FrameSaver® SLV Multiservices Access Unit

Models 9191, 9192, and 9195

USER'S GUIDE

Document No. 9191-A2-GB20-00

August 2000

PARADYNE®

Notice

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

Patent Notification

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

Contents

4 Dial Backup Modules

5 Application Modules

6 Security and Logins

7 Operation and Maintenance

8 Troubleshooting

9 Setting Up OpenLane for FrameSaver Devices

10 Setting Up NetScout Manager Plus for FrameSaver Devices

11 Setting Up Network Health for FrameSaver Devices

A Menu Hierarchy

B SNMP MIBs and Traps, and RMON Alarm Defaults

C Connectors, Cables, and Pin Assignments

D Technical Specifications

E Equipment List

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 9191, 9192, or 9195, a T1 Frame Relay Service Level Verifier (SLV) Multiservices Access (MSA) unit. The device provides a highly modular and scalable, cost-effective system for performing frame relay service level management, while offering access to a variety of voice, video, and non-frame relay digital applications – all in one housing.

The FrameSaver SLV 9192 unit is a FrameSaver SLV 9191 Network Access Module (NAM) that is in a 2-slot housing; the FrameSaver SLV 9195 unit is a FrameSaver SLV 9191 NAM in a 5-slot housing. The FrameSaver SLV 9192/9195 unit incorporates FrameSaver Service Level Verifier (SLV) functionality.

This document 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	*About the FrameSaver SLV.* Describes the system solution and lists the FrameSaver unit's features.
Chapter 2	*User Interface and Basic Operation.* Shows how to navigate the menu-driven user interface.
Chapter 3	*Configuration.* Provides configuration information for the FrameSaver unit.
Chapter 4	*Dial Backup Modules.* Provides information about optional ISDN BRI and PRI DBMs, and their configuration.
Chapter 5	*Application Modules.* Provides information about optional voice, synchronous data, and OCU-DP APMs, and their configuration.

Section	Description
Chapter 6	*Security and Logins.* Provides procedures for controlling access to the FrameSaver unit and setting up logins.
Chapter 7	*Operation and Maintenance.* Provides procedures to display unit identification information and perform file transfers, as well as how to display and interpret status and statistical information.
Chapter 8	*Troubleshooting.* Provides device problem resolution, alarm, and other information, as well as troubleshooting and test procedures.
Chapter 9	*Setting Up OpenLane for FrameSaver Devices.* Identifies where installation and setup information is located and how FrameSaver units are supported.
Chapter 10	*Setting Up NetScout Manager Plus for FrameSaver Devices.* Describes setup of the NetScout Manager Plus application so it supports FrameSaver units.
Chapter 11	*Setting Up Network Health for FrameSaver Devices.* Describes setup of Concord's Network Health application so reports can be created for FrameSaver units, and identifies those reports that apply to FrameSaver units.
Appendix A	*Menu Hierarchy*. Contains a graphical representation of how the user interface screens are organized.
Appendix B	*SNMP MIBs and Traps, and RMON Alarm Defaults.* Identifies the MIBs supported and how they can be downloaded, describes the unit's compliance with SNMP format standards and with its special operational trap features, and describes the RMON-specific user history groups, and alarm and event defaults.
Appendix C	*Connectors, Cables, and Pin Assignments.* Shows the rear panel, tells what cables are needed, and provides pin assignments for interfaces and cables.
Appendix D	*Technical Specifications*.
Appendix E	*Equipment List.*
Index	Lists key terms, acronyms, concepts, and sections.

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

Product-Related Documents

Document Number	Document Title
Paradyne FrameSaver Documentation:	
9000-A2-GN14	*2-Slot and 5-Slot Housing Wall Mounting Kit Installation Instructions*
9000-A2-GN15	*2-Slot Housing Installation Instructions*
9000-A2-GN16	*5-Slot Housing with AC Power Supply Installation Instructions*
9000-A2-GN17	*5-Slot Housing and 9000 Series Access Carrier AC Power Supply Installation Instructions*
9000-A2-GN1B	*DC Power Supply for 5-Slot Housing Installation Instructions*
9000-A2-GN1C	*5-Slot Housing with DC Power Supply Installation Instructions*
9000-A2-GX42	*Affidavit Requirements for Connection to Digital Service*
9098-A2-GN10	*FrameSaver SLV ISDN Dial Backup Module (DBM) Installation Instructions*
9109-A2-GN10	*9109 Sync Data Application Module (APM) Installation Instructions*
9109-A2-GN11	*9109 E&M Analog Voice Application Module (APM) Installation Instructions*
9109-A2-GN12	*9109 FXS Analog Voice Application Module (APM) Installation Instructions*
9109-A2-GN14	*9109 FXO Analog Voice Application Module (APM) Installation Instructions*
9109-A2-GN15	*9109 OCU-DP Application Module (APM) Installation Instructions*
9191-A2-GL10	*FrameSaver SLV Multiservices Access Unit, Models 9191, 9192, and 9195, Quick Reference*
9191-A2-GN10	*FrameSaver SLV 9191 Multiservices Network Access Module (NAM) Installation Instructions*
Paradyne OpenLane NMS Documentation:	
7800-A2-GZ41	*OpenLane 5.x Service Level Management for UNIX Quick Start Installation Instructions*
7800-A2-GZ42	*OpenLane 5.x Service Level Management for Windows NT Quick Start Installation Instructions*

Document Number	Document Title
NetScout Documentation:	
2930-170	*NetScout Probe User Guide*
2930-610	*NetScout Manager/Plus User Guide*
2930-620	*NetScout Manager/Plus & NetScout Server Administrator Guide*
2930-788	*NetScout Manager Plus Set Up & Installation Guide*
Concord Communications Documentation:	
09-10010-005	*Network Health User Guide*
09-10020-005	*Network Health Installation Guide*
09-10050-002	*Network Health – Traffic Accountant Reports Guide*
09-10070-001	*Network Health Reports Guide*

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

To order a paper copy of this manual:

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

About the FrameSaver SLV

1

This chapter includes the following:

- *System Overview*
- *FrameSaver SLV 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

The FrameSaver SLV unit is a multiservices access (MSA) unit that provides a flexible, completely modular approach to handling frame relay performance monitoring, service level management, analog/digital voice, video, fax, and data. Using either the 2-slot or 5-slot housing, this solution consists of a 9191 Network Access Module (NAM) to terminate circuit(s) from the service provider, ISDN dial backup capability, if desired, and a variety of Application Modules (APMs).

