonexistent	98	An unexpected message was received in a state other than Null.	Retry the call.
Msg Type Nonexistent or Unimplemented	97	Device sending this cause has received a nonexistent or not implemented message type while in the call state. Device sending this cause has received a status message that indicates an incompatible call state.	Contact your service representative.
Network Out of Order	38	Network is not functioning correctly, and the condition is expected to continue.	Contact your service representative.
No Call Suspended	85	A call resume has been issued, but no calls have been suspended.	No action is needed.

Table 5-12. Most Recent and Previous Cause Value Messages (4 of 6)

Message	Cause No.	What It Indicates	What To Do
No Circuit/Channel Available	34	No circuit/channel is currently available to handle the call.	Wait and try again.
No Destination Route	3	Network through which call has been routed does not serve the destination area or device.	Contact your service representative.
None	—	No causes have been generated.	No action is needed.
Non-selected User Clearing	26	User has not been awarded the incoming call.	No action is needed.
No Route to Specify Transit Network	2	The device sending or receiving this cause does not recognize the transit network that the call is being/has been routed through.	1. Verify that the network exists. 2. Verify that the network serves the device sending the cause.
Normal Call Clearing	16	Call is being cleared because either the caller or receiver has requested that it be cleared.	No action is needed.
Normal, Unspecified	31	Remote user has sent a release message to the network. No other cause in the normal class applies for this normal event.	No action is needed.
No User Responding	18	Called device does not respond to the call with an alert or connect indication within the prescribed period of time. Internal network timers may be a cause.	Contact the network provider if the cause continues.
Number Changed	22	Called number is no longer assigned.	Look in the diagnostic field for the new number, then change the phone number in your ISDN link profile.

Table 5-12. Most Recent and Previous Cause Value Messages (5 of 6)

Message	Cause No.	What It Indicates	What To Do
Only Restricted Bearer Capability Available	70	An unrestricted bearer service has been requested, but the device sending the cause only supports the restricted version.	Arrange for the desired capability.
Outgoing Calls Barred	52	Network is using Call Screening.	Contact the network provider to turn Call Screening off.
Pre-empted	45	Call has been pre-empted.	Contact the network provider.
Protocol Error, Unspecified	111	No other cause in the protocol error class applies for this protocol error event.	Contact your service representative.
Quality of Service Unavailable	49	Requested Quality of Service requested cannot be provided (e.g., throughput cannot be supported).	No action is needed.
Recovery of Timer Expired	102	Error-handling procedure has been initiated as a result of the expiration of a timer.	Retry the call.
Requested Channel Not Available	44	Circuit or channel requested cannot be provided by the other side of the interface.	Allow the DBM to automatically call using the alternate link if Auto Backup is enabled, or manually select an alternate path for the call.
Requested Facility Not Implemented	69	Supplemental service requested is not supported by this device.	No action is needed.
Requested Facility Not Subscribed	50	The supplementary service requested cannot be provided by the network until user completes arrangement with its supporting networks.	Arrange for the desired capability.
Resource Unavailable, Unspecified	47	No other cause in the resource unavailable class applies for this resource unavailable event.	No action is needed.

Table 5-12. Most Recent and Previous Cause Value Messages (6 of 6)

Message	Cause No.	What It Indicates	What To Do
Response to STATus ENquiry	30	Status enquiry message received, generating this message.	No action is needed.
Service/Option Not Implemented	79	No other cause in the service or option not available class applies for this not implemented event.	No action is needed.
Service/Option Unavailable, Unspecified	63	No other cause in the service or option not available class applies for this not available event.	Wait and try again.
Switching Equipment Congestion	42	Switching equipment sending the cause is experiencing heavy traffic.	Wait and try again.
Suspended Call Exists, But Not Call ID	83	A call resume has been attempted, but no suspended call exists for this phone number.	1. Verify the number in the Inbound Calling ID # field for the suspended call. 2. Reissue the Call Resume command using the correct number.
Temporary Failure	41	Network is not functioning correctly, but the condition is not expected to continue for long.	Wait and try again.
Unallocated Number	1	Destination requested cannot be reached because the Inbound Calling ID number is not assigned or allocated.	Assign the Inbound Calling ID.
User Access Information Discarded	43	Network was unable to deliver the access information when trying to establish the call.	No action is needed.
User Alerting, No Answer	19	During call establishment, an alerting was received but a connection was not.	1. Verify that the remote device is operational and configured to answer. 2. Retry the call.
User Busy	17	Called number cannot receive the call.	Wait and try again.

IP Routing Table

The IP Routing Table shows all the routes configured in the FrameSaver unit.

Main Menu → Status → IP Routing Table

IP Routing Table Screen Example

main/status/ip_route						9128-II
Device Name: Node A						5/26/2000 23:32
						Page 1 of 2
IP ROUTING TABLE						
Destination	Mask	Gateway	Hop	Type	Interface	TTL
135.001.001.000	255.255.255.000	135.026.001.254	1	Tmp	PVCMgmt1001	130
135.001.002.111	FFF.FFF.FFF.FFF	135.026.001.254	1	NMS	PVCMgmt1002	130
135.001.220.000	255.255.255.000	135.042.001.254	1	Loc	Ethernet	999
135.001.221.000	255.255.255.000	135.042.001.254	1	Loc	Modem	999
135.001.220.000	255.255.255.000	135.042.001.254	1	Loc	COM	999
135.001.222.111	255.255.255.000	135.026.001.254	1	RIP	Modem	30
135.001.222.113	255.255.255.255	135.026.001.254	1	RIP	PVCMgmt1003	30
135.001.002.111	255.255.255.255	135.026.001.254	1	NMS	PVCMgmt1004	2
135.001.002.111	255.255.255.255	135.026.001.254	1	NMS	PVCMgmt1005	48
135.001.002.111	255.255.255.255	135.026.001.254	1	NMS	PVCMgmt1006	21

ESC for previous menu						MainMenu Exit
Refresh	PgDn	PgUp				

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

Table 5-13. IP Routing Table Values (1 of 2)

Column	What It Indicates
Destination	The Destination IP Address for the route: 001.000.000.000 – 223.255.255.255
Mask	The Destination Subnet Mask for the route: 000.000.000.000 – 255.255.255.255 for network routes - FFF.FFF.FFF.FFF for host routes 127 may appear as well. It is a reserved number.
Gateway	The Gateway IP Address for the route: 001.000.000.000 – 223.255.255.255

Table 5-13. IP Routing Table Values (2 of 2)

Column	What It Indicates
Hop	The number of hops in the route to the destination (1–15). If 16 appears, the route is in the process of being aged out.
Type	The method used to add the route to the table. ■ RIP: The route was discovered through Routing Information Protocol. The route remains until its TTL (Time to Live) expires, a better route is provided via RIP, or there is a power reset. ■ Loc: The route was added due to the FrameSaver unit's local configuration; a Default IP Address or an SNMP Manager Initial Route Destination have been configured. The route remains until the unit's configuration changes. ■ NMS: The route was added by a Network Management System using SNMP (Simple Network Management Protocol). The route remains until there is a power reset of the unit. ■ ICMP: The route was added because an ICMP (Internet Control Management Protocol) redirect message was received from a router indicating a better route to the destination. That is, a datagram was sent to a router and the router is informing the datagram source through an ICMP redirect message of a better route. ■ Tmp: The route was added as a temporary route in order to respond to an IP packet that was received. The route remains until its TTL expires or there is a power reset.
Interface	Specifies the interface to be used to reach the destination. ■ COM: Communications port ■ PVCname: Name of the management PVC (e.g., PVCmgmt1001) ■ Internal: The interface to be used for software loopbacks or internal device functions in order to reach the destination.
TTL	The Time to Live that was set for the route, in seconds: 1 – 999. If 999 appears, the route is a permanent one.

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          9128-II
Device Name: Node A              5/26/2000 23:32

                                PERFORMANCE STATISTICS

                                Service Level Verification
                                DLCI
                                Frame Relay
                                ESF Line
                                DBM Call
                                Ethernet
                                Clear All Statistics

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

DBM Call Statistics only appear when the FrameSaver unit has the ISDN DBM feature, and Ethernet only appears for the FrameSaver SLV 9128-II.

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 CIrSLV&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 CIrLinkStats function key to reset the frame relay link performance statistics.

Performance Statistics → Frame Relay

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

Performance Statistics → ESF Line

- Use the CIrDBMStats function key to reset the DBM call performance statistics.

Performance Statistics → DBM Call

- Use the CIrStats function key to reset all Ethernet port 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 5-14. 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 <i>xx,yyy</i>, <i>xx</i> being the VPI number (0–15) and <i>yyy</i> 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 ¹ ■ Above CIR ¹ ■ Within CIR ¹ ■ Between CIR&EIR ¹ ■ Above EIR ¹	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 3-2, Service Level Verification Options) must be enabled for these statistics to appear. ■ The number of frames transmitted by the far-end device that were above the committed information rate and were dropped in transit. ■ The number of frames transmitted by the far-end device that were within the committed information rate, but were dropped in transit. ■ 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. ■ The number of frames transmitted by the far-end device that were above the excess information rate and were dropped in transit.
¹ Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.	

Table 5-14. Service Level Verification Performance Statistics (2 of 2)

Statistic	What It Indicates
Inbound Dropped Characters ¹	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 3-2, 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 ¹ ■ Within CIR ¹ ■ Between CIR&EIR ¹ ■ Above EIR ¹	■ The number of bytes transmitted by the far-end device that were above the committed information rate and were dropped in transit. ■ The number of bytes transmitted by the far-end device that were within within the committed information rate, but were dropped in transit. ■ 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. ■ 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 3-2, 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.
¹ Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.	

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

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

DLCI Performance Statistics

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

Main Menu → Status → Performance Statistics → DLCI

Table 5-15. 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 by the far-end device for on the selected DLCI of the frame relay link that were within the committed information rate.
■ Between CIR&EIR	■ The number of frames and octets sent by the far-end device on the selected DLCI of the frame relay link that were between the committed information rate and excess information rate.
■ Above EIR	■ The number of frames and octets sent by the far-end device on the selected DLCI of the frame relay link that were above the excess information rate.
■ With DE Set	■ The number of frames and octets sent on the selected DLCI of the frame relay link with the discard eligible bit set.
¹ Only appears for the network interface.	

Table 5-15. DLCI Performance Statistics (2 of 2)

Statistic	What It Indicates
Total Tx Frames/ Tx Octets ■ 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 ■ Within CIR ■ Between CIR&EIR ■ Above EIR ■ With DE Set ■ With BECN Set ■ With FECN Set	Total number of data frames and octets (8-bit bytes) received for the selected DLCI on the frame relay link. ■ The number of frames and octets received on the selected DLCI of the frame relay link that were within the committed information rate. ■ 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. ■ The number of frames and octets received on the selected DLCI of the frame relay link that were above the excess information rate. ■ The number of frames and octets received on the selected DLCI of the frame relay link with the discard eligible bit 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. ■ 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.

For FrameSaver units with an ISDN DBM:

All enabled multilink aggregate links are available for selection from the Frame Relay Performance Statistics screen. The multilink aggregate link must be enabled if statistics are to be collected for this frame relay link. When the frame relay link is the multilink aggregate link, statistics for its related constituent links can be viewed.

To view the statistics for a multilink constituent link, select the ConstLinkStats function key. All enabled multilink constituent links become available for selection. Select the desired constituent link from the Multilink Constituent Link field.

The frame relay performance statistics collected for any frame relay link are collected for multilink frame relay links, unless the link is a multilink aggregate link. In this case, statistics for Frame Relay LMI and Frame Relay HDLC Errors are not collected; these statistics are available for multilink constituent links only.

Table 5-16. Frame Relay Performance Statistics (1 of 4)

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.

Table 5-16. Frame Relay Performance Statistics (2 of 4)

Statistic	What It Indicates
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.
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.

Table 5-16. Frame Relay Performance Statistics (3 of 4)

Statistic	What It Indicates
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 5-16. Frame Relay Performance Statistics (4 of 4)

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.

ESF Line Performance Statistics

These statistics appear when ESF Line is selected from the Performance Statistics menu for the network interface.

Main Menu → Status → Performance Statistics → ESF Line

Only seven T1 network statistical intervals appear on the screen at any one time. You can choose which intervals to display on your screen by entering:

- Interval Number (01–96)
- or –
- Time (Hours and Minutes)

NOTES:

Interval 01 is the interval occurring just prior to the current one;
Interval 02 is 2 intervals prior to the current one, etc.

Selecting a specific time is useful when the approximate time at which a specific event occurred is known.

Edit any of the interval or time fields on lines 10, 13, or 16. When Enter is pressed, the values change to the selected range.

To select intervals . . .	You must enter an interval or time on . . .
Occurring on and before a selected interval or time	Line 10. The display will include the selected interval plus the 6 intervals recorded before it.
Bracketing a selected interval or time	Line 13. The display will include the selected interval plus the 3 intervals recorded before it and the 3 intervals recorded after it.
Occurring on and after a selected interval or time	Line 16. The display will include the selected interval plus the 6 intervals recorded after it.

The following performance statistics are collected for ESF line conditions.

Table 5-17. ESF Line Condition Performance Statistics

Statistic	What It Indicates
Errored Seconds (ES)	Any second with one or more ESF Error events.
Unavailable Seconds (UAS)	Any second in which service is unavailable. Begins incrementing at the onset of 10 consecutive seconds of severely errored seconds (SES), and stops incrementing after 10 consecutive seconds of no SESs.
Severely Errored Seconds (SES)	Any second with 320 or more CRC errors or one or more Out Of Frame (OOF) events.
Bursty Errored Seconds (BES)	Any second with more than one, but less than 320 CRC errors.
Controlled Slip Seconds (CSS)	Any second with one or more controlled slips (a replication or deletion of a DS1 frame by the receiving device). This is collected for network performance statistics only.
Loss of Frame Count (LOFC)	The number of Loss of Frame conditions.
Worst Interval	The largest number of seconds for either ES, UAS, SES, BES, or CSS, or the greatest Loss of Frame Count (LOFC). If more than one interval contains the same worst value, then the oldest interval is displayed.

DBM Call Performance Statistics

When an ISDN DBM is installed, these statistics are available for ISDN calls and call attempts.

You can clear these statistics by selecting the ClrDBMStats function key, or you can clear all performance statistics for the system.

Main Menu → Status → Performance Statistics → Clear All Statistics

Clearing these statistics will not affect performance statistics stored in user history for the system. The statistics are only cleared locally.

Table 5-18. DBM Call Performance Statistics

Statistic	What It Indicates
Total Call Attempts	Number of call attempts made by the DBM.
Total Calls Originated	Number of successful calls made by the DBM.
Total Calls Answered	Number of successful calls answered by the DBM.
Total Calls Rejected (Security)	Number of calls rejected by the DBM due to security.
Total Calls Rejected (Other)	Number of calls rejected by the DBM due to reasons other than security, like incoming voice call requests.
Average Call Duration (mins)	Average amount of time, in minutes, that successful calls take.
Longest Call Duration (mins)	Amount of time spent, in minutes, during the longest successful call.
Total Call Duration (mins)	Sum of all successful calls in minutes.

Ethernet Performance Statistics

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

Main Menu → Status → Performance Statistics → Ethernet

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

Trap Event Log

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

Main Menu → Status → Trap Event Log

Trap Event Log Screen Example

main/status/event_log		9128-II
Device Name: Node A		5/26/2000 23:32
TRAP EVENT LOG		Total Trap Events: 535
Time Elapsed Since Event	Event	
0d 23:59:59	Change in Frames Discarded due to Inbound Resource Errors on Sync Data Port S01P1 frame relay link "Port-1" exceeded threshold of 1 by 105.	
2d 23:59:59	Change in Total LMI Errors on Network T1 frame relay link "Net1-FR1" exceeded threshold of 1 by 59.	
6d 23:59:59	DLCI 101 of Sync Data Port S01P1 frame relay link "Port-1" up.	
10d 23:59:59	DLCI 101 of Sync Data Port S01P1 frame relay link "Port-1" down.	
20d 23:59:59	Primary clock failed.	
56d 23:59:59	Sync Data Port S01P1 frame relay link "Port-1" LMI down.	
64d 23:59:59	Network T1 frame relay link "Net1-FR1" LMI down.	
122d 23:59:59	Network T1 down.	
364d 23:59:59	Unit reset.	

<u>R</u> efresh	<u>P</u> gUp	<u>P</u> gDn
ESC for previous menu		<u>M</u> ainMenu <u>E</u> xit

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

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

Modem Operation

This section includes the following:

- *Activating the Modem PassThru Feature*
- *Canceling Modem PassThru Operation*
- *Manually Disconnecting the Modem*
- *Verifying Modem Operation*

See *Setting Up the Modem* in Chapter 3, *Configuration*, for additional information.

Activating the Modem PassThru Feature

Access to the router's VT100-compatible user interface is provided through the FrameSaver unit's Modem PassThru feature, also known as Router Assist. A dial-up connection to the FrameSaver unit is used to access the router when the unit is set up for this use. See *Setting Up to Use the Modem PassThru Feature* in Chapter 3, *Configuration*, to configure the unit for Modem PassThru operation.

Once the unit is set up to use this feature, each time access to the router is needed, the feature is activated from the Control menu.

Main Menu → Control → Enable Modem PassThru to COM

When this feature is active, a logical connection between the unit's modem and COM ports is made, and data received over the modem port is transmitted out the COM port to the router's AUX or console port, and data received from the router on the COM port is transmitted out the modem port. While Modem PassThru is active, normal access to the FrameSaver unit through either its modem or COM port is suspended.

When an escape sequence (minus, minus, minus, with a minimum of 50 ms between each) is detected, the FrameSaver unit switches back to normal user interface operation.

Canceling Modem PassThru Operation

When Modem PassThru is active, but access to the FrameSaver unit's menu-driven user interface is needed, Modem PassThru can be cancelled from the Control menu.

Main Menu → Control → Disable Modem PassThru to COM

Manually Disconnecting the Modem

If Trap Disconnect is disabled, a modem connection remains until it is manually disconnected. Select Disconnect Modem from the Control menu.

Main Menu → Control → Disconnect Modem

Respond yes to the **Are you sure?** prompt.

Verifying Modem Operation

► Procedure

If Port Use is set to Terminal (dial-in access):

1. Dial the modem's phone number using a remote VT100-compatible asynchronous terminal or PC.
2. Verify that the Main Menu appears.

► Procedure

If Port Use is set to Net Link (SNMP, Telnet, FTP, and trap dial-out):

1. Dial the modem's phone number using a PC running PPP or SLIP link protocol.
2. From the PC, run an IP Ping test to the modem interface.

If your results using either method are unsuccessful, make sure both ends of the modem cable are properly seated and secured. Then, verify that the modem was configured correctly (see *Setting Up the Modem* in Chapter 3, *Configuration*).

ISDN DBM Operation

The following sections only apply to units with an ISDN DBM. They include the following:

- *Forcing Backup (Disruptive)*
- *Placing a Call (Nondisruptive)*
- *Verifying ISDN Lines*
- *Verifying That Backup Can Take Place*

Forcing Backup (Disruptive)

Use this procedure to force backup when network maintenance is planned, when equipment problems are reported, or when testing the backup path – whenever data needs to be forced from the primary destination interface to the alternate destination, typically from the T1 network to the ISDN.

► Procedure

1. Make sure the ISDN Link Profiles are set up correctly, Auto Backup is enabled, and the ISDN interface is enabled (see *Setting Up Dial Backup* in Chapter 3, *Configuration*).
2. Have someone at the far end disconnect the network cable to initiate backup.
3. Verify that backup is taking place.
See *Verifying That Backup Can Take Place*.

NOTE:

When an alarm requiring backup is received, backup can be manually controlled by enabling or disabling the Auto Backup option (see Step 2).

4. Have the far-end network cable reconnected to return to standard operation.

Placing a Test Call (Nondisruptive)

Use this procedure to test the ISDN path to each remote site. This procedure will not put the system into backup.

► Procedure

1. Make sure the ISDN Link Profiles and DLCIs are set up correctly for the DBMs at each end (see *Setting Up ISDN Link Profiles* in Chapter 3, *Configuration*).

Main Menu → Configuration → ISDN → Link Profiles

Main Menu → Configuration → ISDN → DLCI Records

2. Place a Test Call from one of the devices.

Main Menu → Test → ISDN Call/PVC Tests

- Select the link to be tested.
- Start a Test Call. The Status should be Active.

If the Result is . . .	Then . . .
Frame Relay Link Up	The call was successful.
Frame Relay Link Down	The call was not successful. Verify the configuration and Link Status in the ISDN Link Profile.

- Select Stop to end the Test Call.

Use this procedure to test the ISDN path to each remote site. This procedure will not put the unit into backup.

Verifying ISDN Lines

Use either of the following methods to verify operation of the ISDN lines.

- Check the status of the DBM interface:

Main Menu → Status → DBM Interface Status

Line Status should display Active. If an invalid (Inv) status appears (e.g., Inv SPID for an ISDN BRI DBM) in the Line Status field, verify that you entered ISDN physical options correctly.

- Check the status of the unit:

*Main Menu → Status → System and Test Status →
Health and Status column*

System Operational should appear.

If **ISDN Network Failed** appears, check that both ends of the ISDN cable are seated properly for a good physical connection. If that does not clear the message, verify that you entered ISDN physical option information correctly, then contact the network service provider.

See *DBM Interface Status* and Table 5-7, *Health and Status Messages*, for additional status information.

Verifying That Backup Can Take Place

As each remote site is installed, verify its backup operation by unplugging the network cable so the system is forced into backup.

- Verify the ISDN lines by checking the DBM Interface Status.

Main Menu → Status → DBM Interface Status

Line Status should be Active. If an invalid (Inv) status (e.g., Inv SPID) is displayed, verify that you entered ISDN physical options correctly.

- Check backup setup and that data can be passed between DBMs.
- Reconnect the network cable.

See Table 5-7, *Health and Status Messages*, *Viewing LEDs and Control Leads*, and *DBM Call Performance Statistics* for additional information.

FTP File Transfers

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

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

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

- You must have Access Level 1 permission to use the **put** and **get** commands, and to access the LMI packet capture data. 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.sys`) cannot be **put** into a FrameSaver node.
- LMI packet capture data (`lmitrace.sys`) 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 4, *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
<code>cd <i>directory</i></code>	Change the current directory on the FrameSaver node to the specified <i>directory</i> .
<code>dir [<i>directory</i>]</code>	Print a listing of the directory contents in the specified <i>directory</i> . If no directory is specified, the current one is used.
<code>get <i>file1</i> [<i>file2</i>]</code>	Copy a file from the remote directory of the FrameSaver node to the local directory on the host (for configuration files only).
<code>remotehelp [<i>command</i>]</code>	Print the meaning of the command. If no argument is given, a list of all known commands is printed.
<code>ls [<i>directory</i>]</code>	Print an abbreviated list of the specified directory's contents. If no directory is specified, the current one is used.
<code>put <i>file1</i> [<i>file2</i>]</code>	Copy <i>file1</i> from a local directory on the host to <i>file 2</i> in the current directory of the FrameSaver node. If <i>file2</i> is not specified, the file will be named <i>file1</i> on the FrameSaver node.
<code>recv <i>file1</i> [<i>file 2</i>]</code>	Same as a get .
<code>send <i>file1</i> [<i>file 2</i>]</code>	Same as a put .
<code>pwd</code>	Print the name of the current directory of the FrameSaver unit node.
<code>bin</code>	Places the FTP session in binary-transfer mode.

Upgrading System Software

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

NOTE:

Upgrades can be performed through the network using a Management PVC, or through the COM port if Port Use is set to Net Link (see Table 3-20, [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 Rxxxxxx.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 Rxxxxxx.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.

Upgrading ISDN BRI DBM Software

A separate download to update PRI DBM functionality is not necessary; a PRI upgrade is incorporated in the unit's program code. However, if the FrameSaver unit has a BRI DBM, the program code must be upgraded separately.

To upgrade a FrameSaver unit's BRI DBM program code, you must transfer the **dbmprog.ocd** file in the Dial Backup Module directory using the **put** command.

► Procedure

To perform a BRI DBM upgrade:

1. Initiate an FTP session to the device that you are upgrading.
2. Type **bin** to enter binary transfer mode.
3. Type **cd dbm** to change to the Dial Backup Module directory.

NOTE:

If the FrameSaver unit is not equipped with a DBM or the DBM does not contain any downloadable software, the message **dbm: no such file or directory** appears.

4. Perform a **put** of Rxxxxxx.ocd (xxxxxx being the software release number) to the dbmprog.ocd file to start the upgrade.

If the message displayed is . . .	Then . . .
DBM Download Required	Errors were detected during the DBM download. The dbmprog.ocd file will need to be downloaded again.
dbmprog.ocd: File Transfer Complete	The download was successful.
dbmprog.ocd: File Transfer Failed	The download was not successful. Possible cause: A bad or invalid file, or the wrong checksum. A different dbmprog.ocd file will need to be downloaded for the DBM to become operational. Repeat the step or end the FTP session.

5. Close the FTP session.
6. Verify that the new software release was successfully installed as the DBM Software Revision.

Main Menu → Status → Identity

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 *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* to see what is included on the unit's Identity screen.

Transferring Collected Data

SLV user history statistics and LMI packet capture data can be uploaded to an NMS or a Network Associates Sniffer using FTP, which is faster than other methods. The rate at which the data file is transferred is the rate set by the FTP Max Transfer Rate (Kbps) option (see Table 3-17, [Telnet and FTP Session Options](#) in Chapter 3, *Configuration*).