FrameSaver SLV 9191 NAMs/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 units are also compatible with the OpenLane SLM system, the NetScout Manager Plus application, Netscout probes, and Concord Communication's Network Health software.

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.

FrameSaver SLV Features

The FrameSaver SLV MSA unit provides the following features:

- **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 (both within and above CIR) 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.
- **Modular Design.** Provides upgradability (e.g., you can start with a 2-slot housing, and move the NAM and APM to a 5-slot housing at a later date). Any NAM or APM can be physically removed from one housing and moved to another.
- **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.
  - Backup Configuration – When an ISDN DBM (Integrated Services Digital Network Dial Backup Module) is installed, provides automatic configuration of an alternate route and DLCI for automatically created PVCs. When the automatic backup feature is enabled, backup and restoration occur automatically.

- **Choice of Multislot Housings.** Provides the flexibility of using either a 2-slot or 5-slot housing.
  - The 2-slot housing holds one 9191 NAM, and one APM.
  - The 5-slot housing holds one 9191 NAM, and up to four APMs. A redundant load-sharing AC or DC power supply can also be ordered for the 5-slot housing.

  Order a Model 9192 to get the 2-slot housing, and a Model 9195 for the 5-slot housing. The housing is shipped with the NAM already installed.

- **Integral Modem.** Provides an internal 14.4 kbps modem to support dialing in to the system for out-of-band management and automatic dialing out of SNMP traps.

- **Optional ISDN Backup.** When an ISDN BRI or PRI DBM (Basic Rate Interface or Primary Rate Interface Dial Backup Module) is installed:
  - 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. Supports alarm generation and call security, as well.
  - Provides automatic configuration of an alternate route and DLCI for automatically created PVCs at either the remote site or central site. When the automatic backup feature is enabled, backup and restoration occur automatically. Alarm generation and call security are also supported by units with ISDN backup capability.

  FrameSaver units can be equipped with a BRI DBM, which supports up to two B-channels, each having a different destination, or a PRI DBM, which supports up to 23 B-channels.

- **Optional Multiservices APMs.** Provides optional multiservices Application Modules, which can be installed in any combination, allowing expansion capability as your network needs grow. As additional DTE or voice ports are needed for your network applications, APMs can be added. The following APMs are available:
  - **Synchronous Data APM** – Adds four additional data ports. Each port can be set for V.35, RS-530A, RS-449, or X.21 operation.
  - **FXO voice APM** – Supports voice traffic and the FXO, FXODN, FXODN with Wink, and DPT operation modes. This APM passes Caller ID information when supplied by the network, and supports up to eight ports.
  - **FXS voice APMs** – Supports voice traffic and the FXS, FXSDN, FXSDN with Wink, and DPO operation modes. This APM provides its own –48 VDC battery and low-frequency AC ringing power, and supports up to eight ports.
  - **E&M voice APM** – Supports both voice and analog private line (APL) modem traffic. This APM provides its own –48 VDC battery power, and contains eight ports.
  - **OCU-DP APM** – Supports aggregation of multiple DDS circuits onto a single T1 line and video conferencing. This APM is available in either a 2-port or 6-port model.

- **Optional Wall-Mount Bracket.** Allows one 5-slot, or up to two 2-slot housings to be mounted on a wall.
- **Hot Swapping.** Provides the ability to insert and remove NAMs and APMs without powering-off the system, and without having to reconfigure the cards each time they are moved.
- **Standards-Based Protocol Support.** Supports the three standard LMI protocols for communication over the frame relay interface, as well as the two link-layer protocols for connection to an external SNMP manager or network device via the COM or modem port.
- **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.
- **Maximum Number of PVCs and Management PVCs Supported.**

Feature	FrameSaver SLV
Through Connections (PVCs)	120
Dedicated Management PVCs	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.
- **SNMP Management Capability.** Provides network management via an external Simple Network Management Protocol management system using industry-standard and Paradyne-specific MIB (Management Information Base) objects.
- **IP Management Connectivity.** Supports management connectivity within an IP (Internet Protocol) network for up to 300 IP routes to provide IP routing for SNMP, Telnet, and FTP messages without requiring direct connections.
- **Security.** Provides multiple levels of security to prevent unauthorized access to the unit.
- **Extensive Monitoring Capability.** Provides status information to monitor and evaluate the system’s and network’s operation via the Status menu, performance statistics, LEDs and control leads.
- **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.

- **User-Selectable Ranges for Frame and Burst Sizes**. Provides user configurability for statistical data collection using the OpenLane system to set upper and lower limits for data collection. The accumulated data is used for graphs and reports, and to trigger alarms.

- **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.

- **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.

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

- **LMI Packet Capture.** Provides a way to upload data that has been captured in a trace file so the data can be uploaded and transferred to a Network Associates Sniffer for analysis.

- **Configuration Upload/Download and Software Download Capability.** Provides quick transfer of configuration options to and from nodes and software downloads while the unit is running using a standard file transfer protocol (FTP). Two software loads can be stored.

- **Dual Flash Memory.** Allows software upgrades while the system is up and running. Two software loads can be stored, to be implemented at the user's discretion for quick switching of the system's configuration.

- **Menu-Driven User Interface.** Provides an easy to use, menu-driven interface to locally or remotely configure, manage, maintain, and access the system's extensive diagnostic capability.

- **Multiple DTE Ports.** Provides two data ports that have standard connectors. Port-1 is dedicated to frame relay data, but Port-2 can be configured for frame relay or synchronous data. Additional ports can be added when a Synchronous Data APM is added to the system.

- **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.

OpenLane SLM System

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

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

Some of the OpenLane system's features include:

- Real-time performance graphs provide exact performance measurement details (not averages, which can skew performance results) of service level agreement (SLA) parameters.
- Historical SLV graphs provide service level management historical reports so frame relay SLAs can be verified.
- Diagnostic troubleshooting provides an easy-to-use tool for performing tests, which include end-to-end, PVC loopback, connectivity, and physical interface tests.
- Basic configuration allows you to configure FrameSaver devices, and set RMON alarms and thresholds. Network DLCI Circuit IDs can also be assigned.
- Automatic SLV device and PVC discovery allows all SLV devices with their SLV Delivery Ratio configuration option enabled to be discovered automatically, along with their PVCs.
- A FrameSaver unit can be reset from the OpenLane system.
- Firmware downloading provides an easy-to-use tool for downloading to an entire network or a portion of the network.
- On-demand polling of FrameSaver devices, and SNMP polling and reporting are available.
- Multiple maintenance schedules allow for the scheduling of more than one periodic maintenance period, and provides a report for each scheduled task.
- Multiple Circuit IDs allow multiple access levels so network service providers can offer their customers service level-specific access to network management information, and so end users can have open access to network management information without losing control of their network(s).

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:

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** (Exit) 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                       9191
Device Name: Node A                                           05/26/2000 23:32
Slot: 1  Type: T1 FR NAM

                                     MAIN MENU

                                    Status
                                    Test
                                    Configuration
                                    Auto-Configuration
                                    Control

------------------------------------------------------------------------------
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.

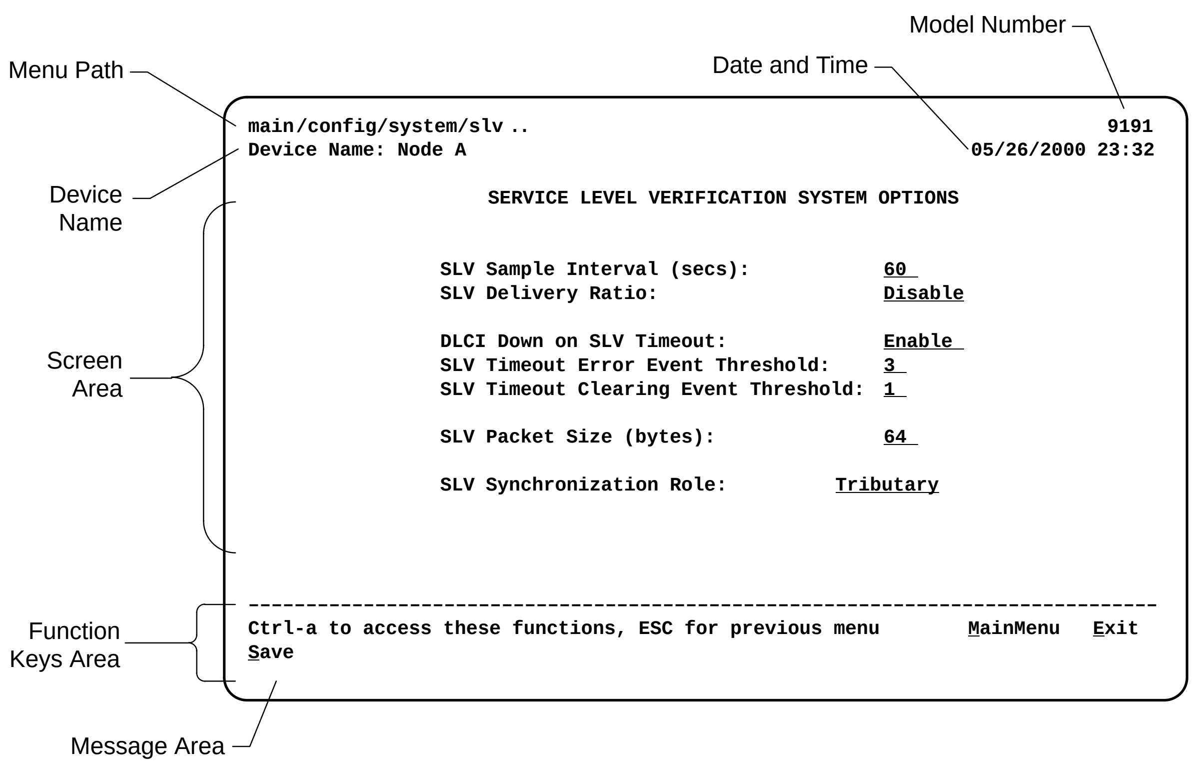
See Appendix A, *Menu Hierarchy*, for a pictorial view of the menu hierarchy, which represents the organization of the FrameSaver unit's menus and screens.

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.
9191	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	MainMenu	Return to the Main Menu screen.
E or e	Exit	Terminate the asynchronous terminal session.
N or n	New	Enter new data.
O or o	Modify	Modify existing data.
L or l	Delete	Delete data.
S or s	Save	Save information.
R or r	Refresh	Update screen with current information.
C or c	ClrStats	Clear network performance statistics and refresh the screen. Variations include: ■ ClrSLV&DLCIStats for clearing SLV and DLCI statistics. ■ ClrLinkStats for clearing frame relay link statistics. ■ ClrDBMStats for clearing DBM call statistics.
U or u	PgUp	Display the previous page.
D or d	PgDn	Display the next page.

Selecting from a Menu

▶ Procedure

To select from a menu:

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

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

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

▶ Procedure

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

Switching Between Screen Areas

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

▶ Procedure

To switch to the function keys area:

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

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

Selecting a Field

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

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

Entering Information

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

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

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

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

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

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

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

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

Configuration

3

This chapter includes the following:

- *Configuring the Physical Interfaces*
  - *Configuring the Network Interface*
  - *Configuring a User Data Port*
  - *Configuring the DSX-1 Interface*
- *Assigning Time Slots/Cross Connections*
  - *Assigning Frame Relay Time Slots to the Network Interface*
  - *Assigning DSX-1 Time Slots to the Network Interface*
  - *Assigning Synchronous Data Ports 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 Communication Port*
  - *Configuring the Modem Port*

If your system has an ISDN DBM and/or APM installed, see the following chapter(s) for additional information:

- For an ISDN DBM, see Chapter 4, *Dial Backup Modules*.
- For an APM, see Chapter 5, *Application Modules*.