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 6, *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 uhbcsfull.dat file. ■ File Transfer Complete – Transfer was successful. ■ File Transfer Failed – Transfer was not successful. Try again or end the session.
LMI packet capture data	1. Stop the LMI Packet Capture Utility. <i>Main Menu → Control → LMI Packet Capture Utility</i> LMI packet capture data is not available (readable) when the LMI Packet Capture Utility is Active. 2. Perform a get of the lmitrace.sysc file. One of the following will display for the file: – File Transfer Complete – File Transfer Failed – Permission Denied – The LMI Packet Capture Utility was not readable. Stop the LMI Packet Capture Utility and try again.

3. Close the FTP session.

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

Turning Off the System Alarm Relay

For carrier-mounted FrameSaver units, an alarm system relay is provided by the 9000 Series Access Carrier. This relay activates a light or buzzer when an alarm condition is detected in one of the FrameSaver units.

Once the alarm relay is connected, enabling the System Alarm Relay option activates this feature (see Table 3-3, **General System Options**).

Once activated, the relay is turned off in one of the following ways:

- The alarm condition that activated the relay no longer exists. The relay stays on until all alarm conditions have been corrected.
- The System Alarm Relay option can be disabled.

Main Menu → Configuration → System → General

- System Alarm Relay Cut-Off can be selected.

Main Menu → Control → System Alarm Relay Cut-Off

See *Alarm Relay Connector* in the *9000 Series Access Carrier Installation Instructions* for information about connecting the alarm relay.

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 a Misconfigured Unit*
- *Troubleshooting Management Link Feature*
- *LMI Packet Capture Utility Feature*
 - *Viewing Captured Packets from the Menu-Driven User Interface*
- *Alarms*
- *Viewing the Trap Event Log*
- *Troubleshooting Tables*
 - *Device Problems*
 - *Frame Relay PVC Problems*
 - *ISDN DBM Problems*
- *Tests Available*
 - *Test Timeout Feature*
 - *DBM Tests*
- *Starting and Stopping a Test*
 - *Aborting All Tests*
- *PVC Tests*
 - *PVC Loopback*
 - *Send Pattern*

- *Monitor Pattern*
- *Connectivity*
- *Test Call*
- *Physical Tests*
 - *Line Loopback*
 - *Payload Loopback*
 - *Repeater Loopback*
 - *DTE Loopback*
 - *Send Line Loopback*
 - *Data Channel Loopbacks on a Frame Relay Link*
 - *Send Remote Line Loopback*
 - *Send and Monitor Pattern Tests*
- *IP Ping Test*
- *Lamp Test*

Problem Indicators

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

Indicators . . .	See . . .
LEDs	<i>Viewing LEDs and Control Leads</i> and <i>LED Descriptions</i> in Chapter 5, <i>Operation and Maintenance</i> , as well as the user interface screen. <i>Main Menu → Status → Display LEDs and Control LEDs</i>
Health and Status	Table 5-7, <i>Health and Status Messages</i> , in Chapter 5, <i>Operation and Maintenance</i> . <i>Main Menu → Status → System and Test Status</i> Messages also appear at the bottom of any menu-driven user interface screen.
Performance statistics	<i>Performance Statistics</i> in Chapter 5, <i>Operation and Maintenance</i> , to help you determine how long a problem has existed.
Alarm conditions that will generate an SNMP trap	<i>Alarms</i> on page 6-7.
SNMP traps	Appendix B, <i>SNMP MIBs and Traps, and RMON Alarm Defaults</i> . Traps supported include warm-start, authentication-failure, enterprise-specific (those specific to the unit), link-up, and link-down.

Resetting the Unit and Restoring Communication

You can reset the unit in one of four ways:

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

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

Resetting the Unit from the Control Menu

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

► Procedure

To reset the unit from the Control menu:

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

Resetting the Unit By Cycling the Power

Disconnecting, then reconnecting the power cord resets the unit.

Restoring Communication with a Misconfigured Unit

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

► Procedure

To reset COM port settings:

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

If selecting . . .	The following occurs . . .
Reset COM Port usage	■ Port Use is set to Terminal so the asynchronous terminal can be used. ■ Data Rate (Kbps), Character Length, Stop Bits, and Parity are reset to the factory defaults. ■ Unit resets itself.
Reload Factory Defaults	■ All configuration <u>and</u> 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 3, *Configuration*, 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.sys 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. Select an enabled frame relay link.
Main Menu → Control → LMI Packet Capture Utility
2. Select an enabled frame relay link, or Capture Interface, either Net1-FR1 Port-1, Port-2, or an ISDN Link Name if a DBM is present.
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 5, *Operation and Maintenance*, 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                               9128-II
Device Name: Node A                                              5/26/2000 23:32

                                LMI TRACE LOG                                Page 1 of 3

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

                                                                LMI Record #2 at 0 s
                                                                Status Enquiry Message, 13 bytes
                                                                LMI Type is Standard on DLCI 1023
                                                                Sequence Number Exchange
                                                                Send Seq #181, Rcv Seq #177

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

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

The following information is provided:

- The internal LMI record number assigned to the packet (1–8000), and the amount of time the utility was running when the packet was captured.
The maximum amount of time displayed is 4,294,967 seconds (s), which is reset to 1 second when this amount of time is exceeded.
- The type of message, either Status or Status Enquiry, from the captured packet, and the number of bytes in the packet.
- The LMI Type identified in the Protocol Discriminator portion of the captured packet, and the DLCI number for the packet.
- The type of information contained in the captured packet, either Sequence Number Exchange or Full Status Report.
- The send and receive (rcv) sequence numbers from the captured packet (0–255).
- On the Packets Received side of the screen, PVC status for up to ten DLCIs can be shown. It shows the DLCI number, its active bit status, and if Standard LMI is running, the DLCI's CIR value.

Alarms

The following table describes the alarm conditions that will generate an SNMP trap for a physical interface, and the frame relay LMIs and DLCIs. These alarm conditions also generate Health and Status messages seen on the System and Test Status screen.

Main Menu → Status → System and Test Status

Table 6-1. Alarm Conditions (1 of 7)

Alarm Condition	What It Indicates	What To Do
AIS at DSX-1	For the DSX-1 interface, the attached DTE is transmitting an AIS.	For the DSX-1 interface, check the DTE attached to the interface.
AIS at Network 1	An Alarm Indication Signal (AIS) is being received by the interface. AIS is an unframed, all ones signal.	For the network interface, report the problem to your T1 service provider.
CTS down to Port-1 Device	The CTS control lead on the device's interface is off.	Check DTR and RTS from Port-1. ■ Verify that the port is enabled. ■ Check DTR from the user data port.
DBM BRI Card Failed	The ISDN BRI DBM failed to pass the self-test.	Reset the FrameSaver unit (<i>Main Menu → Control → Reset Device</i>). If the DBM fails again, contact your service representative.
DLCI <i>nnnn</i> Down, <i>frame relay link</i> ^{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 provider, or your ISDN service provider if an ISDN Link Name is the link.
DTR Down from Port-1 Device	The DTR control lead on the device connected to Port- <i>n</i> is disasserted. The DTR control lead on the device connected to the specified port is off. This message applies to data ports that act as DCEs.	Examine the attached DTE and cable connected to the system's port. ■ Check that the port cable is securely attached at both ends. ■ Check the status of the attached equipment.
¹ <i>nnnn</i> indicates a DLCI number of 16 through 1007. ² <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i>. The frame relay link associated with a user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface.		

Table 6-1. Alarm Conditions (2 of 7)

Alarm Condition	What It Indicates	What To Do
EER at Network 1	The error rate of the received network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.	■ Verify that the network cable is securely attached at the network interface. ■ Contact your network provider.
Ethernet Link Down	The communication link for the Ethernet port is down and the Interface Status for the port is enabled.	Check the LAN connected to the Ethernet port.
Internal Modem Failed	The unit's internal modem failed to pass the self-test.	Reset the FrameSaver unit (<i>Main Menu → Control → Reset Device</i>). If the modem fails again, contact your service representative.
ISDN Link Profile Disabled <i>ISDN Link Name</i>	An ISDN backup call could not be made because the ISDN link profile specified Link Name is disabled (<i>Main Menu → Configuration → ISDN → Link Profiles</i>).	Enable the ISDN link profile if you want to make a call.
ISDN Link Profile Invalid, <i>ISDN Link Name</i>	An ISDN backup call could not be made because the ISDN link profile specified (<i>ISDN Link Name</i>) is invalid.	Check that the phone number is correct.
ISDN Network Failed (Active/Idle)	An ISDN network failure was detected when a backup call was in progress or the DBM was in Idle mode.	Contact your network provider if the problem persists.
² <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network port, Network 1. – Port-<i>n</i>. The frame relay link associated with a user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface.		

Table 6-1. Alarm Conditions (3 of 7)

Alarm Condition	What It Indicates	What To Do
Link Profile Disabled, <i>ISDN Link Name</i>	An ISDN backup call could not be made because the specified link profile was disabled.	Change the ISDN Link Profile's Link Status to Auto (<i>Main Menu → Configuration → ISDN → Link Profiles</i>).
LMI Down, <i>frame relay link</i> ²	The Local Management Interface is down for the specified frame relay link.	For the network interface: ■ If LMI was never up, verify that the LMI Protocol setting reflects the LMI type being used. ■ If LMI was never up: – Verify that the proper time slots have been configured. – Verify that the LMI Protocol setting reflects the LMI type being used. ■ Verify that Frame Relay Performance Statistics show LMI frames being transmitted. If all of the above have been verified and the physical link is not in Alarm, contact your network provider. 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 <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network port, Network 1. – Port-<i>n</i>. The frame relay link associated with a user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface.		

Table 6-1. Alarm Conditions (4 of 7)

Alarm Condition	What It Indicates	What To Do
LOS at DSX-1	A Loss of Signal (LOS) condition is detected on the DSX-1 interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. ■ DSX-1 cable problem. ■ No signal being transmitted from the DTE.	■ Check that the DSX-1 cable is securely attached at both ends. ■ Check the DTE status.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. ■ Network cable problem. ■ No signal is being transmitted at the far-end FrameSaver unit. ■ T1 facility problem.	■ Check that the network cable is securely attached at both ends. ■ Check far-end FrameSaver unit status. ■ Contact your network provider.
Network Com Link Down	The communication link for the COM port is down and the COM port is configured for Net Link.	Check the router connected to the COM port.
OOF at DSX-1	An Out of Frame (OOF) condition is detected on the DSX-1 interface. ■ Incompatible framing format between the DTE and the FrameSaver unit. ■ DSX-1 cabling problem.	■ Check that the framing format for the DSX-1 (DTE) interface is correct. ■ Check that the DSX-1 cable is securely attached at both ends.

Table 6-1. Alarm Conditions (5 of 7)

Alarm Condition	What It Indicates	What To Do
OOF at Network 1	An Out of Frame (OOF) condition is detected on the network interface. ■ Incompatible framing format between the network and the FrameSaver unit. ■ Network cabling problem. ■ T1 facility problem.	■ Check that the framing format for the network interface is correct. ■ Check that the network cable is securely attached at both ends. ■ Contact your network provider.
Power Supply/Fan Alarm	The power supply output voltage has dropped below the specified tolerance level required for the system. Or one or both fan trays are not operating properly.	Check the LEDs on the power supply and fan trays to determine which may have failed, then replace the failed component.
Primary Clock Failed	A failure of the configured primary clock source for the unit was detected and the secondary clock is providing the timing for the unit. This condition clears when the configured primary clock is restored.	■ Check that the network cable is securely attached at both ends. ■ Contact your network provider.
Primary & Secondary Clocks Failed	A failure of both clock sources configured for the unit was detected. This condition only applies to T1 network and DSX-1 interfaces. It clears when the configured primary clock is restored.	
Secondary Clock Failed	A failure of the configured secondary clock source for the unit was detected and the internal clock is providing the timing for the unit. The clock source will not automatically switch from internal until the primary clock source returns.	

Table 6-1. Alarm Conditions (6 of 7)

Alarm Condition	What It Indicates	What To Do
Self-Test Failure	The unit did not pass its basic verification tests when it was powered on or reset.	■ Reset the unit. ■ Contact your service representative.
SLV Latency Exceeded, DLCI <i>nnnn</i> , <i>frame relay link</i> ^{1, 2, 3}	The measured latency of SLV communication responses from the remote unit on this DLCI is excessive, so the DLCI has been declared unsuitable for normal multiplexed PVC operation (DLCI Type is set to Multiplexed).	Wait until the DLCI is declared operational again. If the unit has ISDN backup capability, this condition will initiate backup.
SLV Timeout, DLCI <i>nnnn</i> , <i>frame relay link</i> ^{1, 2, 3}	An excessive number of SLV communication responses from the remote system have been missed on the specified multiplexed DLCI and link. If the frame relay link is Net1-FR1, the timeout is on the network FrameRly1 timeslot assignment. When a hardware bypass-capable device has been detected at the other end of the PVC and this condition occurs, only user data for EDLCI 0 will be transmitted as long as the condition exists.	■ Verify that the network LMI is up. If it is, contact your network service provider. ■ If a DBM is present and Auto Backup is enabled, backup is initiated automatically.
Suboptimal Link Rate, <i>frame relay link</i> ²	The specified frame relay multilink has failed to achieve the configured Maximum Link Rate for the link. This message appears for multilink aggregate frame relay links if LMI is down on any of its constituent links.	No action required.
¹ <i>nnnn</i> indicates a DLCI number of 16 through 1007. ² <i>frame relay link</i> is one of the following: – Net1-FR1. The frame relay link specified for the network interface, Network 1. – Port-<i>n</i>. The frame relay link associated with a user data port. – <i>ISDN Link Name</i> on a non-network ISDN DBM interface. ³ Does not apply to a TS Access Management Link DLCI.		

Table 6-1. Alarm Conditions (7 of 7)

Alarm Condition	What It Indicates	What To Do
Two Level-1 Users Accessing Device	Another user with Level-1 security access is currently accessing the unit. Be aware that actions of the other user may override your test commands and configuration changes.	Wait until no other Level-1 users are accessing the unit if testing or configuration will be performed.
Yellow at DSX-1	A yellow alarm signal is received on the DSX-1 interface. DTE has detected a LOS or OOF condition.	■ Check that the DSX-1 cable is securely attached at both ends. ■ Check the status of the attached equipment.
Yellow at Network 1	A yellow alarm signal is received on the network interface. ■ Network cable problem. ■ T1 facility problem.	■ Check that your network cable is securely attached at both ends. ■ Contact your network provider.

Viewing the Trap Event Log

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

See *Trap Event Log* in Chapter 5, *Operation and Maintenance*, for a screen example and additional information.

Troubleshooting Tables

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

Device Problems

Table 6-2. Device Problems (1 of 2)

Symptom	Possible Cause	Solutions
No power, or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle to rear panel connection.	Check that the power cord is securely attached at both ends.
	The wall receptacle has no power.	■ Check the wall receptacle power by plugging in some equipment that is known to be working. ■ Check the circuit breaker. ■ Verify that your site is not on an energy management program.
Power-On Self-Test fails. Only Alarm LED is on after power-on.	The unit has detected an internal hardware failure.	■ Reset the unit and try again. ■ Contact your service representative. ■ Return the unit to the factory (refer to <i>Warranty, Sales, Service, and Training Information</i> on page A of this document).

Table 6-2. Device Problems (2 of 2)

Symptom	Possible Cause	Solutions
Cannot access the unit or the menu-driven user interface.	Login or password is incorrect, COM port is misconfigured, or the unit is otherwise configured so it prevents access.	- Reset the unit (see <i>Restoring Communication with a Misconfigured Unit</i>). - Contact your service representative.
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 6-3. 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 LMI Reported DLCIs screen. If the DLCI(s) is not active, contact the service provider. ■ Verify the LMI Reported DLCI field on the Interface Status screen.
	DTE is configured incorrectly.	Check the DTE's configuration.
	LMI is not configured properly for the DTE or network.	Configure LMI characteristics to match those of the DTE or network.
	LMI link is inactive.	Verify that the LMI link is active on the network; the Status Msg Received counter on the Network Frame Relay Performance Statistics screen increments.
Losing Data	Frame relay network is experiencing problems.	Run PVC Loopback and Pattern tests to isolate the problem, then contact the service provider.
Out of Sync	If Monitor Pattern was selected, it means the test pattern generator and receiver have not yet synchronized. CIR settings for the units at each end are mismatched. If the message persists, it means that 5 packets out of 25 are missing or are out of sequence.	■ Verify that the unit at the other end is configured to Send Pattern. Correct unit configurations. ■ Correct the CIR setting so both units are configured the same. ■ Check the line's error rate – the physical line quality. Contact the service provider.

ISDN DBM Problems

Table 6-4. ISDN DBM Problems

Symptom	Possible Cause	Solutions
Cannot connect to the remote unit	Misconfiguration	■ Verify that the link profiles are correct in both units, both the area codes and phone or ID numbers (see <i>Setting Up ISDN Link Profiles</i> in Chapter 3, <i>Configuration</i>). ■ For a BRI DBM, verify that the SPIDs and local area codes and phone numbers are correct (see <i>Configuring the ISDN DBM Interface</i> in Chapter 3, <i>Configuration</i>). ■ Verify that the unit at one end is configured to originate and the unit at the other end is configured to answer a call. ■ Verify that the ISDN interface is enabled. ■ Verify that Auto Backup is enabled and no time restrictions apply.
DBM LMI comes up, but no data is transferred	Misconfiguration	Check that the DLCI numbers are correct and are the same at both ends.

See Table 5-12, *Most Recent and Previous Last Cause Value Messages*, in Chapter 5, *Operation and Maintenance*, for additional information about ISDN problems. Last Cause Value messages appear on the DBM Interface Status screen.

Main Menu → Status → DBM Interface Status

See *Configuring the ISDN DBM Interface* and *Setting Up ISDN Link Profiles* in Chapter 3, *Configuration*, for more information about ISDN DBM configuration.

Tests Available

The following tests are available to a FrameSaver SLV 9126, 9128, or 9128-II.

Test Menu Example

```
main/test                                     9128-II
Device Name: Node A                          5/26/2000 23:32

                                TEST

                                Network PVC Tests
                                Data Port PVC Tests
                                ISDN Call/PVC Tests

                                Network Physical Tests
                                Data Port Physical Tests
                                DSX-1 Physical Tests
                                PRI Physical Tests
                                IP Ping
                                Lamp Test

                                Abort All Tests

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

If the unit does not have the ISDN DBM feature, **ISDN Call** does not appear with the ISDN PVC Tests. **PRI Physical Tests** only appears when an ISDN PRI DBM is installed.

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 system 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 accidentally 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 3, *Configuration*).

NOTE:

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

DBM Tests

The Test menu allows you to run PVC loopbacks and test patterns on the unit and its DBM interface. It is available to users with a security access level of 1 or 2. Currently, there are no physical tests for a BRI DBM interface.

DBM tests are started and monitored the same as the network tests. See *System and Test Status Messages* in Chapter 5, *Operation and Maintenance*, for ISDN backup-related test messages appearing on the System and Test Status screen. See *PVC Tests* on page 6-22 for additional information.

Starting and Stopping a Test

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

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

Start or stop an individual test using the same procedure.

► Procedure

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

1. Follow this menu selection sequence:

Main Menu → Test

2. Select an interface and test (e.g., Network, Data Port, or ISDN PVC Tests) and press Enter.

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

3. Select the Port number and press Enter.
4. Select the DLCI number and press Enter if a PVC test has been selected.
The cursor is positioned at Start in the Command column of the first available test and is highlighted.
5. To start the test, highlight **Start** under Command for the test you want to run and press Enter. Stop now appears and is highlighted, and the status of the test changes to Active.
The length of time that the test has been running is shown in the Result column.
6. To stop the test, press Enter to send the **Stop** command. Start reappears and the status of the test changes back to Inactive.

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 ISDN backup capability, 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                                     9128-II
Device Name: Node A                                     5/26/2000 23:32

                                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
Test Call:            Stop     Active  Frame Relay Link Up

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

```

If the unit does not have the ISDN DBM feature, or if the ISDN Link Profile's Link Status is disabled, **Test Call** does not appear. An Outbound Phone Number must be configured for **Test Call** to appear.

NOTE:

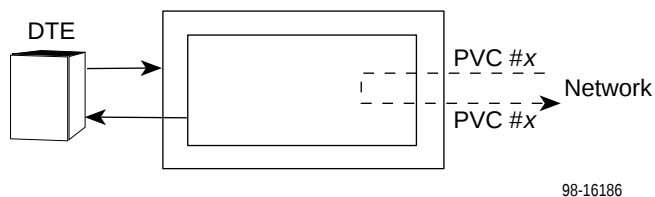
Errors encountered during these tests may be caused by mismatched CIRs in the two FrameSaver units. If errors are detected, verify the CIR configuration and retest.

PVC Loopback

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

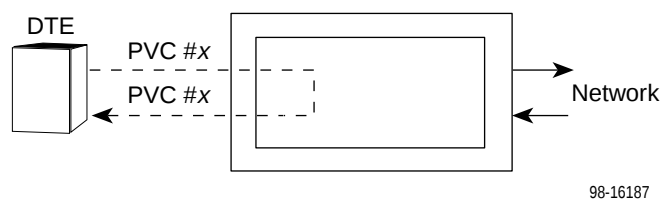
Main Menu → Test → Network PVC Test

Network PVC Loopback



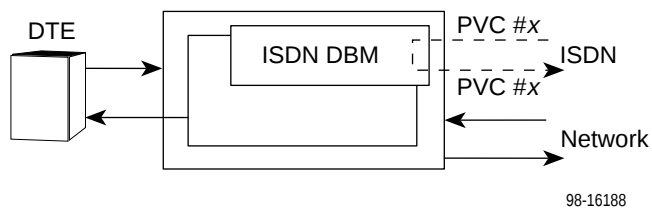
Main Menu → Test → Data Port PVC Tests

Port PVC Loopback



Main Menu → Test → ISDN Call/PVC Tests

ISDN PVC Loopback



Send Pattern

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

To send a pattern test on a link:

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

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

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

Monitor Pattern

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

To monitor a pattern test on a link:

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

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

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

Connectivity

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

To run a connectivity test on a link:

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

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

Test Call

Test Call tests the device's ability to place a call. It allows an alternate means of controlling the activation or deactivation of an ISDN link. This test only appears for a FrameSaver device with a DBM that is configured to originate backup calls (typically, the remote site) and has its ISDN Link Status option set to Auto.

To place a test call:

Main Menu → Test → ISDN Call/PVC Tests

When a test call is started, **Active** appears in the Status column. While the call is Active, the status of the call connection and the link appears in the Results column.

- A **Frame Relay Link Up** message indicates that the required calls have been made and the link is successfully passing LMI data.
- A **Frame Relay Link Suboptimal** message indicates that at least one call has been made on the link, the link is successfully passing LMI data, but the Maximum Link Rate configured in the ISDN Link Profile has not been achieved for the link.
- A **Frame Relay Link Down** message indicates that the call attempts were not successful.

NOTE:

Primary network data is not affected by a test call. If there is a network failure while a test call is active, the test call is terminated and the call is automatically converted to a backup call.

Physical Tests

Physical tests require the participation of your network service provider.

Main Menu → Test → [Network Physical Tests/Data Port Physical Tests/DSX-1 Physical Tests/PRI Physical Tests]

If the unit does not have the ISDN PRI DBM feature, PRI Physical Tests does not appear.

A FrameSaver unit's physical tests screen for the network interface is shown below.

Physical Tests Screen Example

```

main/test/network
Device Name: Node A
9128-II
5/26/2000 23:32

NETWORK 1 PHYSICAL TESTS

Test Command Status Results

Local Loopbacks
Line Loopback: Start Inactive 0:00:00
Payload Loopback: Start Inactive 0:00:00
Repeater Loopback: Start Inactive 0:00:00

Remote Loopbacks
Send Line Loopback: Down Send Inactive 0:00:00

Pattern Tests
Send: user-defined 0a0a Stop Active 0:00:00 - Errors 99999+
Monitor: user-defined 0a0a Stop Active 0:00:00 - Errors 99999+

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

```

The InjectErr function key at the bottom of the screen only appears when a Send Pattern Test is Active. Select InjectErr to inject a single bit error into the pattern being sent.

The ResetMon function key at the bottom of the screen only appears when a Monitor 511 test pattern is Active. Select ResetMon to reset the monitor pattern error counter.

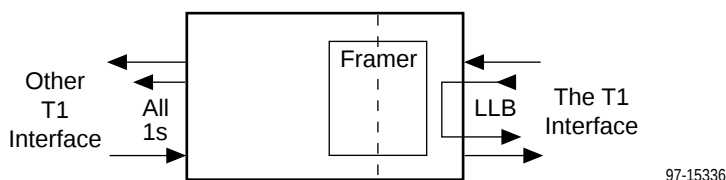
CAUTION:

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

Line Loopback

The Line Loopback (LLB) loops the information received on the selected interface back to the source of the loopback. When used with a pattern test at the remote node, LLB determines whether the problem is with the sending device or the T1 facility.

Main Menu → Test → Network Physical Tests



CAUTION:

This test may affect operation of frame relay PVCs assigned to the selected port. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

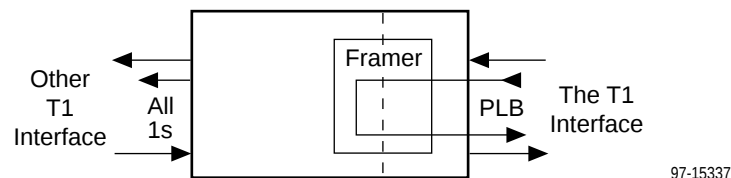
An LLB cannot be started when one of the following tests is active:

- Payload Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this network interface.
- Repeater Loopback on any other T1 interface with DS0s assigned to this network interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) assigned to this network interface.