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 unit with the optional ISDN backup feature, analog voice APMs, and an OCU-DP APM.

Configuration Menu

```
main/config                                                                 9191
Device Name: Node A                                              3/26/2000 23:32

                           CONFIGURATION EDIT/DISPLAY

                             System
                             Network
                             DSX-1
                             Data Ports
                             ISDN
                             Voice Ports
                             OCU-DP Ports
                             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 Multiservices Access Unit, Models 9191, 9192, and 9195, 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.

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 3-10, DLCI Record Options, and Table 3-13, 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 6, *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 3-19, 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.

See *Setting Up Call Directories for Trap Dial-Out* when trap dial-out is desired. See *Limiting Dial-In Access via the Modem Port* in Chapter 6, *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 Automatic Dial-Out to Send SNMP Traps

For generated SNMP traps to initiate a call, a modem port connection must be established.

▶ Procedure

To configure dial-out of SNMP traps:

1. Select Modem Port.

   Main Menu → Configuration → Management and Communication → Modem Port

2. Configure the following:

   — Disable Dial-In Access if only trap dial-out is wanted.

   — Set Port Use to Net Link. See Table 3-19, Modem Port Options, when configuring the modem port. Save any change(s).

3. Select SNMP Traps.

   Management and Communication → SNMP Traps

4. Configure the following:

   — Enable SNMP Traps, Trap Dial-Out to enable automatic call initiation (dial out) to send an SNMP trap message, and Call Retry to hold the trap if the call cannot be completed.

   — Assign SNMP Trap Managers, and specify the IP address of the NMS that traps will be sent to when dialing out.

   — Select Modem as the Destination and select the desired SNMP trap categories.

   — Specify whether to disconnect immediately after dialing out traps, or to allow a manual disconnect to occur (a connection remains until manually disconnected).

   You can also set the delay time and specify an alternate dial-out directory, if desired.

5. Save your changes.

See Table 3-17, SNMP Traps and Trap Dial-Out Options, when configuring SNMP traps.

Setting Up an ISDN DBM

See *Setting Up Dial Backup* in Chapter 4, *Dial Backup Modules*, for this information.

Setting Up an APM

See *Configuring APM Ports* in Chapter 5, *Application Modules*, for this information.

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.

Main Menu → Auto-Configuration

Auto-Configuration Screen Example

```
main/auto-configuration                                                      9191
Device Name: Node A                                                3/26/2000 23:32

                               AUTO-CONFIGURATION


              Frame Relay Discovery Mode:          1MPort
              Automatic Backup Configuration:      Enable















--------------------------------------------------------------------------------
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 the unit does not have the ISDN DBM feature installed, Automatic Backup Configuration does not appear (see *Setting Up Automatic Backup Configuration* in Chapter 4, *Dial Backup Modules*, 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:

Table 3-1. Frame Relay Discovery Modes (1 of 2)

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	▪ 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.

Table 3-1. Frame Relay Discovery Modes (2 of 2)

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. 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.

Setting Up Back-to-Back Operation

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

Changing Operating Mode

When setting up back-to-back operation:

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

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

▶ Procedure

To set up back-to-back operation:

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

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

▶ Procedure

To return the unit to normal operation:

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

Configuration Option Tables

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

The following configuration option tables are included:

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

Configuring the Overall System

The System menu includes the following:

- Frame Relay and LMI
- Service Level Verification
- General

Configuring Frame Relay and LMI for the System

Select Frame Relay and LMI from the System menu to display or change the Frame Relay and LMI options for the entire system (see Table 3-2).

Main Menu →Configuration →System →Frame Relay and LMI

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

Table 3-2. 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 (see *Setting the Criteria for Automatic Backup* in Chapter 4, *Dial Backup Modules*). 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 3-2. 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 *not* 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.
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 3-2. System Frame Relay and LMI 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.

Configuring Service Level Verification Options

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

Main Menu → Configuration → System → Service Level Verification

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

SLV Sample Interval (secs)
Possible Settings: **10 – 3600** Default Setting: **60**
Sets the inband communications interval between FrameSaver SLV devices. Inband communications are used to pass frames that calculate latency, as well as transmission success and other SLV information. **10 – 3600** – Sets the SLV Sample Interval (secs) in seconds.
SLV Delivery Ratio
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether communication of Frame and Data Delivery Ratios (FDR/DDR) between FrameSaver SLV devices is enabled. To use this capability, both ends of all PVCs must be FrameSaver SLV devices. If some of the units are FrameSaver 9124s or 9624s, they must be running software version 1.2 or higher. **Enable** – An extra byte for FDR/DDR statistics collection is included with each frame, which is used at the receiving end to determine the amount of data dropped by the network. **Disable** – Extra byte is not included.
DLCI Down on SLV Timeout
Available Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether 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 3-3. Service Level Verification Options (2 of 2)

SLV Timeout Clearing Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **1**
Specifies the number of consecutive SLV messages that must be received before the DLCI Inactive status is cleared. **1 – 20** – Sets the limit for the clearing event.

Configuring General System Options

Select General from the System menu to configure the general system configuration options (see Table 3-4).

Main Menu →Configuration →System→General

Table 3-4. 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 accidently commanded to execute a disruptive test on the interface providing the management access, control can be regained after the timeout expires, terminating the test. **Disable** – Loopback and pattern tests must be manually terminated.
Test Duration (min)
Possible Settings: **1 – 120** Default Setting: **10**
Specifies the maximum duration of the tests. *Display Conditions* – This option only appears when Test Timeout is set to Enable. **1 – 120** – Sets the Test Timeout period in minutes (inclusive).

Table 3-4. General System Options (2 of 3)

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.
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 3-4. 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.

Display Conditions – This option only appears when the NAM is installed in a 5-slot housing.

Alarm conditions are:

- Abnormal Station Code on any OCU-DP port
- Alarm Indication Signal (AIS) received at the Network, DSX-1, or PRI interface
- An APM is inserted that does not match the configuration
- Continuous Loss of Signal (LOS) condition at the Network, DSX-1, PRI interface, or OCU-DP port
- CTS Down
- DBM Download Required
- DBM BRI Card Failed
- DDS Network Failure on any OCU-DP port
- Device Fail
- DLCI Down
- DTR Down
- Excessive Error Rate (EER) detected at the Network or PRI interface
- Failure of an APM
- Internal Modem Failed
- ISDN Network Failure
- LMI Down
- Loss of Loop Timing on any OCU-DP port
- Network Communication Link Down
- Out of Frame (OOF) at Network, DSX-1, or PRI interface, or for a 64k CC Loop on any OCU-DP port
- Primary or Secondary Clock Failure
- Power Supply/Fan Failure
- RTS Down
- Self-Test Failure
- 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 the Physical Interfaces

Characteristics for the following physical interfaces can be configured:

- Network Interface
- User Data Port(s)
- DSX-1 Interface
- ISDN (To configure the ISDN DBM interface, see *Setting Up the DBM Physical Interface* in Chapter 4, *Dial Backup Modules*.)
- Voice Ports and OCU-DP Ports (To configure analog voice or OCU-DP APM ports, see *Configuring APM Ports* in Chapter 5, *Application Modules*.)

Configuring the Network Interface

When configuring the physical characteristics for the network interface, select Physical from the Network menu (see Table 3-5).

Main Menu → Configuration → Network → Physical

Table 3-5. Network Physical Interface Options (1 of 4)

Interface Status
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the interface selected in the Network field is available for use. **Enable** – The interface is available. **Disable** – The interface is not available for use. When the interface is disabled, any existing cross-connect assignments for this interface will be cleared, no alarms or traps for this interface will be generated, no configuration options will be displayed, and all LEDs associated with this interface will remain off.
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.

Table 3-5. Network Physical Interface Options (2 of 4)

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.
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. *Display Conditions* – 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 3-4, 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.

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

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.
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. *Display Conditions* – 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.
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. *Display Conditions* – 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 3-5. 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. *Display Conditions* – 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 3-6).

Main Menu → Configuration → Data Ports → Physical

The Data Port Physical Options screen appears for Port 1 of the first slot containing a NAM. If desired, enter the slot and port number of another data port.

Use this set of options to configure each port on a Sync Data APM.

Table 3-6. Data Port Physical Interface Options (1 of 5)

Port Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
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. ▪ Existing TDM cross-connect assignments associated with the port will be cleared. The message **This action will clear any Cross Connections for the Port. Are You Sure? <u>No</u>** appears. If you select: **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. *Display Conditions* – This option only appears for user data Port-2 on the NAM. **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 3-6. Data Port Physical Interface Options (2 of 5)

Port Type
Possible Settings: **E530, V.35, RS449, X.21** Default Setting: **V.35**
Selects the type of port to be used for the user data port. *Display Conditions* – This option only appears for Port-2 on the NAM, when Port Use is set to Frame Relay, and for flexible user data ports on an synchronous data APM. **E530** – The port is an EIA-530A-compatible DCE. An EIA-530-compatible DTE can be directly connected to the DB25 connector. **V.35** – The port is a V.35-compatible DCE. A V.35-compatible DTE can be connected to the DB25 connector by using an adapter. **RS449** – The port is an RS449-compatible DCE. An RS449-compatible DTE can be connected to the DB25 connector by using DB37-to-DB25 adapter. **X.21** – The port is a V.11/X.21-compatible DCE. A V.11/X.21-compatible DTE can be connected to the DB25 connector by using an adapter.
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. *Display Conditions* – This option only appears for Port-2 on the NAM, when Port Use is set to Frame Relay, and for flexible user data ports on an synchronous data APM. **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. *Display Conditions* – This option only appears when Port Use is set to Synchronous Data. **Nx64** – The base rate for the port is 64 kbps. **Nx56** – The base rate for the port is 56 kbps.
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.

Table 3-6. Data Port Physical Interface Options (3 of 5)

Invert Transmit Clock
Possible Settings: **Auto, Enable, Disable** Default Setting: *For user data ports on the NAM:* **Auto** *For user data ports on an APM:* **Disable**
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. *Display Conditions* – This option is only available on user data ports on the NAM. **Enable** – Phase inverts the TXC clock. Use this setting when long cable lengths between the FrameSaver unit and the DTE are causing data errors. **Disable** – Does not phase invert the TXC clock.
Monitor DTR
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the DTE Ready (DTR) circuit on the user data port will be used to determine when valid data communication is possible with the DTE. When 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.
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.

Table 3-6. Data Port Physical Interface Options (4 of 5)

Port (DTE) Initiated Loopbacks
When Port Use is set to Frame Relay: **Disable**, **Local** *When Port Use is set to Synchronous Data:* **Disable**, **DTPLB, DCLB, Both** Default Setting: **Disable**
Possible Settings: **Local**, **Disable** Default Setting: **Disable**
When Port Use is set to Frame Relay: 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. *Display Conditions* – This option does not appear when Port Type is set to X.21. **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. *When Port Use is set to Synchronous Data:* Allows local Data Terminal Loopbacks (DTPLBs) and remote Data Channel Loopbacks (DCLBs) to be controlled by the DTE connected to this port. *Display Conditions* – 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. *Display Conditions* – This option only appears 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 3-6. 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.) *Display Conditions* – This option only appears 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, Both** 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. *Display Conditions* – This option only appears 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. **Both** – 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 3-7).

Main Menu → Configuration → DSX-1

Table 3-7. 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 3-7. 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.