Payload Loopback

The Payload Loopback (PLB) loops the information received on the selected interface back to the network after it has passed through the receive and transmit framing section of the device. Use the PLB to determine whether the problem is with the T1 facility or in the circuitry of the remote device.

Main Menu → Test → Network Physical Tests



CAUTION:

This test may affect operation of frame relay PVCs assigned to the selected interface. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

A PLB cannot be started when one of the following tests is active:

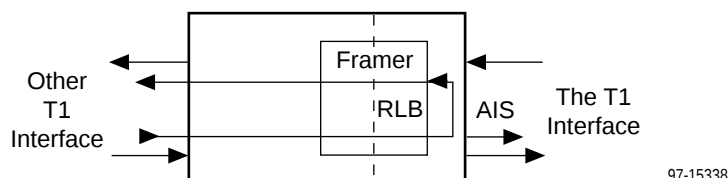
- Line Loopback, Repeater Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this network interface.
- Payload or Repeater Loopback on any other T1 interface with DS0s assigned to this network interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) and assigned to this network interface.

Repeater Loopback

The Repeater Loopback (RLB) loops data received from the data ports and the DSX-1 interface after the signal has passed through the framing circuitry. Use RLB to ensure that all of the data is correct up to the point where it is sent over the interface. This helps to indicate that the FrameSaver unit is operational.

Main Menu → Test → Network Physical Tests

An attached device or test equipment should generate and monitor data to be looped back.



The FrameSaver unit will not respond to any messages from the network during this test.

CAUTION:

This test may affect operation of frame relay PVCs assigned to the selected interface. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

An RLB cannot be started when one of the following tests is active:

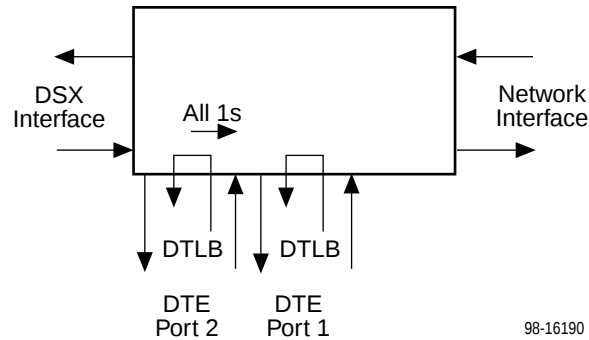
- Payload Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this network interface.
- All loopbacks on any other T1 interface with DS0s assigned to this network interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) assigned to this network interface.

DTE Loopback

The DTE external Loopback (DTLB) test loops the received signal on a DTE interface back to the DTE without affecting the operation of the remaining ports. Use this test for isolating problems on the DTE interface.

Main Menu → Test → Data Port Physical Tests

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



98-16190

CAUTION:

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

Send Line Loopback

The remote Line Loopback (LLB) up and down codes are in-band codes that allow control of a remote device. The LLB Up code invokes a line loopback in the remote unit while the LLB Down code terminates the remote line loopback. Network loopbacks are defined in AT&T TR 62411.

A remote LLB cannot be started when one of the following tests is active:

- Any Loopback on the same interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) and assigned to this network interface.
- Data Channel Loopback on the frame relay link on this network interface.

► Procedure

To start and stop a Line Loopback:

1. Follow this menu selection sequence:
Main Menu → Test → Network Physical Tests
2. Select the **Up** code in the Send Line Loopback row to put a remote device in loopback.
3. To start the test, highlight **Send** under Command in the Send Line Loopback row and press Enter. The code is sent for up to 10 seconds, or until an acknowledgement is received from the remote end. The length of time that the test has been running is shown in the Results column.
4. To stop the test, send the **Down** code to take the remote device out of loopback.

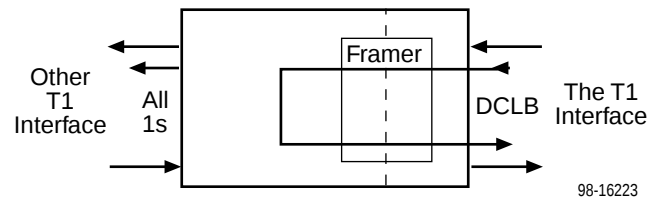
Data Channel Loopbacks on a Frame Relay Link

A network-initiated Data Channel Loopback (DCLB) loops data over the frame relay link (DS0s) received on the network interface through the FrameSaver unit's framing circuitry and back to the same interface.

A DCLB can be controlled over the frame relay link using one of the following in-band methods:

- V.54 Loopback.
- ANSI T1.403 Annex B Fractional T1 (FT1) Channel Loopback.

The frame relay service provider can use DCLB to verify the integrity of the frame relay circuit.



CAUTION:

V.54 and FT1 Loopbacks may affect operation of frame relay PVCs assigned to the selected port. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

Send Remote Line Loopback

The remote Line Loopback (LLB) up and down codes are in-band codes that allow control of a remote device. The LLB Up code invokes a line loopback in the remote unit while the LLB Down code terminates the remote line loopback. Network loopbacks are defined in AT&T TR 62411.

A remote LLB cannot be started when one of the following tests is active:

- Any Loopback on the same interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) and assigned to this network interface.
- Data Channel Loopback on the frame relay link on this network interface.

► Procedure

To start and stop a Remote Line Loopback:

1. Follow this menu selection sequence:
Main Menu → Test → [Network Physical Tests/PRI Physical Tests]
2. Select the desired network interface (shown in the screen title).
3. Select the **Up** code in the Remote Line Loopback row to put a remote device into loopback.
4. To start the test, highlight **Send** under Command in the Remote Line Loopback row and press Enter. The code is sent for up to 10 seconds, or until an acknowledgement is received from the remote end. The length of time that the test has been running is shown in the Results column.
5. To stop the test, send the **Down** code to take the remote device out of loopback.

Send and Monitor Pattern Tests

The pattern tests enable a FrameSaver unit to either send or monitor a known bit pattern. These tests generate industry-standard bit patterns that can be used to determine whether information is being correctly transmitted across a circuit.

The following test patterns are available:

— QRSS	— 511
— All-zeros	— 2047
— All-ones	— $2E15-1$ ($2^{15}-1$)
— 1-in-8	— $2E20-1$ ($2^{20}-1$)
— 3-in-24	— User-defined 2-byte test pattern (a0a0)
— 63	

A Send Pattern test cannot be started when the following tests are running:

- Any Loopback on the same interface.
- Send Pattern Test on any port assigned to this network interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) and assigned to this network interface.

► Procedure

To send and monitor a Pattern Test:

1. Follow this menu selection sequence:
Main Menu → Test → [Network Physical Tests/DSX-1 Physical Tests]
2. Select the desired pattern in the Send or Monitor field. If sending/monitoring a user-defined pattern, enter the the desired 2-byte hexadecimal value in the field next to Send or Monitor.

When sending a pattern, the InjectERR function key appears. Use InjectERR if you want to inject a bit error in the transmitted bit pattern.
3. To send a pattern, highlight the **Send** command to send a pattern and press Enter.

To monitor the test, highlight the **Start** command and press Enter.

The length of time that the test has been running is shown in the Result column. An error count is also displayed. When monitoring a pattern, the ResetMon function key appears. ResetMon resets the error count to zero.
4. To stop the test, press Enter to send the **Stop** command. Start reappears and the status of the test changes back to Inactive.

IP Ping Test

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

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

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

► Procedure 1

To ping any far-end FrameSaver unit:

1. Select the IP Ping test.
Main Menu → Test → IP Ping
2. Enter the IP Address of the device the ping is being sent to, then select Start.

NOTE:

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

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

7

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
- SNMP polling and reporting
- Web-based diagnostic tests: end-to-end, PVC loopbacks, connectivity, and physical interface tests
- Basic device configuration, including RMON alarm and threshold configuration
- ISDN backup support
- Automatic SLV device and PVC discovery of SLV devices with their SLV Delivery Ratio configuration option enabled
- The maintenance scheduling feature allows for the scheduling of multiple periodic maintenance periods, and provides a record of all scheduled maintenance periods – past, present, and future.

- Easy firmware downloads to an entire network or parts of the network
- 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 **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

8

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

- *Preparation*
- *Configuring NetScout Manager Plus*
 - *Adding FrameSaver SLV Units to the NetScout Manager Plus Network*
 - *Verifying Domains and Groups*
 - *Correcting Domains and Groups*
 - *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*
- *Statistical Windows Supported*

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

Preparation

Before getting started, 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.
- Configure agent properties.
- Verify and correct domains and groups.
- Monitor the agent and DLCIs.

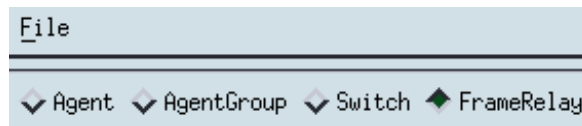
Refer to the NetScout documentation for additional information about accessing and managing the FrameSaver SLV unit through NetScout Manager Plus, refer to the:

- *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

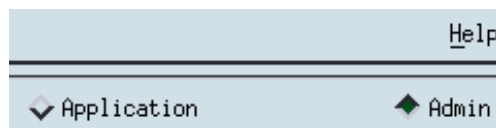
► Procedure

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
 - Enter 1 for the frame relay logical interface to be monitored.
 - 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.

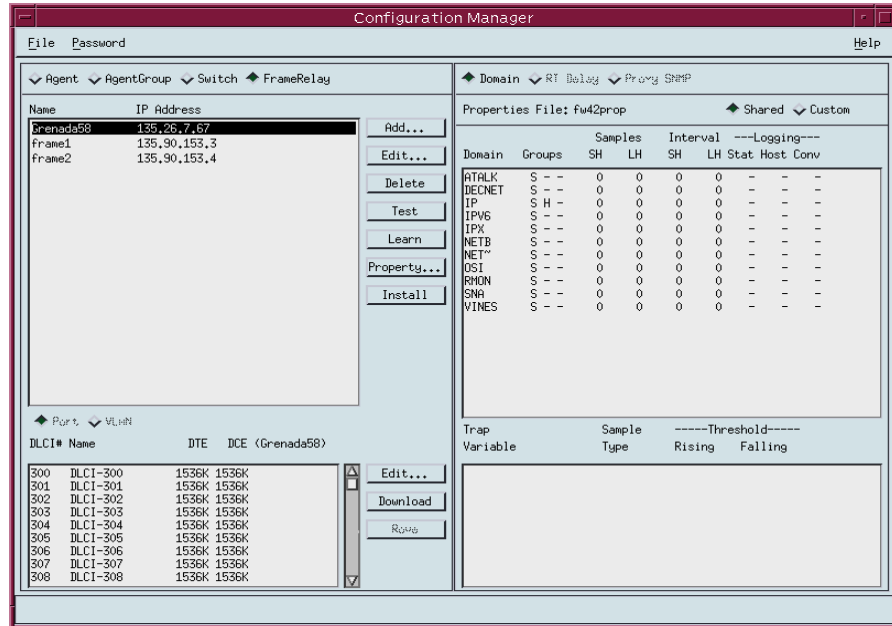
The frame relay agent just entered appears in the agent list box, with its DLCIs in the DLCI list box at the bottom of the screen.
8. Select the Test button (fourth button down, center of the screen) to make sure you can communicate with the agent.

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

Verifying Domains and Groups

► 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	— NEWVINES

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.

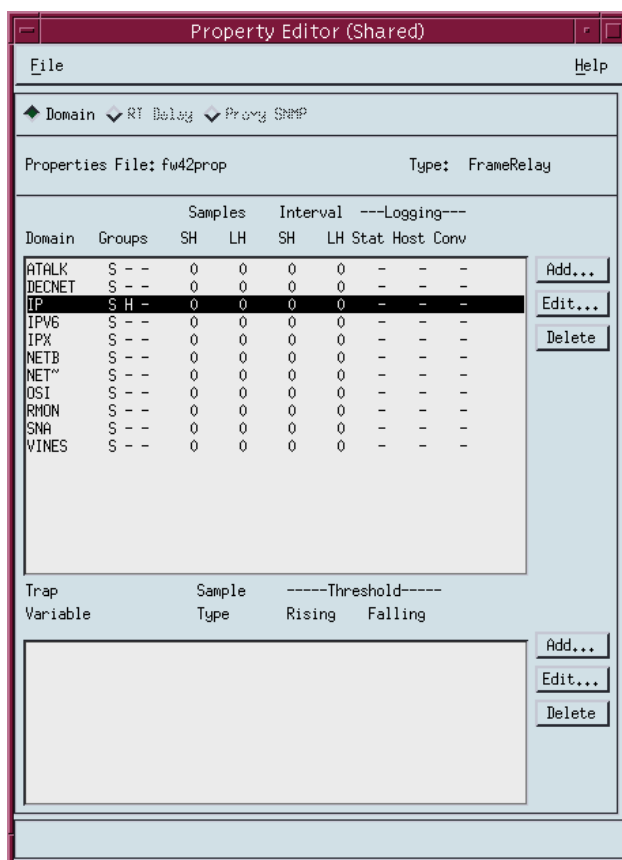
Correcting Domains and Groups

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

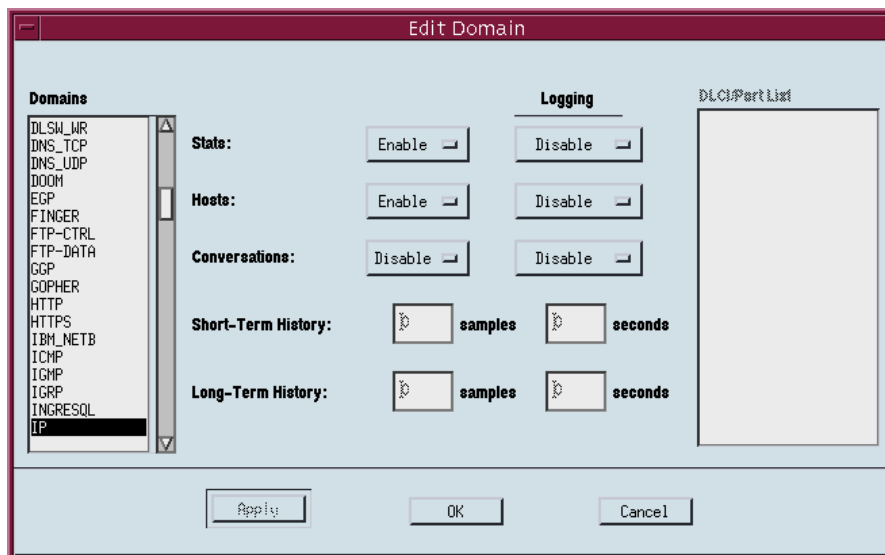
1. Select the the Property... button (down the center of the Configuration Manager main window). The Property Editor window opens.



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.

- 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.



- 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.

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

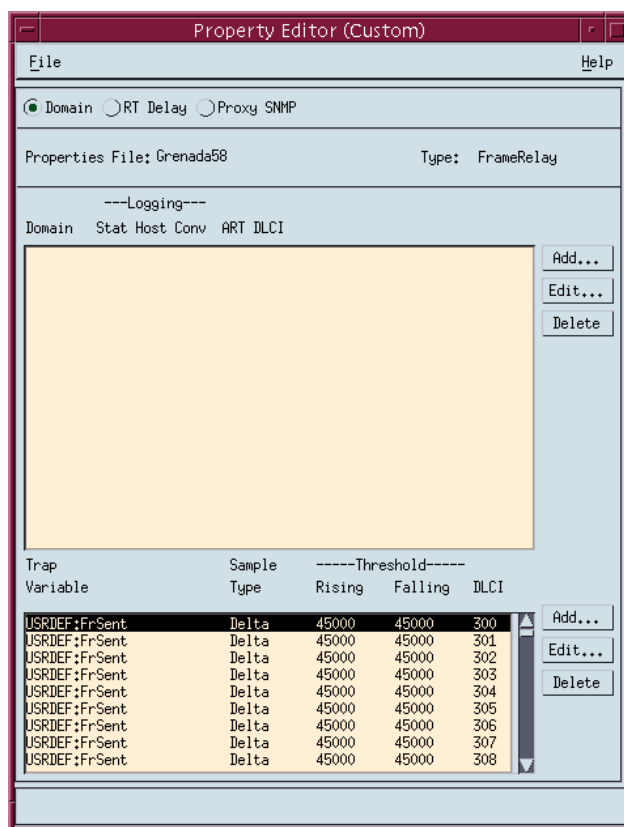
1. Open a terminal window and go to **`$NSHOME/usr`**.
2. Type **`eztrap -i filename.fct -o agentname.fct agentname`** and press Enter to run the eztrap utility to create alarm threshold values across all DLCIs for the copied .fct file.
The message **`eztrap done`** appears when the .fct file is transferred.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

Edit Trap

Domain: USRDEF DLCI: 300

Stats Type: Ethernet Stats

Trap Variable: Drop Events

Key1: 10

Key2: 300

Type: ☐ Absolute ☒ Delta
☒ Rising ☐ Falling ☐ Both

Rising	Falling
Threshold: 45000	Threshold: 45000
Severity: 1	Severity: 1
Script: ...	Script: ...
Description: SLV Frames Snt Rising Thresh	Description: Falling Threshold Reached
Community: public	Community: public
Trap Number: 1	Trap Number: 2
Check every: 30	seconds

ID: 6

OK Cancel

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.

Add Trap

Domain: ... DLCI: ...

State Type: ...

Trap Variable: ...

Key1:

Key2:

Type: ☒ Absolute ☐ Delta
☐ Rising ☐ Falling ☒ Both

	Rising	Falling
Threshold:		
Severity:		
Script:	...	...
Description:		
Community:		
Trap Number:		
Check every:		

seconds

ID:

OK Cancel

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 101015001 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 "**1.3.6.1.2.1.10.32.2.1.6.101015001.301**"

The only valid interface number for a FrameSaver 9126 or 9128 is 101015001.

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 Defaults*, 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

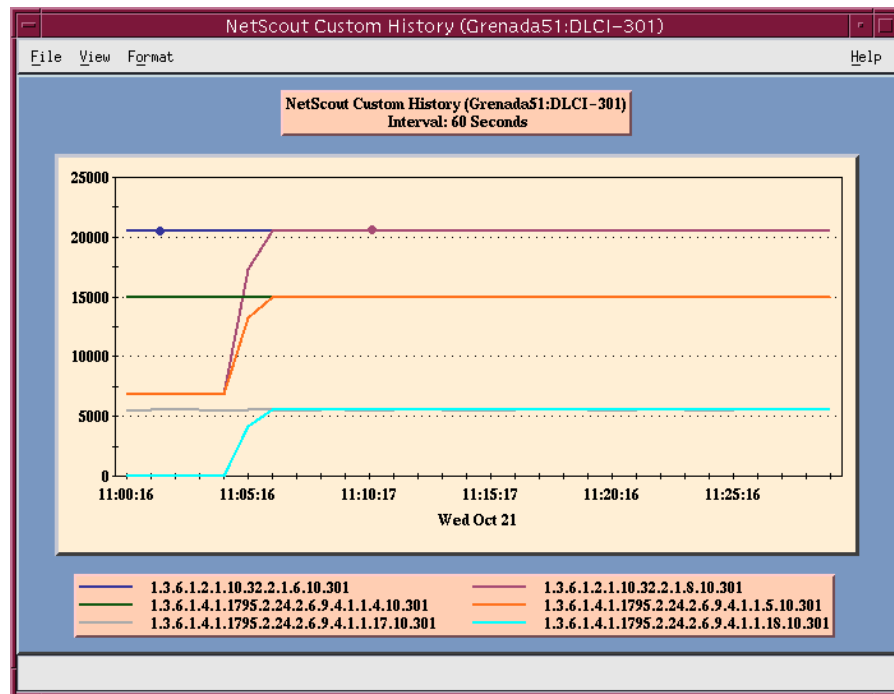
Once the monitoring variables have been defined, a problem DLCI can be monitored.

► Procedure

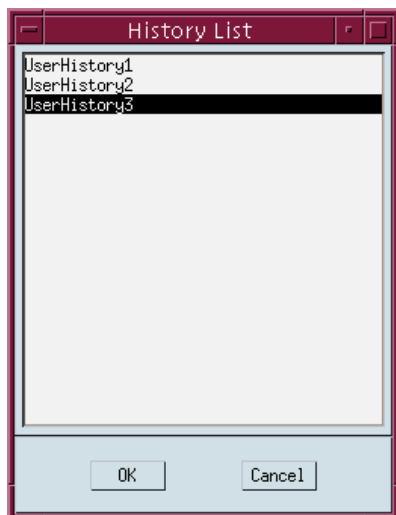
To monitor user history data:

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.

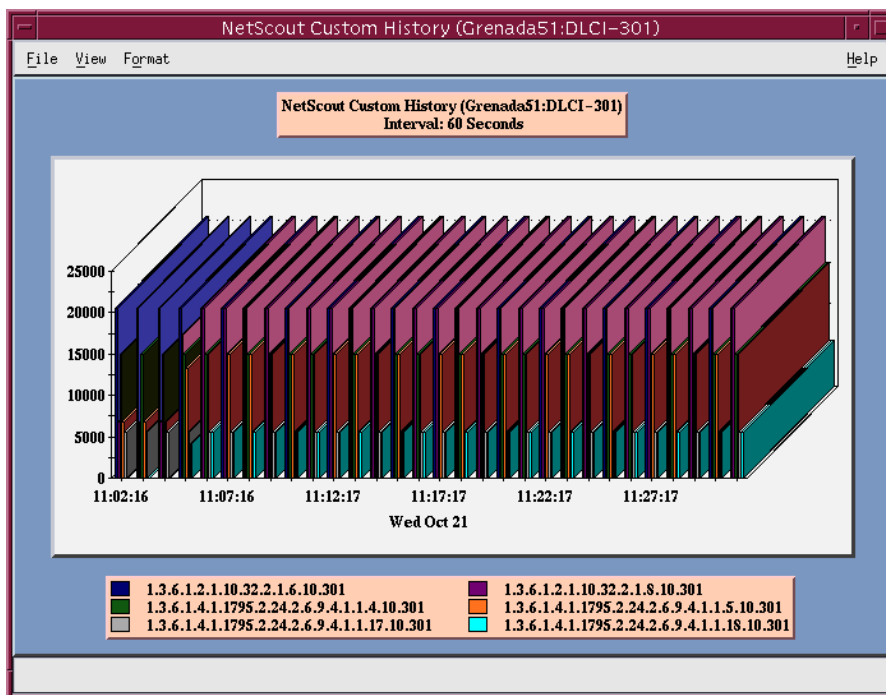
Adjust the size of the window so the entire report can be viewed.



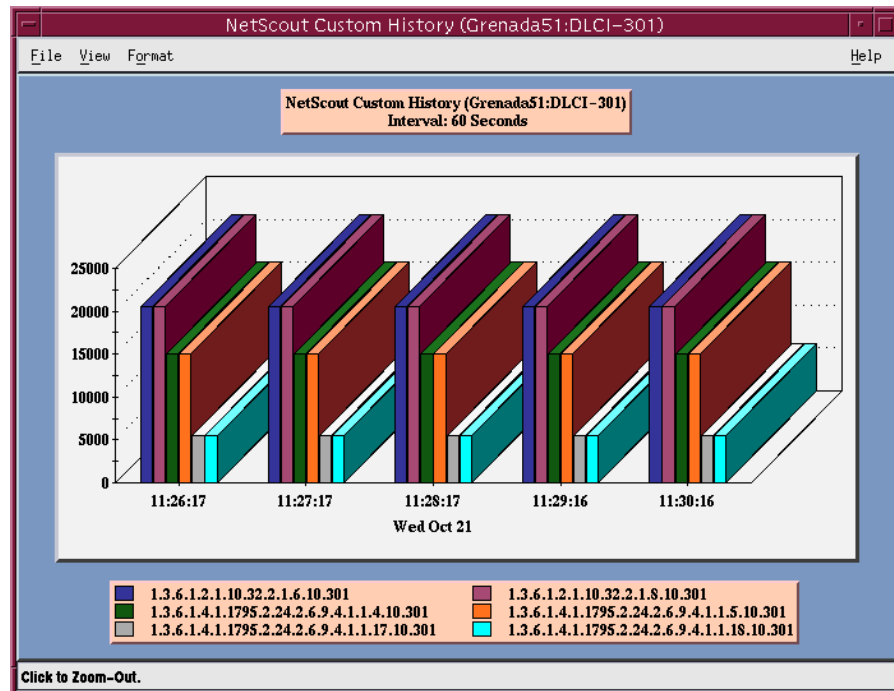
5. Select History List from the View menu. The History List window opens. The newly defined user history variables should appear on this list.



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 Defaults*, to identify OID information being shown.

Monitoring the Agent Using NetScout Manager Plus

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.