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 between various synchronous data interfaces. The system allows you to make the following cross connection assignments:

- Frame Relay Network Assignments
- DSX-1 to Network Assignments
- Synchronous Data Port Assignments
- Voice Port Assignments and OCU-DP Port Assignments (To configure cross connection assignments for analog voice ports or OCU-DP ports, see *Configuring APM Ports* in Chapter 5, *Application Modules*.)

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

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                                       9191
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       N118      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 VocAssign
```

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*tt*	This field represents time slot *tt* 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, and the VocAssign function key to go to the Voice Port Assignment 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 3-7, DSX-1 Physical Interface Options).

Value	Meaning
N*tt*	It represents time slot *tt* 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.
D*s*-1*p*/*tt*	Time slot *tt* of the DSX-1 interface in slot *s* is assigned to the network interface time slot identified right above it (N*tt*).

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

```
main/config/tslot_assign/dsx                                              9191
Device Name: Node A                                                5/26/2000 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       N118      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                         VocAssign    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 N*tt*, pressing the Spacebar causes this field's values to cycle through all valid DSX-1 time slots, starting with D*s*-*p*/*yy*, assuming it is unassigned. If D*s*-*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                                                9191
Device Name: Node A                                             5/26/2000 23:32

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

 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    FrAssign
```

For easy movement between screens, select the FrAssign function key to go directly to the Frame Relay Network Assignments screen, the DSXAssign function key to go to the DSX-1 to Network Assignments screen, and the VocAssign function key to go to the Voice Port Assignment 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 3-8 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 3-8. 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 3-8. 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
FXOl-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).	FXSl-idle
FXOl-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).	FXSl-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
FXSl-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).	FXOl-idle
FXSl-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).	FXOl-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 3-8. 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 Synchronous Data Ports to Network or DSX-1 Time Slots

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-2 on the NAM or a port on the Sync Data APM to:

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

Synchronous Data Port Assignment Screen Example

```
main/config/tslot_assign/sync_data/net                                     9191
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  S2P2      S2P1     Assigned

   N09      N10      N11      N12      N13       N14      N15      N16
Assigned Assigned Assigned Assigned Assigned  S3P2      S3P1     Available