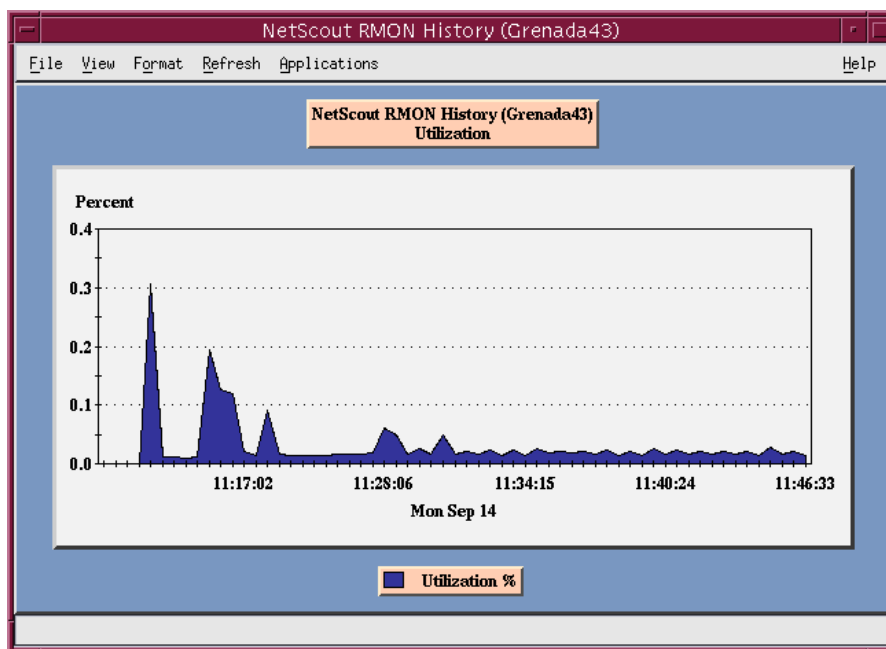
NOTE:

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

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

9

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 9-9). 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 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 9-9, 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:

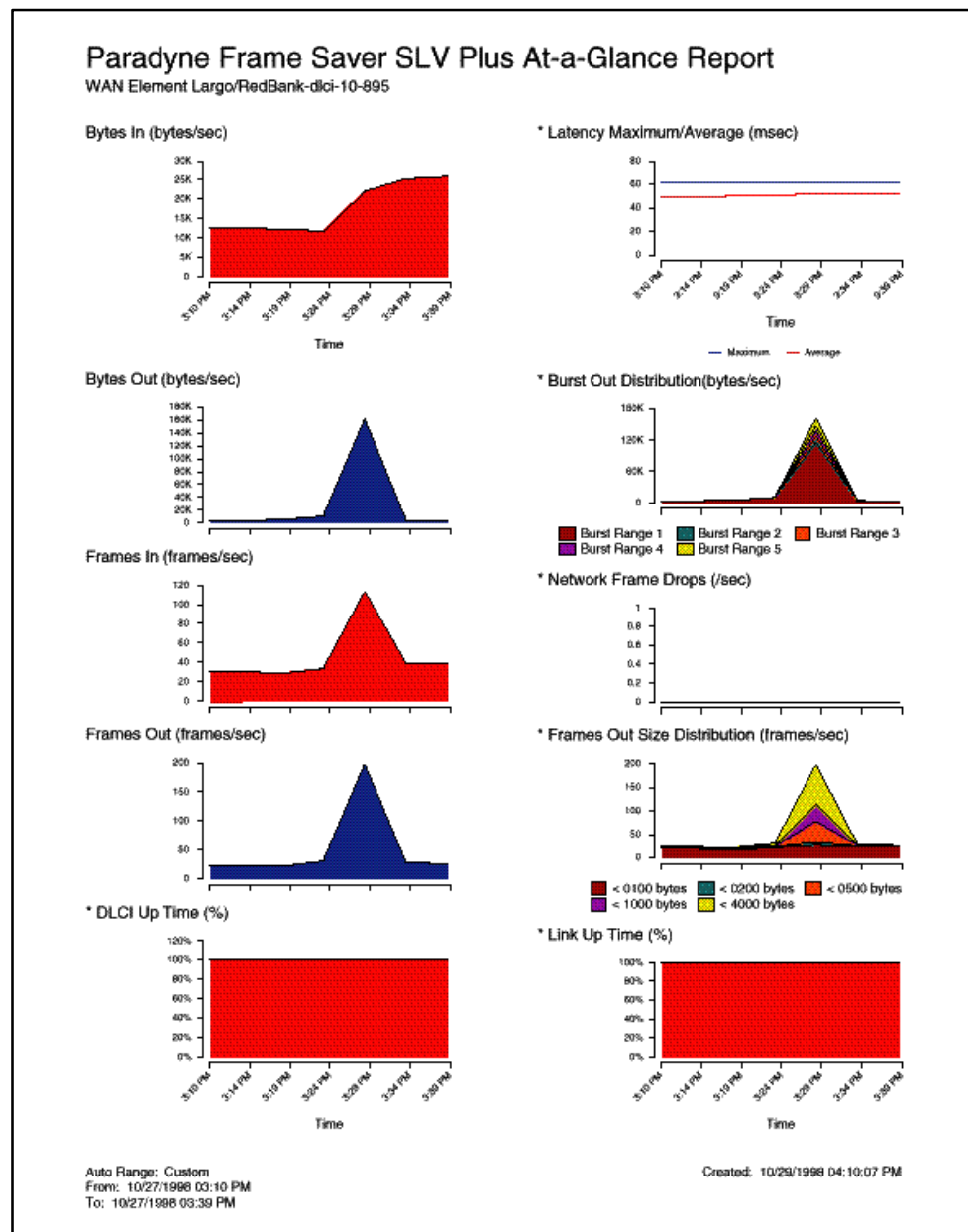
- **Exception Reports** – Provide summary and detail information that identifies DLCIs with the highest incidence of errors, high bandwidth utilization, and trends.

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 9-9](#) 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.

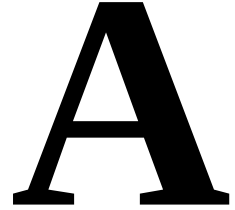


- **Trend Reports** – Perform trend analysis on up to ten specified variables for DLCIs. Variables other than bandwidth can be selected for a trend report (e.g., burst octets), but a bandwidth trend report should be generated when investigating problems that appear on Exceptions Reports, Supplemental 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.

Menu Hierarchy

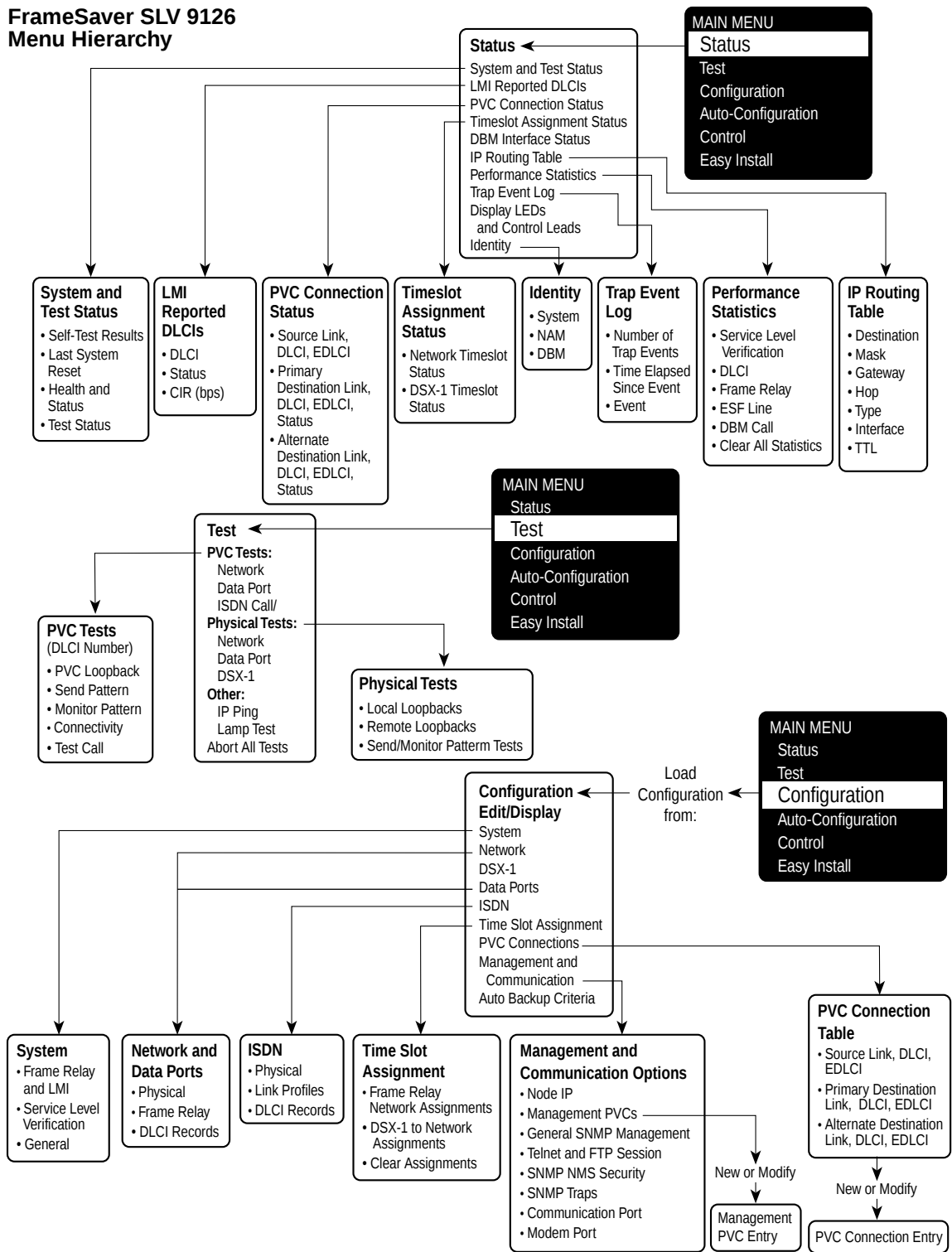


Menus

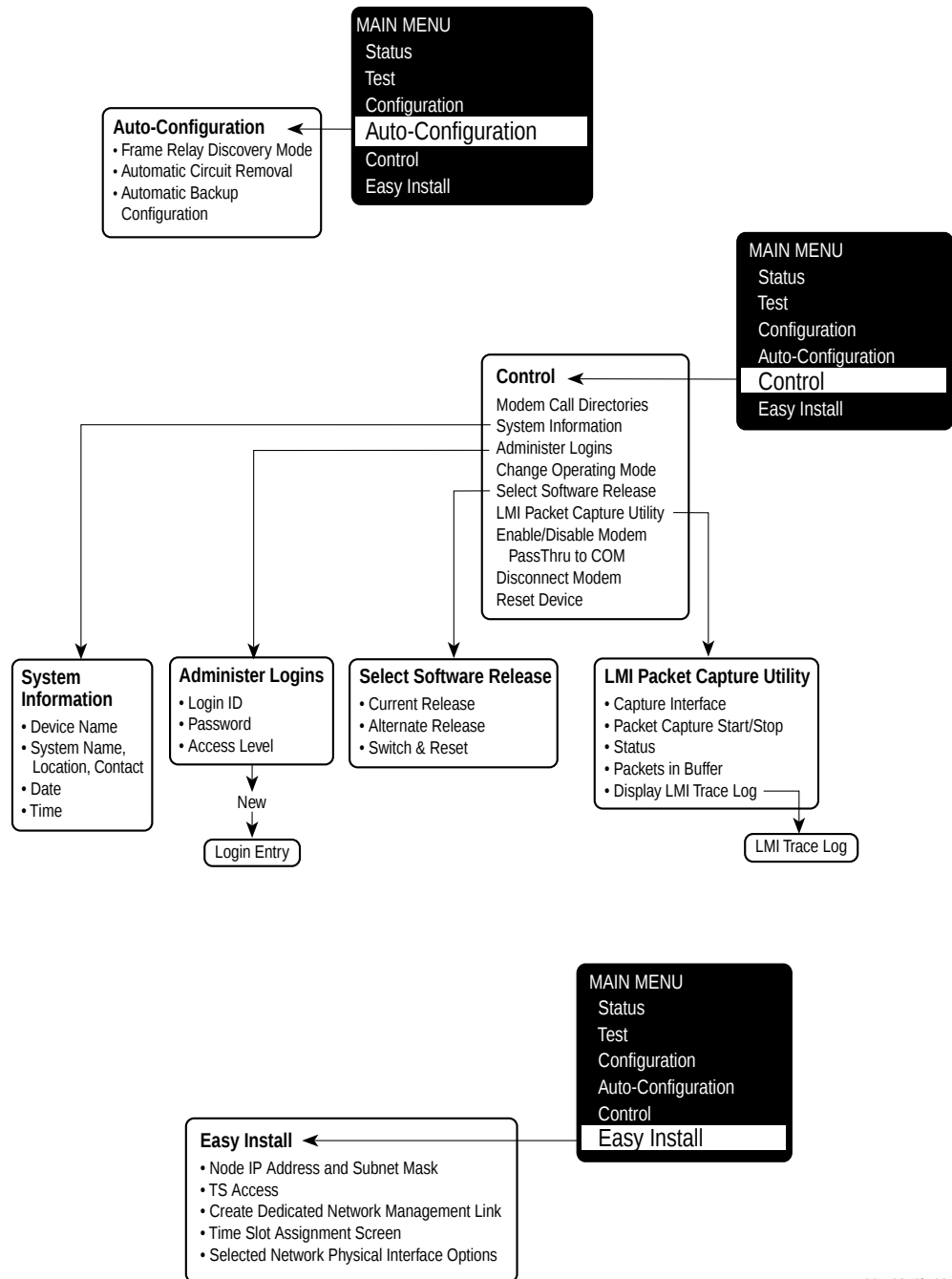
The following is a graphical representations of the FrameSaver SLV unit's menu organization. The following menu structures are shown:

- [FrameSaver SLV 9126 Menu Hierarchy](#) (see page A-2).
- [FrameSaver SLV 9128 and 9128-II Menu Hierarchy](#) (see page A-4).

FrameSaver SLV 9126 Menu Hierarchy

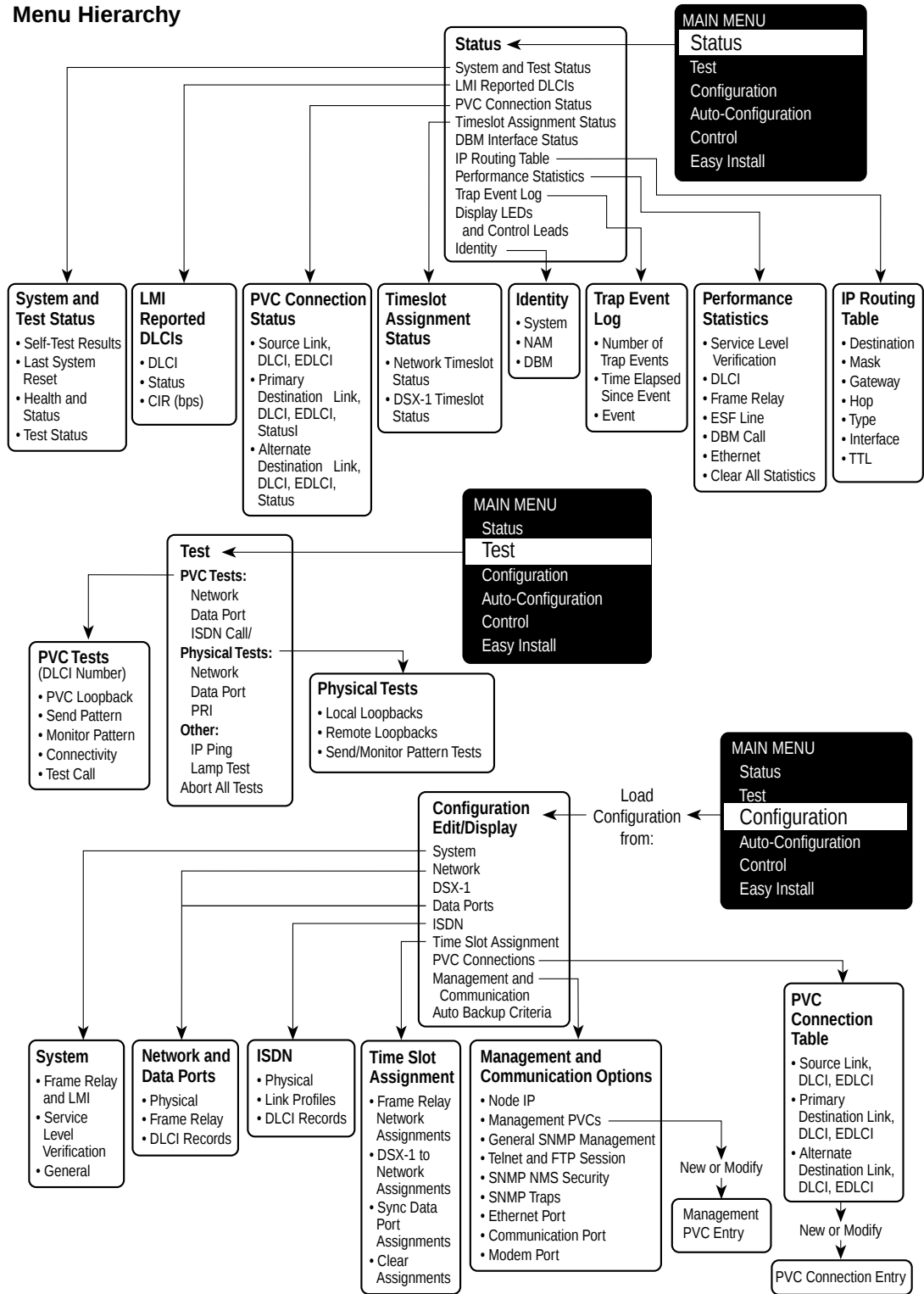


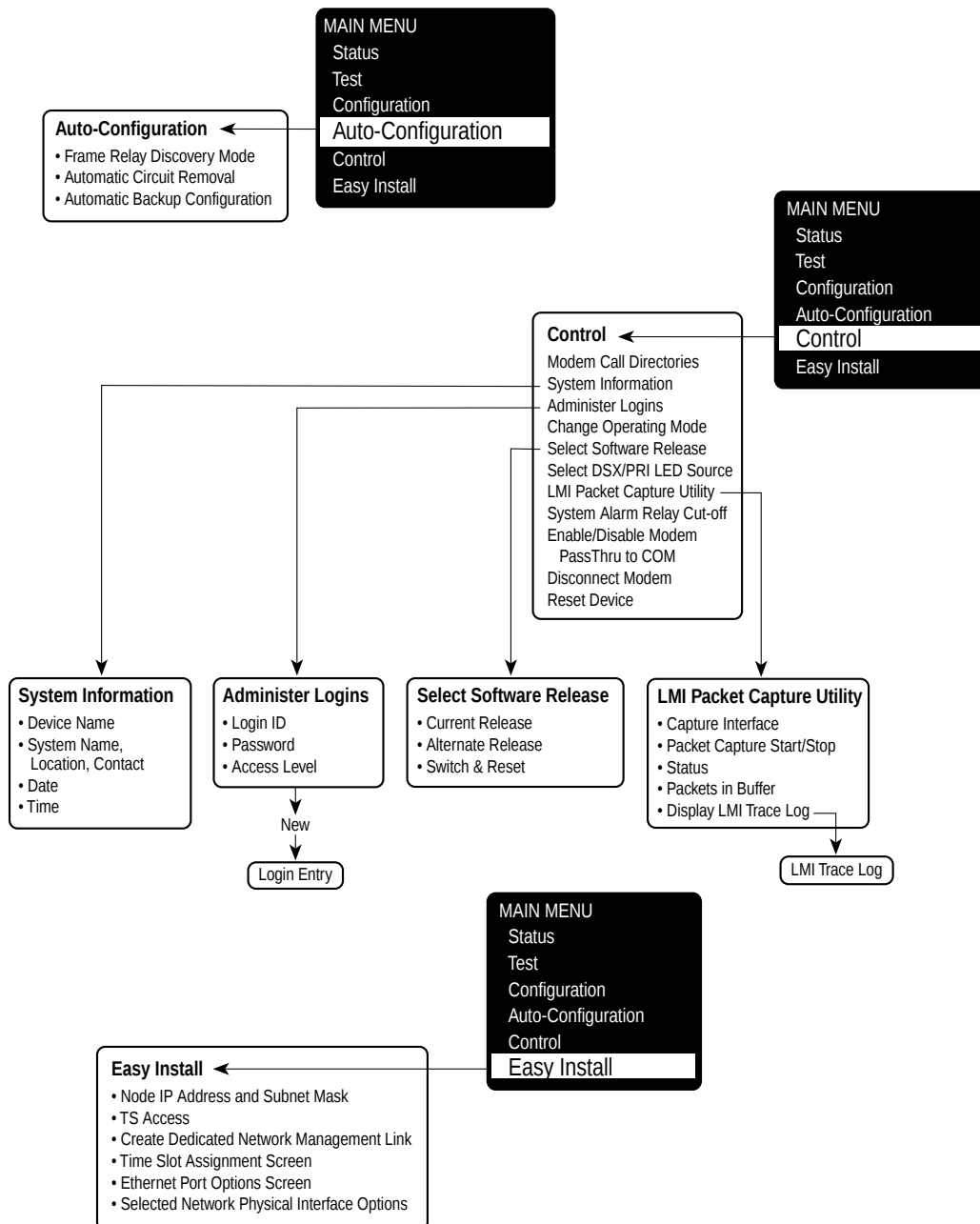
00-16212a-02



00-16212b-02

FrameSaver SLV 9128 and 9128-II Menu Hierarchy





00-16756b

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*
 - *Traps: dialControl*
- *RMON Alarm and Event Defaults*
 - *Physical Interface Alarm Defaults*
 - *Frame Relay Link Alarm Defaults*
 - *DLCI Alarm Defaults – Paradyne Area*
 - *DLCI Alarm Defaults – NetScout Area*
- *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 SNMP protocol.

The following MIBs are supported:

- MIB II (RFC 1213 and RFC 1573)
- Frame Relay DTEs MIB (RFC 2115)
- DS1/E1 MIB (RFC 1406)
- RS-232-Like MIB (RFC 1659)
- Frame Relay Service MIB (RFC 1604)
- Enterprise MIB
- Dial Control MIB using SMIv2 (RFC 2128)
- 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 object identifier and system description for the System Group for the FrameSaver 9126 or 9128 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 unit:

PARADYNE T1 FrameSaver SLV; Model: *[9126/9128]*; S/W Release: *(MM.mm.bb [Major.minor.build] format)*; NAM CCA number: *(hardware version in hhhh-hhh format)*; Serial number: *sssssss*

FrameSaver Unit's sysObjectID (system 2)

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

FrameSaver SLV 9126: 1.3.6.1.4.1.1795.1.14.2.4.4.7

FrameSaver SLV 9128: 1.3.6.1.4.1.1795.1.14.2.4.4.8

FrameSaver SLV 9128-II: 1.3.6.1.4.1.1795.1.14.2.4.4.13

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 (1 of 3)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Physical Layer			
Network T1	T1 network interface	Network T1; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101001001
DSX-1 T1	DSX-1 interface	DSX-1 T1; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101002001
Sync Data Port S01P1	Synchronous Data Port-1	Synchronous Data Port, Slot: 1, Port: 1; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101003001
Sync Data Port S01P2	Synchronous Data Port-2 (if applicable)	Synchronous Data Port, Slot: 1, Port: 2; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101003002

Table B-1. Paradyne Interface Objects Information (2 of 3)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Physical Layer (cont'd)			
COM	Communications port	COM Port; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101004001
Modem	Modem port	Modem Port; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101005001
ISDN BRI DBM	ISDN BRI DBM interface (if applicable)	ISDN BRI DBM; T1 FR NAM; Child Card: ISDN-BRI DBM; S/W Release: <i>MM.mm.bb</i> ; Hardware Version: <i>hhhh-hhh</i>	101110001
ISDN PRI DBM	ISDN PRI DBM interface (if applicable)	ISDN PRI DBM; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: <i>MM.mm.bb</i> ; Hardware Version: <i>hhhh-hhh</i>	101111001
Frame Relay Logical Layer			
FR Bundle	Multilink Frame Relay (MFR) Bundle	FR Bundle, Profile: <i>[Link Name]</i> ; Hardware Version: <i>hhhh-hhh</i>	9126: 101025001 to 101025051 9128: 101025001 to 101025120
FR UNI	Frame relay logical link on the T1 network interface	<i>For the DTE side:</i> Network T1 of FR DTE; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101015001
		<i>For the DCE side:</i> Network T1 of FR SERVICE; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	
	Frame relay logical link on the Sync Data Port-1	<i>For the user side:</i> Synchronous Data Port of FR DTE, Slot: <i>s</i> , Port: 1; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101016001
		<i>For the network side:</i> Synchronous Data Port of FR SERVICE, Slot: <i>s</i> , Port: 1; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	

Table B-1. Paradyne Interface Objects Information (3 of 3)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Frame Relay Logical Layer (cont'd)			
FR UNI	Frame relay logical link on the Sync Data Port-2 (if applicable)	<i>For the user side:</i> Synchronous Data Port of FR DTE, Slot: s, Port: 2; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	101016002
		<i>For the network side:</i> Synchronous Data Port of FR SERVICE, Slot: s, Port: 2; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	
	Frame relay logical link on BRI (if applicable)	<i>For the user side:</i> ISDN BRI DBM of FR DTE; Profile: <i>[Link Name]</i> ; T1 FR NAM; Child Card: ISDN-BRI DBM; S/W Release: <i>MM.mm.bb</i> ; Hardware Version: <i>hhhh-hhh</i>	101018001 101018002
		<i>For the network side:</i> ISDN BRI DBM of FR SERVICE; Profile: <i>[Link Name]</i> ; T1 FR NAM; Child Card: ISDN-BRI DBM; S/W Release: <i>MM.mm.bb</i> ; Hardware Version: <i>hhhh-hhh</i>	
	Frame relay logical link on PRI (if applicable)	<i>For the user side:</i> ISDN PRI DBM of FR DTE; Profile: <i>[Link Name]</i> ; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: <i>MM.mm.bb</i> ; Hardware Version: <i>hhhh-hhh</i>	101017001 to 101017024
		<i>For the network side:</i> ISDN PRI DBM of FR SERVICE; Profile: <i>[Link Name]</i> ; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: <i>MM.mm.bb</i> ; Hardware Version: <i>hhhh-hhh</i>	

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 (1 of 2)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Frame Relay Logical Layer			
Frame Relay 1 Network	Frame relay logical link on the network interface	<i>For the DTE side:</i> RMON (IN/OUT); Network T1 of FR DTE; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	1
		<i>For the DCE side:</i> RMON (IN/OUT); Network T1 of FR SERVICE; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	
Frame Relay 3 Sync Data Port 1	Frame relay logical link on Synchronous Data Port-1	<i>For the user side:</i> RMON (IN/OUT); Synchronous Data Port of FR DTE, Slot: <i>s</i> , Port: 1; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	3
		<i>For the network side:</i> RMON (IN/OUT); Synchronous Data Port of FR SERVICE, Slot: <i>s</i> , Port: 1; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	
Frame Relay 4 Sync Data Port 2	Frame relay logical link on Synchronous Data Port-2	<i>For the user side:</i> RMON (IN/OUT); Synchronous Data Port of FR DTE, Slot: <i>s</i> , Port: 2; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	4
		<i>For the network side:</i> RMON (IN/OUT); Synchronous Data Port of FR SERVICE, Slot: <i>s</i> , Port: 2; T1 FR NAM; Hardware Version: <i>hhhh-hhh</i>	

Table B-2. NetScout Interface Objects Information (2 of 2)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
RMON Logical Layer			
RMON Frame Relay Logical Interfaces	These values are calculated. ■ For the DTE: $(\text{ifIndex} - 1) * 2 + 17$ ■ For the DCE: DTE calculated value +1	IN – RMON (IN); [<i>ifName of the interface</i>]	17–48
		OUT – RMON (OUT); [<i>ifName of the interface</i>]	
RMON Virtual Interfaces	These values are calculated based on the probe's internal circuit index: circuit index +65.	ALL – VIRTUAL PVC [<i>interface number</i>] [<i>DLCI number</i>] ALL	65–512
RMON Virtual Logical Interfaces	These values are calculated. ■ For the DTE: (virtual interface $\text{ifIndex} - 65) * 2 + 513$ ■ For the DCE: DTE calculated value +1	IN – VIRTUAL PVC [<i>interface number</i>] [<i>DLCI number</i>] DTE	513–1023
		OUT – VIRTUAL PVC [<i>interface number</i>] [<i>DLCI number</i>] 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 "\$circuitId" only appears when a DLCI is associated with the trap.
- \$circuitId is the name given to the circuit. It can be an empty string, or a 1–64 byte string within quotes (e.g., "Chicago to New York"), and only appears when a DLCI with "circuitID" is associated with the trap.
- \$linkName is the name given to the link. Frame relay \$linkName only appears when a frame relay link has been named and is associated with the trap.
- \$ifName is the string returned for the SNMP ifName variable.