   N17      N118     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  VocAssign  FrAssign
```

Value	Meaning
Assign To	Specifies either Net1 (network) or DSX1-1 (DSX-1) time slots.
N*tt* D*tt*	This field represents time slot *tt* of the network interface. This field represents time slot *tt* 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.
S*s*P2	Synchronous data port in slot *s* is assigned to the time slot.

For easy movement between screens, select the FrAssign function key to go directly to the Frame Relay Network Assignments screen, the DSXAssign function key to go to the DSX-1 to Network Assignments screen, and the VocAssign function key to go to the Voice Port Assignment screen.

Time Slot Assignment Rules:

- To assign a synchronous data port to network or DSX-1 time slots, the data port's Port Use option must be set for Synchronous Data (see Table 3-6, 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 3-7, DSX-1 Physical Interface Options).

▶ Procedure

1. Select the following menu selection sequence:

   Main Menu → Configuration → Time Slot Assignment → Sync Data Port Assignments

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 time slots to **Available** (unassigned).

Main Menu → Configuration → Time Slot Assignment → Clear Assignments

When Clear Assignments is selected, the **`Delete assignments for which slot?`** prompt appears.

To clear assignments for . . .	Select . . .
The network and DSX-1 interfaces and all APM ports	All
A specific slot	2, 3, 4, or 5
A specific port	The ClearAll function key *or* Disable for the Port Status option for the port

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 3-9).

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

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

Table 3-9. Interface Frame Relay Options (1 of 3)

LMI Protocol
Possible Settings: **Initialize_From_Net1FR1**, **Initialize_From_Interface,** **Auto_On_LMI_Fail,** **Standard,** **Annex-A,** **Annex-D** Default Setting: *For a user data port link:* **Initialize_From_Interface** *For a network link:* **Auto_On_LMI_Fail**
Specifies either the LMI protocol supported on the frame relay interface or the discovery source for the LMI protocol. **Initialize_From_Net1FR1** – The LMI type supported on this frame relay link will be configured to match the LMI protocol initially discovered on the primary Network frame relay link (Net1FR1). LMI Protocol is set to None internally, but once a protocol has become active or is set on the primary Network link, the protocol will be set to the same value on this link (Standard, Annex-A or Annex-D). The protocol will *not* be updated based on changes to Net1FR1 after being set initially. *Display Conditions* – This option value only appears for a user data port. **Initialize_From_Interface** – The LMI type supported on this frame relay link will be configured to match the LMI protocol discovered from the attached Network line or DTE device. Once a protocol has become active, the protocol will be set to the protocol discovered (Standard, Annex-A or Annex-D) on the frame relay link. The protocol will *not* be updated after being initially discovered. Frame relay links on 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 3-9. 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 3-2, 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. *Display Conditions* – This option only appears for the network interface. **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 3-9. 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.
Network Initiated DCLB
Possible Settings: **Disable, V.54, ANSI_FT1, Both** Default Setting: **Both**
Allows the starting and stopping 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. When enabled, this option causes the FrameSaver unit to initiate a DCLB on the DS0s allocated to this frame relay link when a DCLB-actuate sequence is received. *Display Conditions* – This option only appears for the network interface. **Disable** – The DCLB-actuate and DCLB-release sequences are ignored for this frame relay link. **V.54** – DCLB-actuate and DCLB-release sequences that comply with V.54 standard for “Inter-DCE signaling for point-to-point circuits” will be recognized and will control initiation and termination of a DCLB (V.54 Loop 2) for this frame relay link. **ANSI_FT1** – DCLB-actuate and DCLB-release sequences that comply with ANSI T1.403, Annex B standard for “In-band signaling for fractional-T1 (FT1) channel loopbacks” will be recognized and will control initiation and termination of a DCLB for this frame relay link. **Both** – 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 this 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).

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 3-10).

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 3-10. 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: *For user data port DLCIs:* **Standard** *For network and ISDN interface DLCIs:* **Multiplexed**
Specifies whether the DLCI is standard or multiplexed. This field is read-only when the selected DLCI is used in a PVC or Management link connection and the DLCI Type is Standard. *Display Conditions* – This option does not appear for 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.
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.

Table 3-10. DLCI Record Options (2 of 3)

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. *Display Conditions* – This option only appears when Committed Burst Size is set to Other.
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.
DLCI Priority
Possible Settings: **Low, Medium, High** Default Setting: **High**
Specifies the relative priority for data received on the DLCI from an attached device (also known as *quality of service*). All data on Port 1 is cut-through, as long as there is no higher-priority data queued from another user port. The DLCI priority set for an interface applies to data coming into that interface. For example, the priority set for DLCIs on Port 1 applies to data coming into Port 1 from the attached equipment (such as a router). 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 . *Display Conditions* – 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.

Table 3-10. DLCI Record Options (3 of 3)

Outbound Management Priority
Possible Settings: **Low, Medium, High** Default Setting: **Medium**
Specifies the relative priority for management traffic sent on management PVCs on this DLCI to the network. *Display Conditions* – This option is not available on a user data port. **Low** – Management data configured for the DLCI has low priority. **Medium** – Management data configured for the DLCI has medium priority. **High** – Management data configured for the DLCI has high priority.

Configuring PVC Connections

The Auto-Configuration feature automatically configures PVC Connections and their DLCI Records. PVC Connections can also be created manually (see Table 3-11).

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 3-11. PVC Connection Options (1 of 3)

Source Link
Possible Settings: **Port-1, Net1-FR1** Default Setting: Initially blank; no default.
Specifies the frame relay interface that starts a PVC connection; the **from** end of a from-to link. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined that are not part of a PVC connection or management link. For example, if Port-1 has no DLCIs defined, Port-1 would not appear as a valid setting. **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. **SxPort-*n*** – Specifies the port *n* in slot *x* as the source link. Refers to frame relay links on data ports capable of having the Port Use option set to Frame Relay (see Table 3-6, Data Port Physical Options). **Clear All** – Clears all Link and DLCI settings, and suppresses EDLCIs.

Table 3-11. PVC Connection Options (2 of 3)

Source DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the source DLCI for a frame relay interface. The DLCI must be defined and cannot be part of a PVC connection or management link. For multiplexed DLCIs, at least one EDLCI must be unconnected for the DLCI to be a valid selection. NOTE: Source DLCI has no value if Source Link contains no value. **16 – 1007** – Specifies the DLCI number.
Source EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the source Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection. *Display Conditions* – This option only appears when Source DLCI contains a multiplexed DLCI record number. **0 – 62** – Specifies the EDLCI number.
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. NOTE: Primary Destination DLCI has no value if Primary Destination Link contains no value. **16 – 1007** – Specifies the DLCI number.
Primary Destination EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the primary destination Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection. *Display Conditions* – This option only appears when the Primary Destination DLCI contains a multiplexed DLCI record number. **0 – 62** – Specifies the EDLCI number.

Table 3-11. 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 *to* 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 *ISDN Link Name* 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. *Display Conditions* – 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. *Display Conditions* – 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
- Communication Port Options
- Modem Port Options

Configuring Node IP Information

Select Node IP to display, add, or change the information necessary to support general IP communications for the node (see Table 3-12). 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 3-12. Node IP Options (1 of 2)

Node IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the node. Since an IP address is not bound to a particular port, it can be used for remote access via a management PVC. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the node, which can be viewed or edited. **Clear** – Fills the node IP address with zeros.
Node Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the node. Since the subnet mask is not bound to a particular port, it can be used for remote access via a management PVC. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the node, which can be viewed or edited. **Clear** – Fills the node subnet mask with zeros. When the node's subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.
Default IP Destination
Possible Settings: **Default, Modem, COM, *PVCname*** Default Setting: **Default**