Examples:

'DLCI 100 "Chicago to New York" of Network T1 frame relay link'

In this example, a DLCI and a frame relay link are associated with the trap.

Typically, the \$circuitId is a coded string encoded by the network service provider. The following shows an example.

'DLCI 100 "cc0402–dec0704.RG21" of Network T1 frame relay link'

The unit supports the following traps:

- warmStart
- authenticationFailure
- linkUp and linkDown
- enterprise-Specific
- RMON-Specific
- dialControl

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. <i>String:</i> '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 (1 of 2)

Trap	What It Indicates	Possible Cause
authenticationFailure	Access to the FrameSaver unit was attempted and failed.	■ Bad password on COM port terminal. <i>String:</i> 'Unauthorized access attempted from COM port.' ■ Bad password on modem port terminal. <i>String:</i> 'Unauthorized access attempted from modem port.' ■ Bad password through telnet. <i>String:</i> 'Unauthorized access attempted from telnet user at \$ipAddress.' ■ SNMP bad community, unauthorized IP address, or unauthorized operation. <i>String:</i> 'Unauthorized access attempted from SNMP user at \$ipAddress.'

Table B-4. authenticationFailure Trap (2 of 2)

Trap	What It Indicates	Possible Cause
authenticationFailure	Variable-Binding	■ An ISDN backup call has been received, but the call was rejected. <i>String:</i> 'Bad Caller ID \$phone.' (\$phone is either a phone number or "no number.")
	devLastTrapString (devHealthAndStatus.mib)	

Traps: linkUp and linkDown

These traps are supported on the following interfaces:

- Network, DSX-1, 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		
T1 Network, DSX-1, PRI (Supported by the media-specific DS1 MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the interface. Alarm conditions include: – Loss of Signal (LOS) or far-end loss of signal – Out of Frame (OOF) – Alarm Indication Signal (AIS) – Excessive Error Rate (EER) – Yellow Alarm <i>Strings:</i> ‘\$ifString down.’ No alarms exist. (e.g., ‘Network T1 down due to yellow alarm.’) ‘\$ifString administratively shutdown.’ (Due to an intentional shutdown.) ■ linkUp – No alarms on the interface. <i>String:</i> ‘\$ifString up.’
Synchronous Data Port (Supported by the media-specific RS232-like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the port. Alarm conditions include: – DTR off ¹ – RTS off ² – ‘ – Not DTR or RTS, but link is down. <i>String:</i> ‘\$ifString \$alarmString down.’ (e.g., ‘Sync Data Port S01P1 DTR and RTS down.’) ‘\$ifString administratively shutdown.’ (Due to an intentional shutdown.) ■ linkUp – No alarms on the port. <i>String:</i> ‘\$ifString up.’
¹ The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state. ² The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state.		

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

Interface	Variable-Bindings	Possible Cause
Physical Sublayer (Cont'd)		
BRI (Supported through ifIndex – RFC 1573.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the interface. <i>Strings:</i> '\$ifString down.' No alarms exist on the link. '\$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the interface. <i>String:</i> '\$ifString up.'
Logical Link Sublayer		
T1 Network, BRI, PRI, Synchronous Data Port Service Side of the Frame Relay UNI (Supported by the media-specific Frame Relay Services MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured,³ or Frame Relay link is disabled. <i>Strings:</i> '\$ifString down.' No alarms exist on the link due to LMI. '\$ifString LMI down.' No alarms exist on the link. (e.g., 'Sync Data Port S01P1 frame relay link "Port-1" LMI down.') '\$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. <i>String:</i> '\$ifString up.'
T1 Network, BRI, PRI, Synchronous Data Port DTE Side of the Frame Relay UNI (Supported by the media-specific Frame Relay DTE's MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured,³ or Frame Relay link is disabled. <i>Strings:</i> '\$ifString LMI down.' '\$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. <i>String:</i> '\$ifString up.'
³ If the LMI Protocol is not configured, a linkUp/linkDown trap is based solely upon whether the interface is enabled or disabled.		

Traps: enterprise-Specific

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

Table B-7. enterprise-Specific Traps and Variable-Bindings (1 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseCIR-Change(15)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciCIR (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib)	CIR has changed due to the LMI report. LMI Protocol is set to Standard and the network's CIR changed. <i>String:</i> '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. <i>String:</i> '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. <i>Strings:</i> '\$ifString deleted by Auto-DLCI delete.'
enterpriseDLCI-Down(11)		DLCI Status is set to Inactive; the DLCI is down. <i>Strings:</i> '\$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. <i>String:</i> '\$ifString up.'

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

Trap	Variable-Bindings	Possible Cause
enterpriseMissedSLV-Down(16)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciMissed-SLVs (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib.)	Received SLV communications have been missed; SLV Timeout Error Event Threshold has been exceeded. <i>String:</i> '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. <i>String:</i> 'SLV up on \$ifString because SLV communication was reestablished. Total SLV packets lost is \$numLost.'
enterprisePrimary-ClockFail(1)	■ devLastTrapString (devHealthAndStatus.-mib)	Operating software has detected that the primary clock source has failed. <i>String:</i> 'Primary clock failed.'
enterprisePrimary-ClockFailClear(101)		Operating software has detected that the primary clock source is operational again. <i>String:</i> 'Primary clock restored.'
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. <i>String:</i> 'RMON database reset to defaults.'
enterpriseSecondary-ClockFail(4)	■ devLastTrapString (devHealthAndStatus.-mib)	Operating software has detected that the secondary clock source has failed. <i>String:</i> 'Secondary clock failed.'
enterpriseSecondary-ClockFailClear(104)		Operating software has detected that the secondary clock source is operational again. <i>String:</i> 'Secondary clock restored.'

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

Trap	Variable-Bindings	Possible Cause
enterpriseSelfTest-Fail(2)	devLastTrapString (devHealthAndStatus.-mib)	Unit has completed (re)initialization and a hardware failure was detected. <i>String:</i> '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)	At least one test has been started on an interface or virtual circuit. <i>String:</i> '\$testString test started on \$ifString.' (e.g., 'DTE Loopback test started on Sync Data Port S01P1.')
enterpriseTest-Stop(105)	For virtual circuits (DLCIs): - devFrExtDlciIfIndex (devFrExt.mib) - devFrExtDlciDlci (devFrExt.mib) - devLastTrapString (devHealthAndStatus.-mib)	All tests have been halted on an interface or virtual circuit. <i>String:</i> '\$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-8. RMON-Specific Traps and Variable-Bindings

Trap	Variable-Bindings	Possible Cause
risingAlarm	■ alarmIndex (RFC 1757) ■ alarmVariable (RFC 1757) ■ alarmSampleType (RFC 1757) ■ alarmValue (RFC 1757) ■ alarmRisingThreshold (RFC 1757) ■ devLastTrapString (devHealthAndStatus.-mib)	Object being monitored has risen above the set threshold. <i>String:</i> 'Change in \$variableName \$typeString threshold of \$alarmRisingThreshold by \$(alarmValue – AlarmRisingThreshold.' (e.g., Octets received on Network T1 frame relay rose to threshold of 1.)'
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. <i>String:</i> 'Change in \$variableName \$typeString threshold of \$alarmFallingThreshold by \$(alarmValue – AlarmFallingThreshold.' (e.g., Octets received on Network T1 frame relay fell to threshold of 1.)'

Trap: dialControl

These traps indicate when an ISDN backup call is initiated or terminated, or when an outgoing call is rejected by the far end device.

Table B-9. dialControl Traps (1 of 2)

Trap	Variable-Bindings	Possible Cause
Standard Dial Control MIB		
dialCtlPeerCall-Information	■ callHistoryPeerId (RFC 2128) ■ callHistoryPeerIfIndex (RFC 2128) ■ callHistoryLogicalIfIndex (RFC 2128) ■ ifOperStatus (RFC 1573) ■ callHistoryPeerAddress (RFC 2128) ■ callHistorySubAddress (RFC 2128) ■ callHistoryDisconnect-Cause (RFC 2128) ■ callHistoryConnectTime (RFC 2128) ■ callHistoryDisconnect-Time (RFC 2128) ■ callHistoryInfoType (RFC 2128) ■ callHistoryCallOrigin (RFC 2128)	A peer-to-peer call has been ended. <i>String:</i> 'Call sequence on \$ifString [using B-Chnl \$channel] terminated due to \$causeString.' The \$causeString is the The B-channel in this example is only provided if it is known. See Table 5-11, Most Recent and Previous Cause Values, in <i>DBM Interface Status of Operation and Maintenance</i> for a list of the \$causeStrings and their cause numbers.
dialCtlPeerCall-Setup	■ callActivePeerId (RFC 2128) ■ callActivePeerIfIndex (RFC 2128) ■ callActiveLogicalIfIndex (RFC 2128) ■ ifOperStatus (RFC 1573) ■ callActivePeerAddress (RFC 2128) ■ callActiveSubAddress (RFC 2128) ■ callActiveInfoType (RFC 2128) ■ callActiveCallOrigin (RFC 2128)	A peer-to-peer call has been sent or received. <i>String:</i> 'Call sequence on \$ifString [using B-Chnl \$channel] initiated [remotely/locally].' The B-channel in this example is only provided if it is known.

Table B-9. dialControl Traps (2 of 2)

Trap	Variable-Bindings	Possible Cause
Dial Control Extension MIB		
dialCtlPeerCall-Rejected	■ callHistoryPeerId (RFC 2128) ■ callHistoryPeerIfIndex (RFC 2128) ■ callHistoryLogicalIfIndex (RFC 2128) ■ callHistoryPeerAddress (RFC 2128) ■ devLastTrapString (devHealthAndStatus.-mib)	A peer-to-peer call was not successful; the call was rejected by the far end. ■ ISDN Call Profile has been disabled. ■ This unit's phone number was not in the far end device's ISDN Call Profile. <i>String:</i> 'Call on \$ifString using B-Chnl \$channel rejected by remote.'

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
65533	Default SLV Rising Event	log-and-trap(4)	0
65534	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 – NetScout Area*

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

Rising Event Operation

If a rising threshold is crossed during the interval shown in a table (e.g., frames dropped by the network), the event is armed and an alarm is generated at the end of the interval. Only one alarm per event per interval is generated. The alarm condition persists until the event has been disarmed (reset).

The event is disarmed when a falling threshold has been crossed and the rising threshold has not been crossed during an interval, allowing the event to return to its original disarmed state.

Physical Interface Alarm Defaults

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

Table B-9. Network Physical Interface Alarm Defaults

Item	Sample Type ¹	MIB/Tag/OID ²	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Unavailable Seconds	D	MIB: DS1/E1 MIB (RFC 1406) Tag: dsx1TotalUASs OID: .1.3.6.1.2.1.10.18.9.1.5.I	900 secs (15 mins)	Rising	1	1
¹ D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB. ² I in the OID = Interface ID of the frame relay link.						

Frame Relay Link Alarm Defaults

These alarms apply to the FrameSaver unit's frame relay link interfaces. They are created during RMON initialization.

Table B-10. Frame Relay Link Alarm Defaults (1 of 2)

Item	Sample Type ¹	MIB/Tag/OID ²	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Invalid Frames	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkRxIIFrames OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.18.I	900 secs (15 mins)	Rising	1	1
Short Frames	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkRxShort OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.6.I	900 secs (15 mins)	Rising	1	1
Long Frames	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkRxLong OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.7.I	900 secs (15 mins)	Rising	1	1
Rx Discards	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkRxDiscards OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.15.I	900 secs (15 mins)	Rising	1	1
Tx Discards	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkTxDiscards OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.14.I	900 secs (15 mins)	Rising	1	1
Rx Total Errors	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkTotRxErrs OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.20.I	900 secs (15 mins)	Rising	1	1
¹ D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB. ² I in the OID = Interface ID of the frame relay link.						

Table B-10. Frame Relay Link Alarm Defaults (2 of 2)

Item	Sample Type ¹	MIB/Tag/OID ²	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Tx Total Errors	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkTotTxErrs OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.19.I	900 secs (15 mins)	Rising	1	1
Rx Overruns	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkRxOverruns OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.28.I	900 secs (15 mins)	Rising	1	1
Tx Underruns	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkTx-Underruns OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.29.I	900 secs (15 mins)	Rising	1	1
Rx Non-octet Aligns	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkRx-NonOctet OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.16.I	900 secs (15 mins)	Rising	1	1
Rx CRC Errors	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkRxCrcErr OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.17.I	900 secs (15 mins)	Rising	1	1
Total LMI Errors	D	MIB: pdn_FrExt.mib (E) Tag: devFrExtLinkTotal-LMIErrs OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.32.I	900 secs (15 mins)	Rising	1	1
¹ D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB. ² I in the OID = Interface ID of the frame relay link.						

DLCI Alarm Defaults – Paradyne Area

These alarms apply to all DLCIs on the network interface and can be created during RMON initialization or when a DLCI is created. They are put into the Paradyne-defined alarm area.

Table B-11. 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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciStsInactive-Secs <i>OID:</i> .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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciMissedSLVs <i>OID:</i> .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	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitReceivedFECNs <i>OID:</i> .1.3.6.1.2.1.10.32.2.1.4. I.D	60 secs (1 min)	Rising	1	1
Rx BECNs	D	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitReceivedBECNs <i>OID:</i> .1.3.6.1.2.1.10.32.2.1.5. I.D	60 secs (1 min)	Rising	1	1
Congested Seconds	D	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciSts-CongestedSecs <i>OID:</i> .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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciNetDropFr <i>OID:</i> .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
¹ D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB. A = Absolute. Indicates that the exact value for the item is contained in the MIB. ² I in the OID = Interface ID of the frame relay link. D = DLCI number.						

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

Item	Sample Type ¹	MIB/Tag/OID ²	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Maximum Latency (FrameSaver 9128 with SLV OS R1.3)	A	MIB: pdn_FrExt.mib (E) Tag: devFrExtLatencyMax OID: .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.I.D	60 secs (1 min)	Rising	0	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.						

DLCI Alarm Defaults – NetScout Area

These alarms can be created during RMON initialization or when a DLCI is created. They are put into the NetScout alarm area. Table B-11 identifies alarm defaults that do not change, and [Table B-12](#) 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 8, *Setting Up NetScout Manager Plus for FrameSaver Devices*.

Table B-12. Static DLCI Alarm Defaults – NetScout Area

Item	Sample Type ¹	MIB/Tag/OID ²	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Current Latency	A	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLatencyLatest <i>OID:</i> .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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLatencyAvg <i>OID:</i> .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	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitReceivedFrames <i>OID:</i> .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	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitSentFrames <i>OID:</i> .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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciTxFrOutCIR <i>OID:</i> .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
Tx CIR Utilization	D	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitSentOctets <i>OID:</i> .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.						

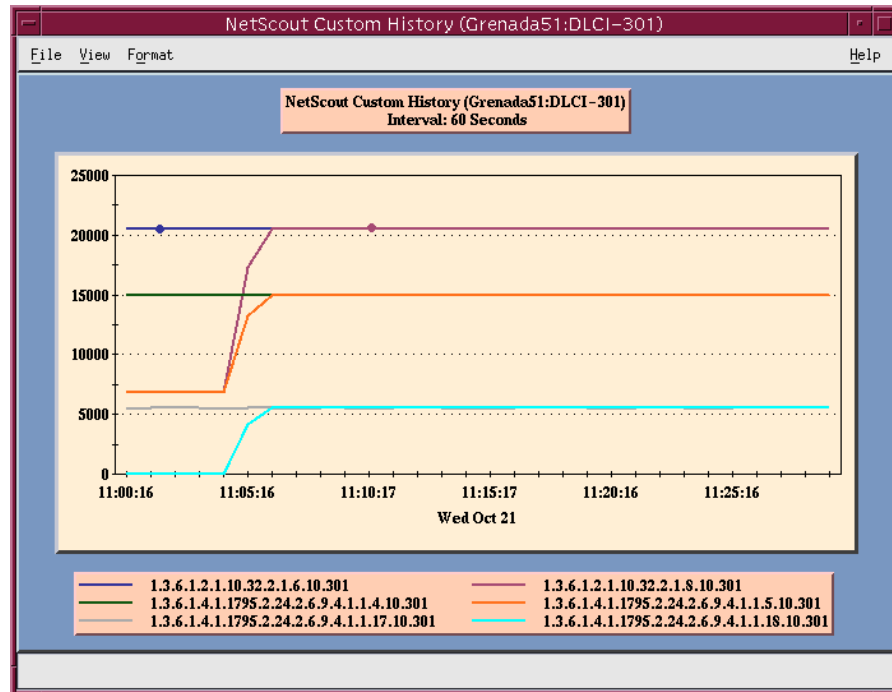
Table B-13. Dynamic DLCI Alarm Defaults – NetScout Area

Item	Sample Type ¹	MIB/Tag/OID ²	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Rx DLCI Link Utilization	D	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitReceivedOctets <i>OID:</i> .1.3.6.1.2.1.10.32.2.1.9.1. D	60 secs. (1 min)	Rising	70% of link capability	65% of link capability
Tx DLCI Link Utilization	D	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitSentOctets <i>OID:</i> .1.3.6.1.2.1.10.32.2.1.7.1. 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 or a log event is sent.

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



See [Table B-14](#) for an RMON history OID cross-reference and [Table B-15](#) for an RMON alarm OID cross-reference.

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

Object ID (OID) ¹	Item	MIB/Tag
.1.3.6.1.2.1.2.2.1. . .		
.1.3.6.1.2.1.2.2.1.5. I	Link Speed	<i>MIB</i> : MIB II (RFC 1573) <i>Tag</i> : ifSpeed
.1.3.6.1.2.1.2.2.1.10. I	All DLCI + LMI Rx Octets	<i>MIB</i> : MIB II (RFC 1573) <i>Tag</i> : ifInOctets
.1.3.6.1.2.1.2.2.1.16. I	All DLCI + LMI Tx Octets	<i>MIB</i> : MIB II (RFC 1573) <i>Tag</i> : ifOutOctets
.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	<i>MIB</i> : FR DTE MIB (RFC 2115) <i>Tag</i> : frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.5. I.D	Rx BECNs	<i>MIB</i> : FR DTE MIB (RFC 2115) <i>Tag</i> : frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.6. I.D	Tx Frames	<i>MIB</i> : FR DTE MIB (RFC 2115) <i>Tag</i> : frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.7. I.D	Tx Octets	<i>MIB</i> : FR DTE MIB (RFC 2115) <i>Tag</i> : frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.8. I.D	Rx Frames	<i>MIB</i> : FR DTE MIB (RFC 2115) <i>Tag</i> : frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.9. I.D	Rx Octets	<i>MIB</i> : FR DTE MIB (RFC 2115) <i>Tag</i> : 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)	<i>MIB</i> : RMON II (RFC 2021) <i>Tag</i> : 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-14. History OID Cross-Reference (2 of 5)

Object ID (OID) ¹	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2. . .		
.1.3.6.1.4.1.1795.2.24.2.6.5.4.8.1.2.I	Unavailable Seconds	MIB: pdn_FrExt.mib (E) Tag: devFreeRunUAS
.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-14. History OID Cross-Reference (3 of 5)

Object ID (OID) ¹	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.41.I.D	Network Frames Dropped In CIR	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciDropOffFrInCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.43.I.D	Network Frames Offered Above CIR	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciRmtOffFrOutCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.45.I.D	Network Frames Lost Above CIR	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciOfferedFrOverEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.61.I.D	Network Frames Dropped Above EIR	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciRxFrNetDrop-OverEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.63.I.D	DLCI EIR	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.2.I.D	DLCI Inactive Seconds	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciStsInactiveSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.8.I.D	Backup Count	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciStsBackupCnt
.1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.9.I.D	Backup Time	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciStsBackupTime
.1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.5.I.D	Average Latency	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.6.I.D	Maximum Latency	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLatencyMax
¹ I = Interface ID of the frame relay link D = DLCI number N = Additional numeric index used by tables, like frame or burst size H = Host control index P = Protocol index T = The time mask		

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

Object ID (OID) ¹	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.8.I.D	Latency Packet Size	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLatencyPacketSz
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.2 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.2.1.2.I.N	Frame Size Upper Limit (1–5)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtFrameSzCount
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1.2.I.D.N	Burst Upper Limit (1–5)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkNoLMISecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.6.I	Rx Short Frames	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxShort
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.7.I	Rx Long Frames	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxLong
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.11.I	LMI Sequence Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkSeqErr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.15.I	Rx Discards	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.17.I	Total Rx CRC Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxCrcErr
¹ I = Interface ID of the frame relay link D = DLCI number N = Additional numeric index used by tables, like frame or burst size H = Host control index P = Protocol index T = The time mask		

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

Object ID (OID) ¹	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. 18.I	Rx Illegal Frames	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxILFrames
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. 19.I	Total Tx Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. 20.I	Total Rx Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. 32.I	Total LMI Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkUtilTxOctets
¹ I = Interface ID of the frame relay link D = DLCI number N = Additional numeric index used by tables, like frame or burst size H = Host control index P = Protocol index T = The time mask		

See Table B-15 on page B-32 for an **RMON alarm OID cross-reference**.

Table B-15. Alarm OID Cross-Reference (1 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.2.1.10.18.9.1. . .		
.1.3.6.1.2.1.10.18.9.1.5.I	Unavailable Seconds	<i>MIB:</i> DS1/E1 MIB (RFC 1406) <i>Tag:</i> dsx1TotalUASs
.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	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.5.I.D	Rx BECNs	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.6.I.D	Frames Sent	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.7.I.D	Tx CIR Utilization	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.7.I.D	Tx DLCI Link Utilization	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.8.I.D	Frames Received	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.9.I.D	Rx DLCI Link Utilization	<i>MIB:</i> FR DTE MIB (RFC 2115) <i>Tag:</i> frCircuitReceivedOctets
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.17.I.D	Tx Frames Exceeding CIR	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciTxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.20.I.D	Frames Dropped by Network	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> frFrExtDlciNetDropFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.23.I. D	Missing Latency Responses	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciMissedSLVs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.6.I.D	Congested Seconds	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciStsCongestedSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.2.I.D	DLCI Inactive Seconds	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtDlciStsInactiveSecs
¹ I = Interface ID of the frame relay link D = DLCI number		

Table B-15. Alarm OID Cross-Reference (2 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.5.I.D	Average Latency	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.7.I.D	Current Latency	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> 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)	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtFrameSzCount
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.6.I	Rx Short Frames	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxShort
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.7.I	Rx Long Frames	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxLong
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.11.I	LMI Sequence Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkSeqErr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.14.I	Tx Discards	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkTxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.15.I	Rx Discards	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.16.I	Rx Nonoctet Aligns	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxNonOctet
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.17.I	Rx CRC Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxCrcErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.18.I	Rx Illegal Frames	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxIIFrames
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.19.I	Tx Total Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.20.I	Rx Total Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.28.I	Rx Overruns	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkRxOverruns
¹ I = Interface ID of the frame relay link D = DLCI number		

Table B-15. Alarm OID Cross-Reference (3 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.29.I	Tx Underruns	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkTxUnderruns
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.32.I	Total LMI Errors	<i>MIB:</i> pdn_FrExt.mib (E) <i>Tag:</i> devFrExtLinkTotalLMIErrs
¹ I = Interface ID of the frame relay link D = DLCI number		

Connectors, Cables, and Pin Assignments

C

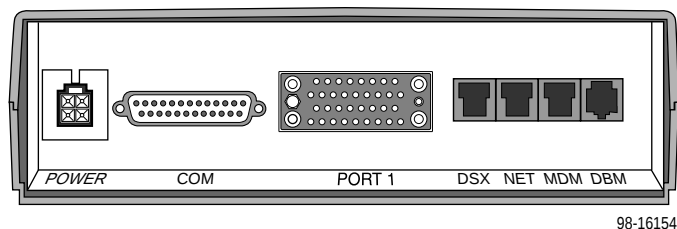
This appendix shows the FrameSaver unit rear panels, and pin assignments for the connectors/interfaces and cables. Standard interfaces are used on the unit, so most cables do not have to be specially ordered; they can be purchased anywhere.

NOTE:

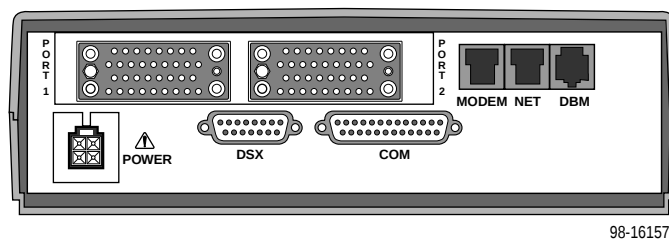
In the pin assignment tables of this appendix, if the pin number is not shown, it is not being used.

Rear Panels

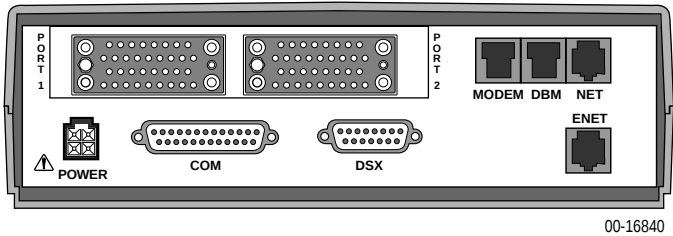
The following illustration shows the FrameSaver SLV 9126 unit's rear panel.



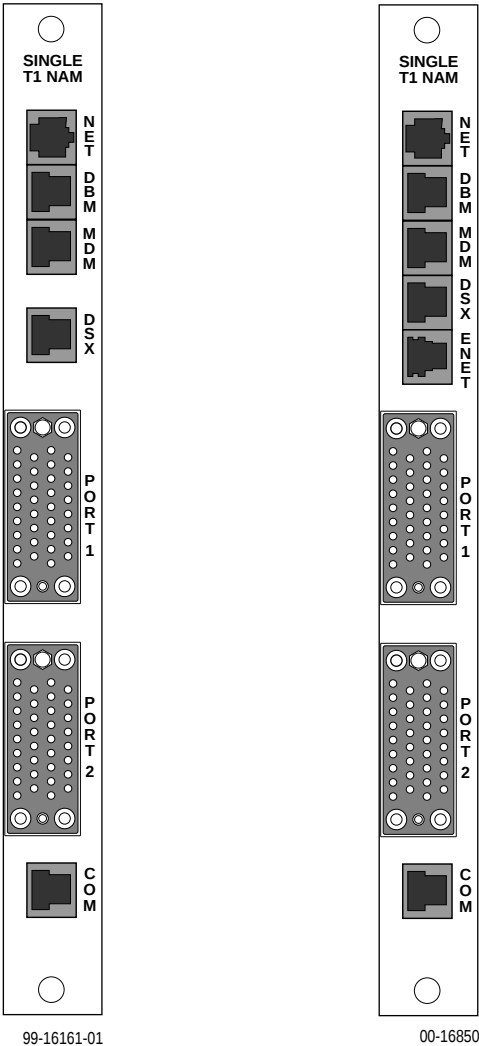
The following illustration shows the 1-slot FrameSaver SLV 9128 (without an Ethernet port, unit's rear panel.



The following illustration shows the 1-slot FrameSaver SLV 9128-II unit's rear panel. This model has an Ethernet port for management.



The following illustration shows the carrier-mounted, single T1, dual port FrameSaver SLV 9128 and 9128-II rear panels.



**Model 9128
without Ethernet**

**Model 9128-II
with Ethernet**

The sections that follow provide pin assignments for each interface.

COM Port Connector

The following table provides the pin assignments for the 1-slot FrameSaver SLV 9128 and 9126 unit's 25-position EIA-232C communication port connector.

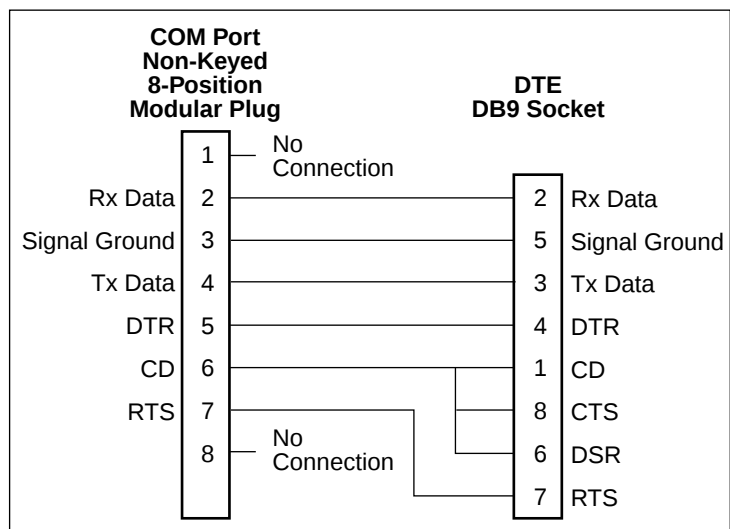
Signal	Direction	Pin #
Shield (GND)	—	1
DCE Transmit Data (TXD)	From DTE (In)	2
DCE Receive Data (RXD)	To DTE (Out)	3
DCE Request to Send (RTS)	From DTE (In)	4
DCE Clear to Send (CTS)	To DTE (Out)	5*
DCE Data Set Ready (DSR)	From DTE (In)	6*
Signal Ground (SG)	—	7
DCE Carrier Detect (CD)	To DTE (Out)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

The following table shows the signals and pin assignments for the carrier-mounted FrameSaver SLV 9128 NAM's 8-position communication port interface/connector.

Signal	Direction	Pin #
DCE Received Data (RXD)	From DCE (Out)	2
Signal Ground (SG)	To/From DCE	3
DCE Transmit Data (TXD)	To DCE (In)	4
DCE Data Terminal Ready (DTR)	To DCE (In)	5
DCE Carrier Detect (CD)	From DCE (Out)	6
DCE Request to Send (RTS)	To DCE (In)	7

COM Port-to-PC Cable (Feature No. 3100-F2-550)

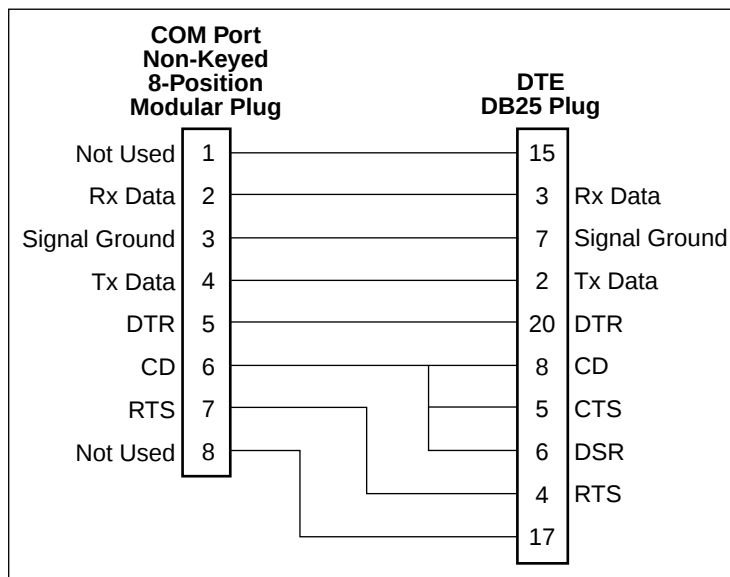
Order this cable when connecting the 8-position COM port to a PC. The following shows the pin assignments from the COM port to the DTE interface.



98-16166

COM Port-to-Terminal/Printer Cable (Feature No. 3100-F2-540)

Order this cable when connecting the 8-position COM port to a terminal or printer, rather than to a PC. The following shows the pin assignments from the COM port to the DTE interface.



98-16167

COM Port-to-Router Cables

The following tables provide the pin assignments for connecting the 1-slot FrameSaver unit's 25-position communication port to various router auxiliary (AUX) or console ports using standard cables.

Cisco 2500 Series Router – RJ45 Jack

COM Port		Direction	AUX Port	
Signal	DB25 Pin #		RJ45 Pin #	Signal
DCE Transmit Data (TXD)	2	To DTE	3	DTE Transmit Data (TXD)
DCE Receive Data (RXD)	3	From DTE	6	DTE Receive Data (RXD)
DCE Request to Send (RTS)	4	To DTE	1	DTE Request to Send (RTS)
DCE Clear to Send (CTS)	5	From DTE	8	DCE Clear to Send (CTS)
DCE Data Set Ready (DSR)	6	From DTE	7	DCE Data Set Ready (DSR)
DCE Signal Ground (SG)	7	—	4, 5	DTE Signal Ground (SG)
DCE Data Terminal Ready (DTR)	20	To DTE	2	DTE Data Terminal Ready (DTR)

Cisco 7000 Series Router – DB25 Plug

COM Port		Direction	AUX Port	
Signal	DB25 Pin #		DB25 Pin #	Signal
DCE Transmit Data (TXD)	2	To DTE	2	DTE Transmit Data (TXD)
DCE Receive Data (RXD)	3	From DTE	3	DTE Receive Data (RXD)
DCE Request to Send (RTS)	4	To DTE	4	DTE Request to Send (RTS)
DCE Signal Ground (SG)	7	—	7	DTE Signal Ground (SG)
DCE Carrier Detect (CD)	8	To DTE	8	DTE Carrier Detect (CD)
DCE Data Terminal Ready (DTR)	20	To DTE	20	DTE Data Terminal Ready (DTR)

3COM Router – DB9 Socket

COM Port		Direction	Console Port	
Signal	DB25 Pin #		DB9 Pin #	Signal
DCE Transmit Data (TXD)	2	To DTE	3	DTE Transmit Data (TXD)
DCE Receive Data (RXD)	3	From DTE	2	DTE Receive Data (RXD)
DCE Request to Send (RTS)	4	To DTE	7	DTE Request to Send (RTS)
DCE Signal Ground (SG)	7	—	5	DTE Signal Ground (SG)
DCE Carrier Detect (CD)	8	To DTE	1	DTE Carrier Detect (CD)
DCE Data Terminal Ready (DTR)	20	To DTE	4	DTE Data Terminal Ready (DTR)

The following tables provide the pin assignments for connecting the FrameSaver SLV 9128 or 9128-II NAM's 8-position communication port to various router auxiliary (AUX) or console ports using standard cables.

Cisco 2500 Series Router – RJ45 Jack

COM Port		Direction	AUX Port	
Signal	RJ45 Pin #		RJ45 Pin #	Signal
DCE Receive Data (RXD)	2	From DTE	6	DTE Receive Data (RXD)
DCE Signal Ground (SG)	3	—	4, 5	DTE Signal Ground (SG)
DCE Transmit Data (TXD)	4	To DTE	3	DTE Transmit Data (TXD)
DCE Data Terminal Ready (DTR)	5	To DTE	2	DTE Data Terminal Ready (DTR)
DCE Request to Send (RTS)	7	To DTE	1	DTE Request to Send (RTS)

Cisco 7000 Series Router – DB25 Plug

COM Port		Direction	AUX Port	
Signal	RJ45 Pin #		DB25 Pin #	Signal
DCE Receive Data (RXD)	2	From DTE	3	DTE Receive Data (RXD)
DCE Signal Ground (SG)	3	—	7	DTE Signal Ground (SG)
DCE Transmit Data (TXD)	4	To DTE	2	DTE Transmit Data (TXD)
DCE Data Terminal Ready (DTR)	5	To DTE	20	DTE Data Terminal Ready (DTR)
DCE Carrier Detect (CD)	6	To DTE	8	DTE Carrier Detect (CD)
DCE Request to Send (RTS)	7	To DTE	4	DTE Request to Send (RTS)

3COM Router – DB9 Socket

COM Port		Direction	AUX Port	
Signal	RJ45 Pin #		DB25 Pin #	Signal
DCE Receive Data (RXD)	2	From DTE	2	DTE Receive Data (RXD)
DCE Signal Ground (SG)	3	—	5	DTE Signal Ground (SG)
DCE Transmit Data (TXD)	4	To DTE	3	DTE Transmit Data (TXD)
DCE Data Terminal Ready (DTR)	5	To DTE	4	DTE Data Terminal Ready (DTR)
DCE Carrier Detect (CD)	6	To DTE	1	DTE Carrier Detect (CD)
DCE Request to Send (RTS)	7	To DTE	7	DTE Request to Send (RTS)

Gender Adapter/Changer

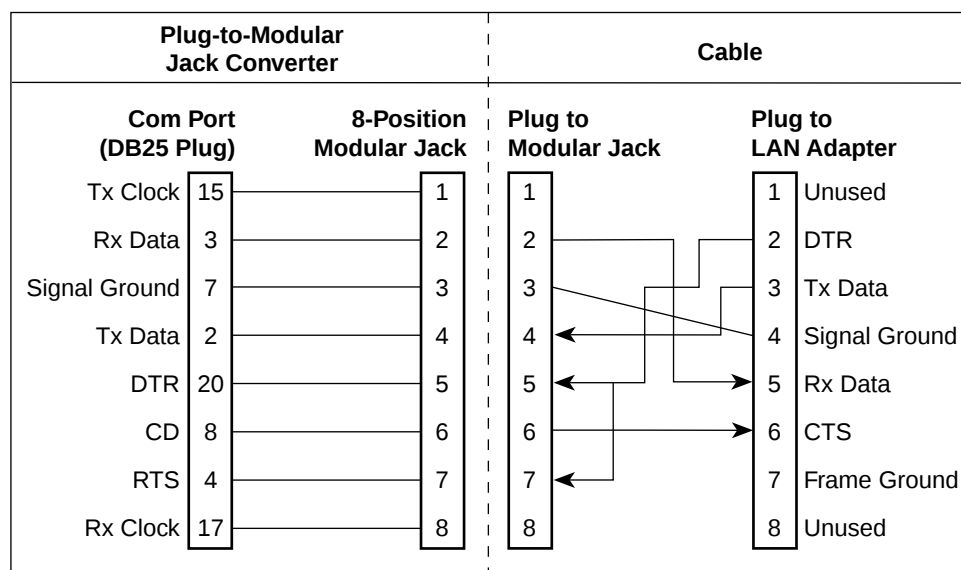
When connecting the COM port to a router or Frame Relay Assembler/Disassembler (FRAD), a gender adapter is required to convert the COM Port-to-Terminal/Printer cable's plug-type interface to a socket-type interface for the router's or FRAD's AUX port.

LAN Adapter Converter and Cable

A LAN adapter converter and cable is not needed for the FrameSaver SLV 9128 carrier-mounted unit since its COM port is an 8-position modular jack.

The following shows the pin assignments for the:

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



98-16214

DTE Port Connector

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

Signal	ITU CT#	Direction	34-Pin Socket
Shield	101	—	A
Signal Ground/Common (SG)	102	—	B
Request to Send (RTS)	105	To DSU (In)	C
Clear to Send (CTS)	106	From DSU (Out)	D
Data Set Ready (DSR)	107	From DSU (Out)	E
Receive Line Signal Detector (RLSD or LSD)	109	From DSU (Out)	F
Data Terminal Ready (DTR)	108/1, /2	To DSU (In)	H
Local Loopback (LL)	141	To DSU (In)	L
Transmit Data (TXD)	103	To DSU (In)	P (A) S (B)
Receive Data (RXD)	104	From DSU (Out)	R (A) T (B)
Transmit Signal Element Timing – DTE Source (XTXC or TT)	113	To DSU (In)	U (A) W (B)
Receive Signal Element Timing – DCE Source (RXC)	115	From DSU (Out)	V (A) X (B)
Transmit Signal Element Timing – DCE Source (TXC)	114	From DSU (Out)	Y (A) AA (B)
Test Mode Indicator (TM)	142	From DSU (Out)	NN

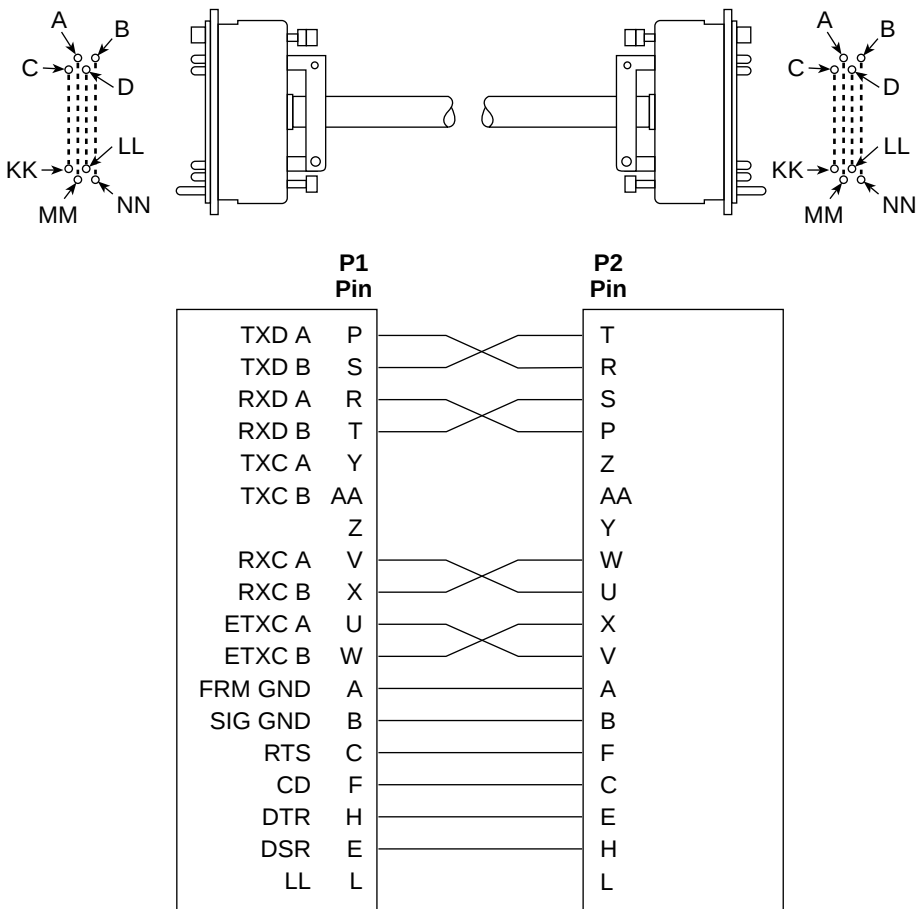
Standard V.35 Straight-through Cable

A standard V.35 straight-through cable can be used to connect a DTE port to a DTE, where a 34-pin plug-type connector is needed for the data port and a 34-position socket-type connector is needed for the DTE. No special-order cables are required.

Standard V.35 Crossover Cable

A standard V.35 crossover cable with a 34-pin plug-type connector on each end of the cable can be used to connect the FrameSaver unit's DTE port to another DCE.

The following illustration provides the pin assignments for the V.35 crossover cable.



98-16165a

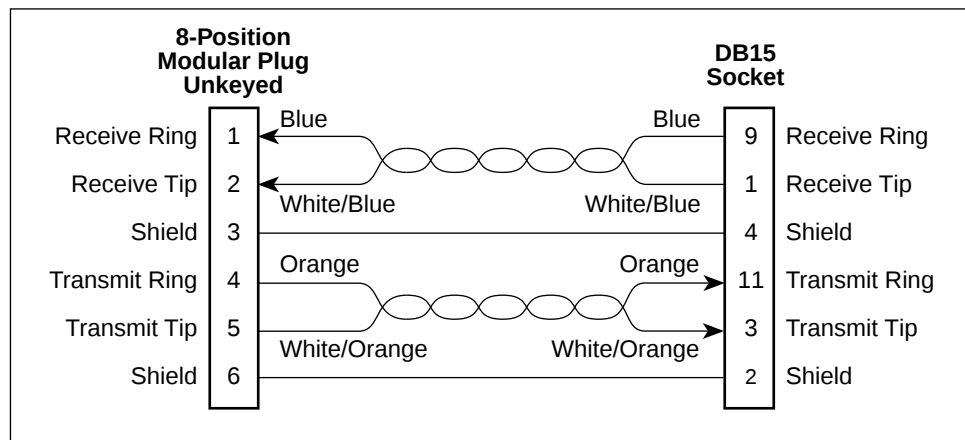
DSX-1 Connector

The following table shows the signals and pin assignments for the 8-position modular DSX-1 interface on the FrameSaver unit. The DSX-1 Adapter is required for this interface.

Function	Circuit	Direction	Pin Number
Receive Ring	R1	From DTE	1
Receive Tip	T1	From DTE	2
Shield	—	—	3
Transmit Ring	R	To DTE	4
Transmit Tip	T	To DTE	5
Shield	—	—	6

DSX-1 Adapter (Feature No. 9008-F1-560)

The DSX-1 adapter cable is used as an interface between the FrameSaver unit's DSX-1 connector and the DTE's DB15 interface. The following shows pin assignments and the purpose of each.



99-16216a

T1 Network Cable (Feature No. 3100-F1-500)

Network access is via a 20-foot cable with an RJ48C unkeyed plug-type connector on each end. The following table shows pin assignments and the purpose of each.

Function	Circuit	Direction	Pin Number
Receive Ring	R1	From Network	1
Receive Tip	T1	From Network	2
Transmit Ring	R	To Network	4
Transmit Tip	T	To Network	5

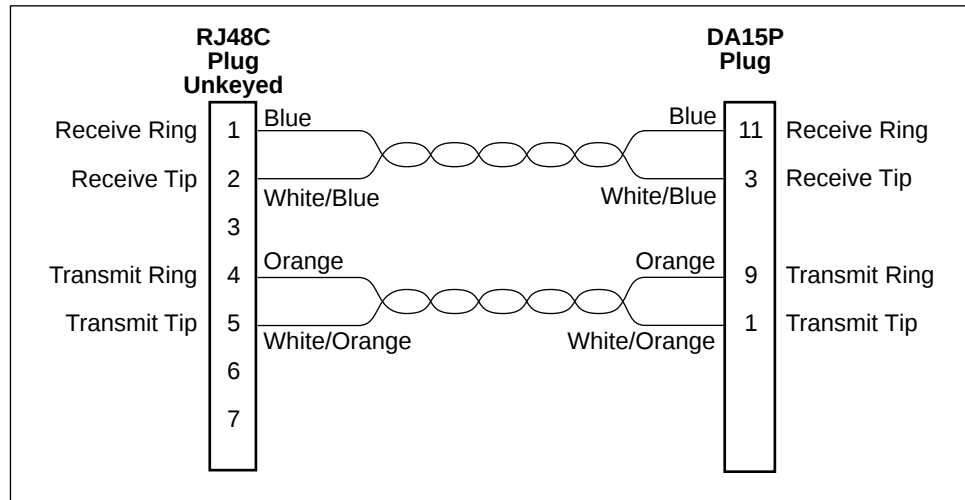
T1 Mass Termination Cable (Feature No. 9007-F1-500)

The following pin assignments are for the T1 Mass Termination cable that connects multiple carrier-mounted FrameSaver units to an M66 block. It has a 50-pin RJ48H plug at one end and seven RJ48C plugs at the other end.

Function	Circuit	Line #	Pin #	Function	Circuit	Line #	Pin #
Receive ring from the network	R1	1	1	Transmit ring to the network	R	1	14
		2	2			2	15
		3	3			3	16
		4	4			4	17
		5	5			5	18
		6	6			6	19
		7	7			7	20
Receive tip from the network	T1	1	26	Transmit tip to the network	T	1	39
		2	27			2	40
		3	28			3	41
		4	29			4	42
		5	30			5	43
		6	31			6	44
		7	32			7	45

Canadian T1 Line Interface Cable (Feature No. 3100-F1-510)

The T1 line interface cable is used in Canada as an interface between the FrameSaver unit's network connector and the T1 network interface. The following shows pin assignments and the purpose of each.



98-16215

Ethernet Port Connector

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

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

Modem Connector

The dial modem interface/connector that is integrated into the FrameSaver unit is an RJ11 6-position, 4-contact unkeyed modular jack. The following table shows pin assignments and the purpose of each.

Function	Circuit	Direction	Pin Number
Ring	R	To Local Loop	2
Tip	T	To Local Loop	3

ISDN DBM Connector

The backup connection is through the DBM interface/connector, which is an 8-position keyed modular jack. The following tables show pin assignments for the ISDN PRI and BRI DBMs and the purpose of each.

FrameSaver SLV 9128 ISDN PRI pin assignments:

Function	Circuit	Direction	Pin Number
PRI Receive Ring	DBM1	From Local Loop	1
PRI Receive Tip	DBM2	From Local Loop	2
PRI Transmit Ring	DBM4	To Local Loop	4
PRI Transmit Tip	DBM5	To Local Loop	5

FrameSaver SLV 9126 ISDN BRI/U pin assignments:

Function	Circuit	Direction	Pin Number
BRI Transmit/Receive Ring	DBM4	To/From Local Loop	4
BRI Transmit/Receive Tip	DBM5	To/From Local Loop	5

ISDN Modular Cable

The ISDN cable comes with the FrameSaver unit ordered with the DBM feature.

Technical Specifications

D

The following technical specifications are included:

- FrameSaver NAM (Network Access Module) and its interfaces
- 1-Slot FrameSaver Unit and its interfaces
- 14-Slot 9000 Series Access Carrier
- ISDN BRI DBM
- ISDN PRI DBM

Table D-1. NAM Technical Specifications (1 of 3)

Specification	Criteria
Approvals	
FCC Part 15	Class A digital device
FCC Part 68	Refer to the equipment's label for the Registration Number.
Industry Canada	Refer to the equipment's label for the Certification Number.
Safety	Refer to the equipment's label for safety information.
Physical Environment	
Operating temperature	32° F to 122° F (0° C to 50° C)
Storage temperature	–4° F to 158° F (–20° C to 70° C)
Relative humidity	5% to 85% (noncondensing)
Shock and vibration	Withstands normal shipping and handling

Table D-1. NAM Technical Specifications (2 of 3)

Specification	Criteria
Physical Dimensions NAM Height Depth I/O Card Height Depth	 8 inches (20.32 cm) 11.58 inches (29.41 cm) 10.15 inches (25.78 cm) 2.9 inches (7.37 cm)
Weight NAM I/O Card	 1 lb. 2 oz. (.51 kg) 6 oz. (.17 kg)
Power Consumption and Dissipation	9.5 watts, 0.080 A at 120 VAC Result: 32 Btu per hour
COM Port/Interface – Communications/Management Standard Data rates	8-position unkeyed modular jack EIA-232/ITU, V.24 (ISO 2110) 9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 kbps
T1 Network Interface Data rates Services supported Physical interface (USA) Physical interface (Canada) Framing format Coding format Line Build-Out (LBO) ANSI PRM Bit stuffing	8-position unkeyed modular USOC RJ48C jack Up to 1.536 Mbps Fractional T1 service, frame relay service RJ48C CA81A using adapter cable D4, ESF AMI, B8ZS 0.0 dB, –7.5 dB, –15 dB, –22.5 dB Selectable AT&T TR 62411
DSX-1 Interface Framing format Coding format DTE line equalization Send AIS	8-position modular connector with 8-position modular-to-DB15 adapter: D-Sub 15 socket D4, ESF AMI, B8ZS 5 selectable ranges from 0 to 655 feet (0 – 196.5 meters) Selectable

Table D-1. NAM Technical Specifications (3 of 3)

Specification	Criteria
Data Port Standard Data rates	34-position V.35 connector V.35/ITU (ISO 2593) Variations for T1 rates; automatically set to the network rate.
Modem (MDM) Interface Data rates Link Protocol	6-position unkeyed modular USOC RJ11C jack Up to 14.4 kbps PPP, SLIP
ISDN PRI DBM Interface Service supported Data rates Framing format Coding format Line Build-Out (LBO) ANSI PRM	8-position unkeyed modular USOC RJ48C jack PRI, NI-1 or NI-2 1.536 kbps D4, ESF B8ZS 0.0 dB, -7.5 dB, -15 dB, -22.5 dB Selectable
Ethernet Port Standard Data rates	8-position modular unkeyed jack ANSI/IEEE Standard 802.3, Ethernet Version 2 10/100 BaseT (auto-sensing 10 and 100 Mbps Ethernet rates)

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

Specification	Criteria
Approvals FCC Part 15 FCC Part 68 Industry Canada Safety	Class A digital device Refer to the equipment's label for the Registration Number. Refer to the equipment's label for the Certification Number. Refer to the equipment's label for safety information.
Physical Environment Operating temperature Storage temperature Relative humidity Shock and vibration	32° F to 122° F (0° C to 50° C) -4° F to 158° F (-20° C to 70° C) 5% to 85% (noncondensing) Withstands normal shipping and handling

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

Specification	Criteria
Physical Dimensions	
Height	2.9 inches (7.4 cm)
Width	8.5 inches (21.6 cm)
Depth	12.5 inches (31.8 cm)
Weight	
FrameSaver SLV 9126	2.10 lbs. (0.95 kg)
FrameSaver SLV 9128 and 9128-II	2.59 lbs. (1.18 kg)
Power Consumption and Dissipation	
Built-in power cord	NEMA 5-15P plug
Normal service voltage ranges for 100–240 VAC power supply:	120 Vac ± 12 , 60 Hz ± 3
FrameSaver SLV 9126 Power consumption	9.1 watts, 60 Hz ± 3 , 0.151 A at 120 VAC ± 12 Result: 31.05 Btu per hour
120 VAC power supply: FrameSaver SLV 9128 and 9128-II power consumption	10.3 watts, 60 Hz ± 3 , 0.125 A at 120 VAC ± 12 Result: 35.14 Btu per hour
COM Port/Interface – Communications/Management	25-position (DB25) connector
Standard	EIA-232/ITU, V.24 (ISO 2110)
Data rates	9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 kbps
T1 Network Interface	8-position unkeyed modular USOC RJ48C jack
Data rates	Up to 1.536 Mbps
Services supported	Fractional T1 service, frame relay service
Physical interface (USA)	RJ48C
Physical interface (Canada)	CA81A using adapter cable
Framing format	D4, ESF
Coding format	AMI, B8ZS
Line Build-Out (LBO)	0.0 dB, –7.5 dB, –15 dB, –22.5 dB
ANSI PRM	Selectable
Bit stuffing	AT&T TR 62411

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

Specification	Criteria
DSX-1 Interface Physical interface FrameSaver SLV 9126 FrameSaver SLV 9128 and 9128-II Framing format Coding format DTE line equalization Send AIS	8-position modular connector with 8-position modular-to-DB15 adapter: D-Sub 15 socket 15-position D-Subminiature connector D-Sub 15 socket D4, ESF AMI, B8ZS 5 selectable ranges from 0 to 655 feet (0 – 196.5 meters) Selectable
Data Port Standard Data rates	34-position V.35 connector V.35/ITU (ISO 2593) Variations for T1 rates; automatically set to the network rate.
Modem (MDM) Interface Data rates Link Protocol	6-position unkeyed modular USOC RJ11C jack Up to 14.4 kbps PPP, SLIP
ISDN BRI DBM Interface Service supported Data rates	8-position keyed modular USOC RJ49C jack BRI, NI-1 56 kbps and 64 kbps
ISDN PRI DBM Interface (FrameSaver SLV 9128 and 9128-II only) Service supported Data rates Framing format Coding format Line Build-Out (LBO) ANSI PRM	8-position unkeyed modular USOC RJ48C jack PRI, NI-1 or NI-2 1.536 kbps D4, ESF B8ZS 0.0 dB, –7.5 dB, –15 dB, –22.5 dB Selectable
Ethernet Port (FrameSaver SLV 9128-II only) Standard Data rates	8-position modular unkeyed jack ANSI/IEEE Standard 802.3, Ethernet Version 2 10/100 BaseT (auto-sensing 10 and 100 Mbps Ethernet rates)

Table D-3. 14-Slot 9000 Series Access Carrier Technical Specifications

Specification	Criteria
Approvals FCC Part 15 FCC Part 68 Industry Canada NRTL/C and CSA	Class A digital device Refer to the equipment's label for the registration number. Refer to the equipment label for the certification number. Refer to the equipment label.
Physical Environment Operating temperature Storage temperature Relative humidity Shock and vibration	35° F to 122° F (1.7° C to 50° C) –4° F to 158° F (–20° C to 70° C) 5% to 85% (noncondensing) Withstands normal shipping and handling
Physical Dimensions Height Width Depth	10.5 inches (26.7 cm) or 6U 17.2 inches (43.7 cm) 14.3 inches (36.3 cm)
Weight	Empty access carrier (without power supply) 11 lbs. 6 oz. (5.16 kg)
AC Power Requirements AC Power Supply DC Power Supply	90 to 265 VAC, 50/60 Hz $\pm$ 3A maximum –48 VDC, 6.6 amps, 316 watts
Heat Dissipation (Max.) 227 VAC –48 VDC	Fully loaded access carrier 585 Btu per hour maximum 465 Btu per hour maximum
Typical Power Consumption AC Power Supply 1 power supply installed 2 power supplies installed DC Power Supply 1 power supply installed 2 power supplies installed	100 VAC 60 Hz 1.7 amps 171 watts 120 VAC 60 Hz 1.03 amps 60 watts 100 VAC 50 Hz 1.15 amps 60 watts Result: 207 Btu per hour 100 VAC 60 Hz 1.25 amps 64.5 watts 120 VAC 60 Hz 1.5 amps 177 watts 230 VAC 50 Hz 0.9 amps 172 watts Result: 221 Btu per hour 104 watts at –48 VDC Result: 355 Btu per hour 124 watts at –48 VDC Result: 423 Btu per hour

Table D-4. ISDN BRI DBM (Optional Feature) Technical Specifications

Specification	Criteria
Standards Compliance	ANSI T1.601 – 1992 (physical layer) Bellcore SR-NWT-001937, Issue 1 – February 1991 ITU Q.921 – 1992 (link layer) ITU Q.931 – 1993 (network layer) TR-TSY-00860, ISDN Calling Number Identification Services – February 1989, and Supplement – June 1990
Power Consumption	60 mA at 15 VDC Average power .9 watt (3.07 Btu per hour)
Weight	0.27 lbs. 4.3 oz. (0.12 kg 122 grams)
Switch Compatibility	National ISDN-1 (NI-1)
Service Supported	Capability Package IOC B for 1B-service, which supports up to two circuit-switched B-channels, BRI-B1 and BRI-B2, with one Service Profile Identification (SPID) number and one local phone number. Capability Package IOC R for 2B-service, which supports up to two circuit-switched B-channels, BRI-B1 and BRI-B2, with two SPID numbers and two local phone numbers.
Switched Network Interface	One USOC RJ49C 8-pin keyed modular plug and jack, specified in ISO/IEC 8877
Transmit Interface Signal Level Impedance	13.5 dBm nominal over frequency band, 0 Hz – 80 kHz 135 Ω
Receive Interface Dynamic Range Impedance	Operates on 2-wire loops, defined in ANSI T1.601-1992 135 Ω
Modulation and Frequency	2B1Q line coding with 4-level amplitude modulation (PAM) at 80 kbps baud
Channel Equalization Receiver	Automatic adaptive equalizer with echo cancellation

Table D-5. ISDN PRI DBM (Optional Feature) Technical Specifications

Specification	Criteria
Standards Compliance	ANSI T1.403 – 1989 (physical layer) and AT&T 62411 Bellcore SR-NWT-002120, Issue 1 – May 1992 ITU Q.921 – 1992 (link layer) ITU Q.931 – 1993 (network layer) TR-TSY-00860, ISDN Calling Number Identification Services – February 1989, and Supplement – June 1990
Power Consumption	8 mA at 120 VAC Average power 1 watt (3.4 Btu per hour)
Weight	0.15 lbs. 2.4 oz. (0.07 kg 68 grams)
Switch Compatibility	National ISDN-2 (NI-2), ATT 4ESS, or ATT 5ESS
Service Supported	PRI, NI-2, ATT 4ESS custom, or ATT 5ESS custom (supporting up to 23 B-channels), with Circuit-Switched Data capability.
Framing Format	D4, ESF
Coding Format	B8ZS
Line Build-Out (LBO)	0.0 dB, –7.5 dB, –15 dB, –22.5 dB
ANSI PRM	Selectable

Equipment List

E

Equipment

See page E-4 for **cables** you can order.

Description	Model/Feature Number
FrameSaver SLV Units	
FrameSaver SLV 9126 T1 remote site unit with integral modem but without ISDN BRI DBM for up to 16 PVCs <i>Includes 1-Slot Housing, Universal 100–240 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.</i>	9126-A1-201
FrameSaver SLV 9126 T1 remote site unit with integral modem and ISDN BRI DBM for up to 16 PVCs <i>Includes 1-Slot Housing, Universal 100–240 VAC Power Supply, Network Cable, RJ49C BRI ISDN/U Cable, Installation Instructions, and Quick Reference.</i>	9126-A1-202
FrameSaver SLV 9128 T1 central site 1-slot unit with integral modem and ISDN PRI DBM for up to 120 PVCs <i>Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, RJ48C PRI ISDN Cable, Installation Instructions, and Quick Reference.</i>	9128-A1-202
FrameSaver SLV 9128 T1 central site 1-slot unit with integral modem but without ISDN PRI DBM for up to 120 PVCs <i>Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.</i>	9128-A1-204
FrameSaver SLV 9128 T1 central site 1-slot unit with integral modem for up to 120 PVCs and an ISDN BRI DBM <i>Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, ISDN BRI DBM, RJ49C BRI ISDN Cable, Installation Instructions, and Quick Reference. (1-Slot 9128 only)</i>	9128-A1-204 and 9098-F1-870

Description	Model/Feature Number
FrameSaver SLV Units	
FrameSaver SLV 9128 T1 central site carrier NAM with integral modem but without ISDN PRI DBM for up to 120 PVCs <i>Includes Network Cable, Installation Instructions, and Quick Reference.</i>	9128-B1-212
FrameSaver SLV 9128 T1 central site 1-slot unit with integral modem and ISDN PRI DBM for up to 120 PVCs, and Ethernet port for management <i>Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, RJ48C PRI ISDN Cable, Installation Instructions, and Quick Reference.</i>	9128-A2-202
FrameSaver SLV 9128 T1 central site 1-slot unit with integral modem for up to 120 PVCs, ISDN BRI DBM, and Ethernet port for management <i>Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, ISDN BRI DBM, RJ49C BRI ISDN Cable, Installation Instructions, and Quick Reference. (1-Slot 9128 only)</i>	9128-A2-204 and 9098-F1-870
FrameSaver SLV 9128 T1 central site carrier NAM with integral modem but without ISDN PRI DBM for up to 120 PVCs, and Ethernet port for management <i>Includes Network Cable, Installation Instructions, and Quick Reference.</i>	9128-B2-212
User Manual	
FrameSaver SLV 9126/9128 User's Guide (Paper Manual)	9128-A2-GB20
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 Up to Two 1-Slot Housings	9001-F1-894
ISDN BRI DBM	9098-F1-870
ISDN PRI DBM	9098-F1-875
FrameSaver SLV 9128 1-Slot Housing-to-9000 Series Access Carrier Upgrade	9128-F1-212

Description	Model/Feature Number
Power Supplies	
100 – 240 VAC for 1-Slot Housing	9001-F1-040
120 VAC for 1-Slot Housing	9001-F1-020
AC Power Supply for Access Carrier	9007-F1-040
DC Power Supply for Access Carrier	9005-F1-050
9000 Series Access Carrier (9128 or 9128-II NAM only)	
Access Carrier <i>Includes 14-Slot Housing, Universal 90 – 250 VAC Power Supply, Power Supply Tray, Baffle, Fan Tray, Mounting Brackets, and Installation Instructions.</i>	9007-B1-409
Access Carrier <i>Includes 14-Slot Housing, Universal –48 VDC Power Supply, Power Supply Tray, Baffle, Fan Tray, Mounting Brackets, and Installation Instructions.</i>	9007-B1-509
Baffle for Access Carrier	9007-S1-897
Fan Tray for Power Supply in Access Carrier	9007-S1-898
Fan Tray for Access Carrier	9007-S1-899

Cables

This table lists cables you can order.

Description	Part Number	Feature Number
RJ48C T1 Network Cable, RJ48C-to-RJ48C – 20 feet/6.1 meters	035-0209-2031	3100-F1-500
RJ48C DSX-1 Network Cable, 8-pin modular-to-8-pin modular – 20 feet/6.1 meters		
ISDN BRI DBM Cable, RJ49C-to-RJ49C – 20 feet/6.1 meters		
ISDN PRI DBM Cable, RJ48C-to-RJ48C – 20 feet/6.1 meters		
T1 Line Interface Cable, RJ48C-to-CA81A – 20 feet/6.1 meters <i>For use in Canada.</i>	035-0221-2031	3100-F1-510
COM Port-to-Terminal Cable, 8-pin modular-to-DB25P – 14 feet/4.3 meters	035-0314-1431	3100-F2-540
COM Port-to-PC Cable, D-Sub9-to-DB25 for PC serial port – 14 feet/4.3 meters	035-0313-1431	3100-F2-550
COM Port-to-LAN Adapter Cable, custom unkeyed 8-pin plug-to-8-pin plug modular cable – 14 feet/4.3 meters <i>Used for a LAN Adapter (LANA).</i>	035-0315-1431	3100-F1-910
Adapter DB25 plug-to-8-position modular receptacle <i>Used with the COM Port-to-LAN Adapter Cable.</i>	002-0069-0031	3100-F1-920
T1 Mass Termination Cable, 50-pin plug-to-seven RJ48S plugs – 5 feet/1.5 meters <i>Connects carrier-mounted units to a M66 block.</i>	035-0363-0531	9007-F1-500
DSX-1 Adapter Cable, RJ48C-to-DB15 – 1 foot/0.3048 meters <i>For use by FrameSaver 9126.</i>	035-0386-0031	9008-F1-560

Index

Numbers

1MPort mode, auto-configuration, 3-13
1Port mode, auto-configuration, 3-13
2MPorts mode, auto-configuration, 3-13
55 hexadecimal, test pattern, 6-24

A

aborting tests, 6-21
Access
 Dial-In, 4-4
 Easy, 3-8
 Level, Port, 3-93
 Name, 3-77
 to another device's interface, 5-63
 Type, 3-81
Access Level, 4-11, 4-12
 assigning, 4-10
 Port, 3-90
 security, 2-1
 Session, 3-78
Action on Network Yellow Alarm, 3-41
activating Modem PassThru, 5-63
adding, SLV units to network, 9-3
AIS
 alarm condition, 6-7
 at DSX-1 or Network, 5-19
 at ISDN PRI, 5-19
 LED, 5-7, 5-9
 linkDown trap, B-11
Alarm, 6-7
 (Fail), 5-7, 5-8
 adding manually, 8-11
 conditions, 6-2, 6-7
 configurable thresholds, 1-2
 editing, 8-9
 LED is lit, 6-14
 Relay, turning off, 5-74
 RMON defaults, B-18
 using template, 8-8
ALM LED, 5-7, 5-8, 5-9
Alternate
 Dial-Out Directory, 3-85
 IP Address, 3-95
 Outbound Phone Number, 3-50
 software revision, 5-3
 Subnet Mask, 3-95

Alternate Destination
 DLCI, 3-68
 EDLCI, 3-68
 Link, 3-68
Annex A and D, LMI Protocol, 3-60
ANSI Performance Report Messages, 3-35, 3-46
ANSI T1.403 Annex B FT1 Channel Loopback, 6-32
ARP
 inverse, 1-2
 Proxy, 3-87
assign
 DSX-1 time slots, 3-52
 frame relay time slots, 3-51
 synchronous data port, 3-58
 time slots and cross connections, 3-50
assigning
 community names and access levels, 4-10
 DLCIs to a Backup Group, 3-22
At-a-Glance report, 9-6
authenticationFailure trap, B-9
Auto Backup
 Criteria, 3-96
 restricting, 3-21
Auto-Configuration, 1-3, 2-4
 Active, 5-19
 setting up, 3-12
availability, LMI and PVC, 1-5

B

back door access when locked out, 6-4
Back-to-Back
 Mode Active, 5-19
 operation, setting up, 3-23
Backspace, 2-6
Backup
 Active, 5-19
 assigning DLCIs to a group, 3-22
 auto, 3-96
 changing automatic configuration, 3-18
 dial, 3-16
 Group, 3-65
 ISDN, 1-4
 manually forcing, 5-65
 over network interface, 3-23
 setting timers and thresholds, 3-21
 verifying setup, 5-67

- Bc, 3-64
- Be, 3-64
- Bearer channel, 3-44
- BECN, ISDN backup, 1-4
- Bit Stuffing, 3-34
- BKP LED, 5-8
- blank, field value, 2-9
- branches/menus, 2-4
- bursting, port, 1-5

C

- Call
 - Directories, 3-10
 - Retry, 3-85
 - Status, 5-37
- Caller
 - ID, 3-50, 4-5
 - Identification Method, 3-50, 4-5
- canceling Modem PassThru, 5-63
- Cause Value messages, 5-39
- central clock, 1-5
- CGA, 3-54
- changing
 - auto-configuration, 3-18
 - automatic backup configuration, 3-18
 - configuration options, 3-6
 - domains and groups, 8-6
 - operating mode, 3-23
 - software release, 5-72
- Channel Loopback, 6-32
- Character
 - Length, 3-88
 - matching, 2-9
- CIR, 3-64
 - enforcement, 3-26
 - statistics, 5-49
- Circuit Identifier, 3-36, 3-47
- circuit multiplexed PVCs, 6-25
- Clearing
 - cross connection assignments, 3-50
 - Event, LMI, 3-27, 3-61
 - existing information, 3-9
 - statistics, 5-48
- Clock
 - Invert Transmit, 3-38
 - setting system, 3-9
 - Source, 3-30, 3-31
 - Transmit, 3-39
- CNIS, 4-5
- COM port, 3-71, 3-82
 - connector, C-3
 - to-PC or terminal/printer cable, C-4
 - to-router cables, C-5
- Committed Burst Size Bc (Bits), 3-64
- Committed Information Rate (CIR), 3-64
- Communication, Port, user interface options, 3-88
- Community Name, 3-76
 - assigning, 4-10
- Concord's Network Health, 1-1
 - compatibility, 9-1
- Configuration
 - Auto, Active, 5-19
 - displaying and changing options, 3-5
 - FTP transfer rate, 1-5
 - menu, 3-3
 - menu/branch, 2-4
 - option areas, 3-4
 - option tables, 3-24
 - saving options, 3-7
 - tables, 3-4
- configuring
 - added SLV units/elements, 9-4
 - DBM, 3-44
 - interface to send traps, 3-22
 - DLCI records manually, 3-63
 - frame relay options, 3-60
 - modem port, 3-92
 - NetScout Manager Plus, 8-3
 - network interface, 3-33
 - SLV options, 3-28
 - System options, 3-25
 - the system, 3-3
- connecting to a PC, terminal, or printer, C-4
- Connectivity, test, 6-25
- Control
 - keys, 2-6
 - lead descriptions, 5-10
 - Leads, Ignore, 3-89
 - menu/branch, 2-4
- Control Leads and LEDs, displaying, 5-5
- controlling
 - asynchronous terminal access, 4-2
 - dial-in access, 4-4
 - FTP access, 4-6
 - ISDN access, 4-5
 - SNMP access, 4-9
 - Telnet access, 4-6
- conversation elements, 9-3
- copyrights, A
- CRC, 5-56
- creating
 - a login, 4-12
 - new PVC connections/management links, 3-6
 - user history files, 8-13
- cross connections, 3-50
- CTS
 - down, 6-7
 - down to Port Device, 5-19
- current software revision, 5-3

D**Data**

- Channel Loopback, 3-35, 5-20, 6-32
- Delivery Ratio (DDR), 1-2
- Link Control Identifier (DLCI), 3-74, 3-75
- Port, physical options, 3-37
- port connector pin assignments, C-9
- Rate (Kbps), 3-88
- selection criteria, 2-1
- uploading SLV and packet capture, 5-73

Date & Time setting, 3-9**DBM**

- BRI Card Failed, 5-19
- call performance statistics, 5-60
- changing BRI software, 5-71
- configuring interface, 3-44
- configuring to send traps, 3-22
- connector, C-14
- Download Required, 5-20
- forcing backup and placing a call, 5-65
- Health and Status messages, 5-19
- interface status, 5-35
- ISDN problems, 6-17
- test status messages, 5-26
- tests, 6-19
- verifying setup, 5-67

DCLB, 6-32**DDR, 1-2****DE, Set, 3-73****Default IP Destination, 3-71****Delete key, 2-6****deleting a login, 4-13****Destination, 3-82**

- Default IP, 3-71
- DLCI, 3-67, 3-68
- EDLCI, 3-67, 3-68
- Link, 3-67, 3-68

Device

- messages, 5-11
- troubleshooting problems, 6-14

dial backup, 3-16**Dial-In Access, 3-92**

- controlling, 4-4

Dial-Out

- Delay Time (Min), 3-85
- Directory, 3-85
- options, 3-10, 3-81
- Trap, 3-84

dialControl, traps, B-17**dialCtlPeerCall, traps, B-17****Directory, Alternate Dial-Out, 3-85****disabling**

- SNMP access, 4-9
- system alarm relay, 5-74

disaster recovery, 3-16, 3-23**Discard Eligible (DE), 3-73****Disconnect**

- modem, 5-64
- Time (Minutes), 3-79, 3-90, 3-94

discovering elements/DLCIs, 9-3**Discovery**

- frame relay (FR), 3-13
- Frame Relay Mode, saving a mode change, 3-15
- time slot, 1-3

displaying

- configuration options, 3-5
- identity information, 5-3
- LEDs and control leads, 5-5

DLCI, 3-74, 3-75

- Alternate, 3-75
- assigning to a Backup Group, 3-22
- Destination, 3-67, 3-68
- Down, 5-20, 6-7
 - on SLV Timeout, 3-28
- interface status, 5-29
- monitoring user history, 8-16
- Number, 3-63
- Priority, 3-65
- Records, 3-63
- Source, 3-66
- statistics, 5-51
- status, 5-28
- Traps on Interfaces, 3-84
- Type, 3-63

domains and groups

- correcting, 8-6
- verifying, 8-5

download, 5-70**downloading**

- determining when completed, 5-72
- MIBs and SNMP traps, B-2
- SLV alarms, 8-8
- software, 5-68
- user history file, 8-13

DSX-1

- adapter pin assignments, C-11
- assigning data port to time slots, 3-58
- assigning time slots, 3-52
- connector pin assignments, C-11
- interface LEDs, 5-9
- setting up, 3-42
- signaling assignments, 3-54
- timeslot assignments, 5-34
- trunk conditioning, 3-54

DTE

- Loopback, 6-30
- port connector pin assignments, C-9
- port-initiated loopbacks, 3-40

DTLB, 6-30**DTR**

- control lead, 5-10
- down, 6-7
- down from Port-1 Device, 5-20
- Ignore Control Leads, 3-89

E

- Easy Install feature, 3-8
- EDLCI, 3-74, 3-76
 - Destination, 3-67, 3-68
 - Source, 3-66
- EER
 - at ISDN PRI, 5-20
 - at Network, 5-20, 6-8
 - LED, 5-7, 5-9
 - linkDown trap, B-11
- EIA-232C, COM Port connector, C-3
- EIR
 - enforcement, 3-26
 - statistics, 5-49
- elements/DLCIs, 9-3
- Embedded Data Link Connection Identifier (EDLCI), 3-66, 3-67, 3-68, 3-74, 3-76
- ending a session, 2-3
- Enter (Return) key, 2-6
- entering ISDN call profiles, 3-48
- entering system information, 3-9
- Enterprise, Specific Traps, 3-83
- enterprise-specific traps, B-13
- equipment list, E-1
- Error, Event, LMI, 3-26, 3-61
- Errors, frame relay statistics, 5-54
- Esc key, 2-6
- ESF Line, statistics, 5-57
- Ethernet
 - Initial Route Destination, 3-82
 - Link Down, 5-20
 - performance statistics, 5-61
 - port, MAC address, 5-3
- Ethernet port, 3-71
 - connector pin assignments, C-13
 - default gateway address, 3-87
 - options, 3-86
- even parity, 3-89
- Event Log, Trap, 5-62, 6-14
- exception points, 9-7
- Excess Burst Size (Bits), 3-64
- Excessive
 - Error Rate linkDown trap, B-11
 - Error Rate Threshold, 3-36, 3-47
- External, Transmit Clock, 3-39

F

- faceplate, 5-5
- faceplates
 - 9126, 5-5
 - 9128, 5-6
- FDR, 1-2
- features, 1-2
- field is blank/empty, 2-9
- file transfer, 5-68
- FTP (file transfer protocol), 3-79
 - Session, 3-79
- FR Mode LED, 5-8
- Frame Delivery Ratio (FDR), 1-2
- Frame Relay
 - assigning time slots, 3-51
 - configuring interface, 3-60
 - configuring system, 3-25
 - Discovery, 3-13
 - saving a mode change, 3-15
 - DS0s Base Rate, 3-61
 - Mode, LED, 5-8
 - statistics, 5-53
 - troubleshooting PVC problems, 6-16
- frames, 3-73
- FTP, 1-5, 5-68
 - file transfers, 5-68
 - initiating a session, 5-68
 - limiting access, 4-6, 4-7
 - Login Required, 3-79
 - Max Transfer Rate (kbps), 3-79
 - Session, 4-7
- function keys, 2-5, 2-7

G

- Gateway, 5-45
- Gateway Address, Default, 3-87
- gender adapter/changer, C-8
- General
 - LEDs, 5-7
 - options, 3-30
 - SNMP management, options, 3-76
 - Traps, 3-82
- generating reports, 9-6
- glossary, x
- grouping elements for reports, 9-5

H

- hardware revision
 - DBM, 5-4
 - NAM, 5-3
- HDLC errors, frame relay statistics, 5-56
- Health and Status, 6-2
 - messages, 5-19
- history
 - adding files, 8-13
 - installing files, 8-15
 - monitoring DLCI, 8-16
- Hop, 5-46
- hyperlink to more information, highlighted text, xii

I

- ICMP, IP routing table type, 5-46
- Identity, displaying, 5-3
- Ignore Control Leads, 3-89
- Inactivity Timeout, 3-79, 3-90, 3-93
- Inbound Calling ID, 3-49
- Initial Route Destination, 3-82
- installation, 1-2
- installation and setup, Network Health, 9-2
- installing
 - Network Health, 9-2
 - user history files, 8-15
- interface
 - DBM status, 5-35
 - status, 4-5
 - user, 2-1
- Interface Status
 - Ethernet port, 3-86
 - Network, 3-42
- Internal, Transmit Clock, 3-39
- Inv SPID, Local Number, Call ID, 5-36
- Inverse ARP, 1-2
- Invert Transmit and Received Data, 3-40
- Invert Transmit Clock, 3-38
- IP
 - Address, 3-95
 - default destination, 3-71
 - node information, 3-70
 - Ping test, 6-35
 - Routing Table, 1-6, 5-45
 - Validation, NMS, 3-80
- IP Address, 3-73, 3-91, 3-94
 - Ethernet port, 3-86
 - NMS number, 3-80, 3-82
 - Node, 3-70
- IP addressing, limiting SNMP access, 4-11

ISDN

- Active, 5-21
- backup, 1-4
- BRI DBM, 1-4
 - troubleshooting problems, 6-17
- controlling access, 4-5
- DBM connector, C-14
- DBM operation, 5-65
- Link Profile Invalid, 5-21, 6-8
- Network Failed, 5-21, 6-8
- physical options, 3-44
- PRI DBM, 1-4
- setting up link profiles, 3-48
- updating software, 5-71
- verifying line, 5-67

K

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

L

- Lamp Test, 5-26, 6-36
- LAN, adapter and cable, C-8
- last reset, 5-18
- latency, 1-5
 - round trip, setting threshold, 3-29
- LEDs, 6-2, 6-14
 - 9126 faceplate and screen, 5-5
 - 9128 faceplate and screen, 5-6
 - and control leads, displaying, 5-5
 - descriptions, 5-7
- limiting
 - async terminal access, 4-2
 - dial-in access, 4-4
 - FTP access, 4-7
 - SNMP access, 4-9
 - through IP addresses, 4-11
 - Telnet access, 4-6
- Line
 - Build Out (LBO), 3-34, 3-46
 - Coding Format, 3-33, 3-42
 - Equalization, 3-43
 - Framing Format, 3-33, 3-42, 3-45
 - Loopback, 6-27
 - Status, 5-36
- Line Loopback, 6-31, 6-33

Link

- Destination, 3-67, 3-68
- frame relay statistics, 5-53
- maximum ISDN rate, 3-49
- Name, 3-48
- Operating Mode, 5-37
- Profile Disabled, 5-21, 6-8
- Protocol, 3-92, 3-94
- setting up ISDN profiles, 3-48
- Source, 3-66
- Status, 3-48
- Traps, 3-83
- Traps Interfaces, 3-83
- troubleshooting management, 6-5
- TS Management, 3-71

linkUp and linkDown

- events, 3-83
- traps, B-10

LLB, 6-27, 6-31, 6-33

LMI

- and PVC availability, 1-5
- Behavior, 3-25, 3-26
- Clearing Event (N3), 3-27, 3-61
- configuring frame relay and, 3-25
- Down, 5-21, 6-9
- Error Event (N2), 3-26, 3-61
- frame relay statistics, 5-55
- Heartbeat (T1), 3-27, 3-62
- Inbound Heartbeat (T2), 3-27, 3-62
- N4 Measurement Period (T3), 3-27, 3-62
- OK control lead, 5-10
- packet utility, 6-5
- Parameters, 3-61
- pass-through, 3-25
- Protocol, 3-60
- Status Enquiry (N1), 3-27, 3-61
- trace log, 6-6
- uploading packet capture data, 5-73

local, external DTE loopback, 3-40

locked out, 4-3, 4-12, 6-4

LOF, LED, 5-9

Log

- LMI Trace, 6-6
- Trap Event, 5-62

logging in, 2-2

logging out, 2-3

Login

- creating, 4-12
- ID, 4-12
- modifying and deleting, 4-13
- Required, 3-78, 3-89, 3-93, 4-3, 4-6, 4-7

logins, 4-1

Loopback

- Data Channel, 6-32
- DTE, 6-30
- Line, 6-27
- Payload, 6-28
- Port (DTE) Initiated, 3-40
- PVC, 6-23
- Remote, 6-31, 6-33
- Repeater, 6-29
- V.54, 6-32

LOS

- at DSX-1, 5-21, 6-10
- at ISDN PRI, 5-22
- at Network, 5-22, 6-10
- LED, 5-7, 5-9
- linkDown trap, B-11

Loss of Signal, linkDown trap, B-11

M

MAC address, 5-3

Main Menu, screen, 2-4

maintenance, 5-1

making input selections, 2-9

Management

- and Communication, options, 3-69
- General SNMP, options, 3-76
- OpenLane, 1-7
- OpenLane system, 1-7
- PVCs, 3-72
 - total number dedicated, 1-3
- SNMP, 3-76
- troubleshooting link, 3-70, 6-5

mass termination cable, C-12

Max Port Rate, 3-38

Maximum Link Rate, 3-49

MDM connector, C-14

menu

- branches, 2-4
- Configuration, 3-3
- main, 2-4
- path, 2-5
- selecting from, 2-8
- structure, A-1

messages

- Cause Values, 5-39
- Device, 5-11
- Health and Status, 5-19
- Self-Test Results, 5-18
- system, 2-5
- System and Test Status, 5-18
- Test Status, DBM, 5-26

MFR, B-4
 MIB
 access, 4-10
 downloading, B-2
 support, B-2
 Mode
 changing Operating, 3-23
 Operating, 5-37
 Test, 5-8
 model number, 2-5
 modem, 1-4
 connector, C-14
 Health and Status messages, 5-19
 manually disconnecting, 5-64
 operation, 5-63
 PassThru, 3-88
 PassThru feature, 1-4, 3-11, 5-63
 port, destination, 3-71, 3-82
 port options, 3-92
 setting up, 3-10
 verifying setup and operation, 5-64
 modifying a login, 4-13
 Monitor
 DTR, 3-39
 Pattern, 6-24
 RTS, 3-39
 monitoring
 DLCI history data, 8-16
 FrameSaver unit, 5-17
 LEDs, 5-5, 5-6
 LEDs and control leads, 5-5
 using NetScout Manager Plus, 8-18
 most recent cause values, 5-39
 Multilink Constituent Link, 5-37
 Multilink Frame Relay
 Bundle, B-4
 implementation, 1-4
 Multiplexed
 DLCI, 3-66, 3-67, 3-68, 3-74, 3-75, 3-76
 DLCI Type, 3-63
 PVCs, 6-25

N

N1, LMI Status Enquiry, 3-27, 3-61
 N2, LMI Error Event, 3-26, 3-61
 N3, LMI Clearing Event, 3-27, 3-61
 NAM, 1-6
 Name, 3-73
 1 or 2 Access, 4-10
 Access, 3-77
 Community, 3-76, 3-77
 navigating the screens, 2-6
 Net Link, Port Use, 3-88, 3-92
 NetOnly mode, 3-14
 NetScout
 Manager Plus, NMS support, 1-8
 NMS support, 1-1

Network

 access module, 1-6
 assigning data port to time slots, 3-58
 cable pin assignments, C-12
 Com Link Down, 5-22, 6-10
 configuring the interface, 3-33
 DLCI records, options, 3-63
 Health (Concord) reports, 9-1
 Health installation and setup, 9-2
 Initiated Data Channel Loopback, 3-41
 Initiated DCLB, 3-35
 Initiated LLB, 3-34, 3-46
 Initiated PLB, 3-35, 3-46
 interface, control leads, 5-10
 interface LEDS, 5-9
 interface options, 3-33
 latency, 1-5
 reference time, 1-5
 timeslot assignments, 5-33

NMS

 IP Address, 3-80, 3-82, 4-11
 IP Validation, 3-80, 4-11
 OpenLane management system, 1-7
 SNMP security, options, 3-80

Node

 IP, configuration option tables, 3-70
 IP Address, 3-70
 Subnet Mask, 3-70

NSP, 3-25

Number of

 Managers, 3-80, 4-11
 Trap Managers, 3-81

O

odd parity, 3-89

OID

 (object identification), user history file, 8-13
 cross-reference (numeric order), B-27, B-32

OK LED, 5-7, 5-9

OOF

 at DSX-1 or Network, 5-22, 6-10
 at ISDN PRI, 5-23
 LED, 5-7, 5-9
 linkDown trap, B-11

OpenLane, 1-7

 copying directory, 8-2
 SLM support, 7-1

operating mode, changing, 3-23

operation, 2-1, 5-1

organization of this document, ix

Out of Frame, 5-7

 linkDown trap, B-11

Out of Sync, message, 6-16, 6-24

Outbound

 Management Priority, 3-65
 Phone Number, 3-49
 alternate, 3-50

P

- packet capture
 - uploading data, 5-73
 - utility, 6-5
- packets, 3-73
- Parity, 3-89
- PassThru, modem feature, 1-4, 5-63
- Password, 4-12
- patents, A
- pattern
 - send/monitor interior, 6-24
 - tests, 6-34
- Payload Loopback, 6-28
- PC, COM port cable, C-4
- peer-to-peer calling, 1-4
- performance statistics, 5-47, 6-2
 - clearing, 5-48
- Phone Number, 3-44, 3-45
- physical
 - data port options, 3-37
 - DSX-1, 3-42
 - ISDN options, 3-44
 - tests, 6-26
- pin assignments
 - COM port, C-3
 - to-LAN cable, C-8
 - to-PC or terminal/printer cable, C-4
 - COM port-to-router
 - 1-slot unit, C-5
 - NAM, C-6
 - Ethernet port, C-13
 - ISDN DBM connector, C-14
 - modem connector, C-14
 - Port-1 V.35 connector, C-9
 - T1 cable, C-12
 - T1 line interface cable, C-13
 - V.35 crossover cable, C-10
- Ping test, 6-35
- placing a test call, 5-66
- PLB, 6-28
- Policing, Traffic, 1-5, 3-26
- Port
 - (DTE) Initiated Loopbacks, 3-40
 - Access Level, 3-90, 3-93, 4-3
 - assigning port to network or DSX-1 time slots, 3-58
 - assignment, clearing, 3-59
 - Base Rate, 3-38
 - bursting, 1-5
 - communication, options, 3-88
 - control leads, 5-10
 - Ethernet, connector pin assignments, C-13
 - Ethernet interface status, 3-86
 - LED, 5-9
 - modem, options, 3-92
 - Status, data ports, 3-37
 - Use, 3-37, 3-88, 3-92

- PPP, 3-92, 3-94
- previous recent cause values, 5-39
- Primary Clock
 - Failed, 5-23, 6-11
 - Source, 3-30
- Primary Destination
 - DLCI, 3-67
 - EDLCI, 3-67
 - Link, 3-67
- Primary Frame Relay Link, 3-74, 3-75
- Primary Link RIP, 3-75
- printed reports, 9-7
- printer, COM port cable, C-4
- problem indicators, 6-2
- product-related documents, xi
- Profile ID (SPID), 3-44
- profiles, entering, 3-48
- Proprietary
 - Caller Identification Method, 3-50, 4-5
 - RIP, 3-75
- Protocol
 - address resolution, 1-2, 3-87
 - Link, 3-92, 3-94
 - LMI, 3-60
 - Point-to-Point (PPP), 3-92, 3-94
 - Routing Information (RIP), 3-75, 3-91
 - Serial Line, IP (SLIP), 3-92, 3-94
 - Simple Network Management (SNMP), 3-76
- Proxy ARP, 3-87
- PVC
 - availability, 1-5
 - backup over network interface, 3-23
 - connection status, 5-30
 - connections, 3-66
 - total number, 1-3
 - Loopback, 6-23
 - Management, 3-72
 - total number dedicated, 1-3
 - name, 3-71, 3-82
 - tests, 6-22
 - troubleshooting problems, 6-16

Q

- quality of service, 3-65
- Quick Reference, 3-4

R

- ratios, FDR and DDR, 1-2
- remote loopbacks, 6-31, 6-33
- Repeater Loopback, 6-29
- reports, Network Health, 9-7
- reset, last time, 5-18
- resetting
 - statistics, 5-48
 - the unit, 6-3
 - unit default configuration options, 6-4
- restoring communication with a misconfigured unit, 6-4
- retrieving statistics, 5-73
- Return (Enter) key, 2-6
- revision, software and hardware, 5-3, 5-4
- RFC 1213 and 1573, B-2
- RFC 1315, B-2
- RFC 1406, B-2
- RFC 1604, B-2
- RFC 1659, B-2
- RFC 1757, B-2
- RFC 2021, B-2
- RFC 2128, B-2
- right arrow key, 2-6
- RIP, 1-2, 3-9, 3-91, 5-46
- RJ11 modem connector, C-14
- RJ48C network cable, C-12
- RLB, 6-29
- RMON
 - alarm and event defaults, B-18
 - Specific Traps, B-16
 - Traps, 3-84
 - user history collection, 1-5
- router
 - assist feature, 1-4, 3-11, 5-63
 - independence, 1-2, 3-25
 - setting up to receive RIP, 3-9
- Routing
 - Information Protocol (RIP), 3-91
 - IP, table, 5-45
 - table, 1-6
- RTS, control lead, 5-10
- running reports, 9-6
- RXD, control lead, 5-10

S

- Sampling, SLV Inband and Interval, 3-28
- saving configuration options, 3-7
- screen
 - area, 2-5
 - function keys area, 2-5
 - how to navigate, 2-6
- scrolling through valid selections, 2-9
- Secondary Clock
 - Failed, 5-23, 5-24, 6-11
 - Source, 3-31
- security, 1-2, 2-1, 2-2, 3-6, 4-1
 - SNMP NMS, options, 3-80
- selecting
 - a field, 2-9
 - from a menu, 2-8
- Self-Test Results messages, 5-18
- Send
 - All Ones on DSX-1 Failure, 3-43
 - and monitor test pattern, 6-34
 - Pattern, 6-24
- serial number, NAM, 5-3
- Service, A
 - Profile ID (SPID), 3-44, D-7
- service level
 - management, 1-7
 - management (SLM), 1-1
 - reports, 9-6
 - verification
 - configuring, 3-28
 - statistics, 5-49
 - verifier (SLV), 1-1
- Session
 - Access Level, 3-78, 4-6, 4-8
 - ending, 2-3
 - starting, 2-2
- Set DE, 3-73
- setting Date & Time (system clock), 3-9
- setting up
 - auto-configuration, 3-12
 - DBM, 3-16
 - ISDN link profiles, 3-48
 - modem, 3-10
 - SNMP trap managers, 3-80
 - so router can receive RIP, 3-9

- SIG, LED, 5-9
 - SLA, 1-2, 1-7
 - SLIP, 3-92, 3-94
 - SLM, ix, 1-7
 - (service level management), 1-1
 - OpenLane, 7-1
 - SLV
 - (service level verifier), 1-1
 - configuring, 3-28
 - Delivery Ratio, 3-28
 - DLCI Down on Timeout, 3-28
 - Packet Size, 3-29
 - performance statistics, 5-49
 - Round Trip Latency
 - Clearing Event Threshold, 3-29
 - Error Threshold, 3-29
 - Sample Interval (secs), 3-28
 - Synchronization Role, 3-29
 - Timeout, Error Event Threshold, 3-28, 3-29
 - SNMP
 - assigning community names/access levels, 4-10
 - limiting access, 4-9, 4-11
 - Management, 3-76, 4-9
 - NMS security, options, 3-80
 - Number of Managers, 3-80
 - setting up Trap Managers, 3-80
 - trap event log, 5-62, 6-14
 - Traps, 3-81
 - downloading, B-2
 - setting up DBM to send, 3-22
 - standards, B-8
 - supported, 6-2
 - software
 - changing, 5-72
 - ISDN BRI DBM, 5-71
 - downloading, 5-68
 - revision
 - DBM, 5-4
 - NAM, 5-3
 - Source
 - DLCI, 3-66
 - EDLCI, 3-66
 - Link, 3-66
 - Spacebar, 2-6
 - specifications, technical, D-1
 - SPID, 3-44, D-7
 - Standard_out RIP, 1-2
 - standards compliance for SNMP Traps, B-8
 - starting
 - a session, 2-2
 - a test, 6-20
 - statistics, 1-5, 5-47
 - DBM call, 5-60
 - elements, 9-3
 - selecting performance intervals for display, 5-57
 - uploading to an NMS, 5-73
 - Status
 - Call, 5-37
 - DBM interface, 5-35
 - DLCI, 5-28
 - Enquiry, LMI, 3-27, 3-61
 - Health and, 5-19
 - information, 5-17
 - LED, 5-7
 - Line, 5-36
 - menu/branch, 2-4
 - PVC connection, 5-30, 5-32
 - test messages, 5-26
 - timeslot assignment, 5-33
 - Stop Bits, 3-89
 - stopping a test, 6-20
 - Subnet Mask, 3-73, 3-86, 3-91, 3-94, 3-95
 - Node, 3-70
 - suggestions, user documentation, A
 - summary, network report, 9-7
 - Switch Type, 3-45
 - switching
 - between screen areas, 2-8
 - to new software, 5-72
 - System
 - Alarm Relay, 3-32
 - turning off, 5-74
 - and test status messages, 5-18
 - configuring options, 3-25
 - displaying information, 5-3
 - entering information, 3-9
 - Frame Relay and LMI, options, 3-25
 - General options, 3-30
 - last reset, 5-18
 - messages, 2-5
 - Name, Contact, and Location, 5-3
 - setting the clock (data & time), 3-9
- ## T
- T1
 - Canadian line interface cable, C-13
 - LMI Heartbeat, 3-27, 3-62
 - mass termination cable, C-12
 - network cable, C-12, C-13
 - network interface options, 3-33
 - T2, LMI Inbound Heartbeat, 3-27, 3-62
 - T3, LMI N4 Measurement Period, 3-27, 3-62
 - Tab key, 2-6
 - Tc, 3-64
 - TCP, 5-68
 - technical specifications, D-1
 - Telnet
 - limiting access, 4-6
 - Session, 4-6
 - user interface options, 3-77

Terminal

- COM port cable, C-4
- Port Use, 3-88, 3-92

Test

- Call, 6-25
- menu/branch, 2-4
- Mode, 5-8
- Status messages, DBM, 5-26

Tests, 1-3

- aborting, 6-21
- available, 6-18
- Connectivity, 6-25
- Data Channel Loopback, 6-32
- DBM, 6-19
- DTE Loopback, 6-30
- Duration, 3-30
- IP Ping, 6-35
- Lamp, 6-36
- Line Loopback, 6-27
- pattern, 6-34
- Payload Loopback, 6-28
- physical, 6-26
- PVC, 6-22
- PVC Loopback, 6-23
- Remote Line Loopback, 6-31, 6-33
- Repeater Loopback, 6-29
- Send/Monitor Pattern, 6-24
- starting or stopping, 6-20
- Test Call, 6-25
- Timeout, 3-30, 6-19

throughput, 1-5**time, setting, 3-9****time slot assignments, synchronous data port to network or DSX-1, 3-58****time slots, 3-50****Timeout**

- Inactivity, 3-79, 3-90, 3-93
- Test, 6-19

timers, setting backup, 3-21**timeslot assignment, status, 5-33****timeslot assignments**

- DSX-1, 5-34
- network, 5-33

Trace Log, LMI, 6-6**trademarks, A****Traffic Policing, 1-5, 3-26****Training, A****transferring data, 5-73****Transmit Clock**

- Invert, 3-38
- Source, 3-39

Transmit Timing, 3-34**Trap**

- Dial-Out, 3-84
- Disconnect, 3-85
- Event Log, 1-6, 5-62, 6-14
- Managers, Number of, 3-81

Traps

- authenticationFailure, B-9
- dialControl, B-17
- dialCtlPeerCall, B-17
- DLCI, 3-84
- Enterprise Specific, 3-83, B-13
- General, 3-82
- Link, 3-83
- Link Interfaces, 3-83
- linkUp and linkDown, B-10
- RMON, 3-84
- RMON Specific, B-16
- SNMP and dial-out, options, 3-10, 3-81
- standards, B-8
- supported, 6-2
- warmStart, B-9

Trend reports, 9-7**troubleshooting, 6-1**

- creating a management link, 3-70
- device problems, 6-14
- frame relay PVC problems, 6-16
- ISDN BRI DBM problems, 6-17
- management link, 6-5
- PVC, 1-6
- tables, 6-14

TruePut technology, 1-2**TS Access Management Link, 3-70, 3-71**

- Access Level, 3-72, 4-8
- limiting Telnet access, 4-6, 4-8

TST LED, 5-8**TTL, 5-46****turning off system alarm relay, 5-74****TXD, control lead, 5-10****Type, Access, 3-81****U****UNI, 1-2, 3-26, 3-27, 3-61, 3-62****upgrade, ISDN BRI DBM, 5-71****upgrading system software, 5-70****uploading data, 5-73****user history**

- adding files, 8-13
- installing files, 8-15
- monitoring DLCI, 8-16
- statistics gathering, 1-5

user interface, 2-1

- cannot be accessed, 6-15
- communication port, options, 3-88
- resetting/restoring access, 6-4
- Telnet session, 3-77

user-defined history, 8-13

V

V.35

- connector, C-9
- crossover cable, C-10
- straight-through cable, C-10

V.54 Loopback, 3-35, 5-20, 5-26, 6-32

Value Out of Range message, 3-63, 3-64

variable-bindings, B-11, B-16

VCI, 1-6

verifying

- DBM setup, 5-67
- ISDN lines, 5-67
- modem setup, 5-64

viewing

- LEDs, 5-5, 5-6
- packet capture results, 6-6

virtual path or channel identifier, 1-6

VPI, 1-6

W

warmStart

- events, General Traps, 3-82
- trap, B-9

warranty, A

Web-site

- access to documentation, xii
- glossary, x

Y

Yellow

- Alarm, B-11
- Signal, 5-7
- at DSX-1 or Network, 5-25, 6-13
- at ISDN PRI, 5-25