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 3-13, Management PVC Options). NOTE: If the link to the IP destination selected as the default route becomes disabled or down, the unrouteable data will be discarded. Make sure that the link selected is operational, and if that link goes down, change the default destination. CAUTION: Use care when configuring a default route to an interface that has a subnet route configured at a remote end where the NMS, router, LAN adapter, terminal server, etc. is connected. Communicating with an unknown IP address on the subnet will cause temporary routing loops, which will last 16 iterations times the retry count. **None** – No default network destination is specified. Unrouteable data will be discarded. This is the recommended setting. **Modem** – Specifies that the default destination is connected to the modem port. Only appears when 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 3-18, Communication Port Options). ***PVCname*** – Specifies a name for the management PVC. Only appears when a management PVC name is defined for the node. For example, when the network is connected to a remote device located in the London office, London can be specified as the PVC name, which is the link between the local FrameSaver unit and the one located in London. London would appear as one of the available selections.

Table 3-12. Node IP Options (2 of 2)

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. *Display Conditions* – This selection only appears when a dedicated management PVC has been defined on the network frame relay link as a DLCI with DLCI Type set to Standard.
TS Management Link Access Level
Available Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the highest access level allowed when accessing the unit via a Telnet or FTP session when the service provider is using the TS Access Management Link. *Display Conditions* – This option only appears when TS Access Management Link is set to None. NOTES: Telnet and FTP sessions on this link *are not* affected by the access level set by the Session Access Level, Login Required, or FTP Login Required option settings (see Table 3-15, Telnet and FTP Session Options). Telnet and FTP sessions on this link *are* affected by the Telnet Session, Inactivity Timeout, Disconnect Time and FTP Session option settings. **Level-1** – Allows Telnet or FTP access by network service providers with the capability to view unit information, change configuration options, and run tests. This is the highest access level allowed. Use this setting when downloading files. **Level-2** – Allows Telnet or FTP access by network service providers with the capability to view unit information and run tests only; they cannot change configuration options. **Level-3** – Allows Telnet access by network service providers with the capability to view unit information only; they cannot change configuration options or run tests.

Configuring Management PVCs

Select Management PVCs to define inband management links by adding or changing Management PVCs (see Table 3-13). 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 3-13. 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** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-IP-Address**
Specifies the IP address needed to access the unit via this management PVC, providing connectivity to an external IP network through the frame relay network. **Node-IP-Address** – Uses the IP address contained in the Node IP Address (see Table 3-12, Node IP Options). **Special** (001.000.000.000 – 223.255.255.255) – Allows you to display/edit an IP address for the unit's management PVC when the IP address for this interface is different from the node's IP address.

Table 3-13. Management PVC Options (2 of 4)

Intf Subnet Mask
Possible Settings: **Node-Subnet-Mask, Calculate, Special** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-Subnet-Mask**
Specifies the subnet mask needed to access the unit when the management PVC is providing connectivity to an external IP network (through frame relay) that requires a specific subnet mask for the interface. **Node-Subnet-Mask** – Uses the *Interface* IP Subnet contained in the Node-Subnet Mask configuration option (see Table 3-12, Node IP Options). **Calculate** – Calculates the subnet mask created by the IP protocol based on the class of the IP address (Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000). Cannot be displayed or edited. **Special** (000.000.000.000 – 255.255.255.255) – Allows you to edit/display the subnet mask for the management PVC when the subnet mask is different for this interface. A text field displays where you can enter the subnet mask for this unit's management PVC.
Set DE
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether frames (packets) sent on a management PVC have the Discard Eligible (DE) bit set. This bit is used by the network to prioritize which frames to discard first during periods of network congestion. This allows management traffic to be viewed as lower priority than customer data. **Enable** – Sets the DE bit to one on all frames sent on the management PVC. **Disable** – Sets the DE bit to zero on all frames sent on the management PVC. This is the recommended setting, particularly for NSPs providing a managed network service.
Primary Link
Possible Settings: **Net1-FR1, SsPort-*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. **SsPort-*n*** – Specifies the frame relay link on the specified user data port in slot *s* 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.

Table 3-13. Management PVC Options (3 of 4)

Primary DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the DLCI number used for the management PVC after the frame relay interface is selected. The DLCI must be defined for the link (i.e., has a DLCI record), and it must not be part of a PVC connection or already assigned as a management PVC. For multiplexed DLCIs, at least one EDLCI must be unconfigured for the DLCI. NOTES: – DLCI cannot be entered if the Link field is blank. – Clearing the Link also clears the DLCI. **16 – 1007** – Specifies the DLCI number (inclusive).
Primary EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the EDLCI number used for a management PVC when a multiplexed DLCI is selected. EDLCIs identify individual connections within multiplexed DLCIs that are unique to those DLCIs. Use a unique EDLCI to identify an individual connection within a multiplexed DLCI. Use 0 to identify the primary EDLCI. Use 1 – 62 to identify secondary EDLCIs. Use the primary EDLCI for customer data, which has a higher utilization rate than management data, with slightly less line overhead. *Display Conditions* – This option does not appear if the DLCI field does not reference a multiplexed DLCI. NOTE: Clearing the DLCI or changing it to a standard DLCI suppresses EDLCI field. **0 – 62** – Specifies the EDLCI number (inclusive).
Primary Link RIP
Possible Settings: **None, Proprietary, Standard_out** Default Setting: *For multiplexed DLCIs:* **Proprietary** *For nonmultiplexed DLCIs:* **Standard_out**
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 3-10, DLCI Record Options). **Standard_out** – The device will send standard RIP messages to communicate routing information only about FrameSaver SLV and FLEX units in the network. This is the factory default for management PVCs configured on standard DLCIs. NOTE: The router must be configured to receive RIP on the port connected to the FrameSaver unit for the management interface (e.g., Cisco: **`config-t, router RIP, int serialx, IP RIP Receive version 1, ctl-z WR`**). See *Setting Up So the Router Can Receive RIP*.

Table 3-13. Management PVC Options (4 of 4)

Alternate Link
Possible Settings: **Net1-FR1, S1Port-*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. *Display Conditions* – This option does not appear unless ISDN backup is available. **Net1-FR1** – Specifies the Network interface as the frame relay link. **S1Port-*n*** – Specifies the frame relay link on the NAM's 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. *Display Conditions* – 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).
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. *Display Conditions* – 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 3-14).

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

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

Table 3-14. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the FrameSaver unit can be managed as an SNMP agent by an SNMP-compatible NMS. **Enable** – Can be managed as an SNMP agent. **Disable** – Cannot be managed as an SNMP agent. The FrameSaver unit will not respond to SNMP messages nor send SNMP traps.
Community Name 1
Possible Settings: ***ASCII text entry*, Clear** Default Setting: **Public** in ASCII text field
Specifies the first of two names that are allowed to access the objects in the FrameSaver unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB. ***ASCII text entry*** – Adds to or changes Community Name 1 (maximum 255 characters). **Clear** – Clears Community Name 1.
Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read/Write**
Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 1. **Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP **get** and **set** commands).
Community Name 2
Possible Settings: ***ASCII text entry*, Clear** Default Setting: **Clear**
Specifies the second of two names that are allowed to access the objects in the FrameSaver unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB. ***ASCII text entry*** – Adds to or changes Community Name 2 (maximum 255 characters). **Clear** – Clears Community Name 2.

Table 3-14. General SNMP Management Options (2 of 2)

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

Configuring Telnet and/or FTP Session Support

Telnet and FTP options control whether a Telnet or FTP (File Transport Protocol) session is allowed through an interconnected IP network and the access security applicable to the session. Two Telnet sessions can be active at a time (see Table 3-15).

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 3-15. Telnet and FTP Session Options (1 of 3)

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

Table 3-15. Telnet and FTP Session Options (2 of 3)

Session Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the highest security level allowed when accessing the menu-driven user interface via a Telnet session. If a login is required for the session, the effective access level is also determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. This option does not affect the TS Access Management Link. NOTE: The effective access level is always the lowest one assigned to either the session or the user. For example, if the assigned Session Access Level is Level-2, but the User Access Level is Level-3, then only level-3 access is allowed for the session. **Level-1** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information, change configuration options, and run tests. This is the highest access level allowed. CAUTION: Before changing the session access level to Level-2 or 3, make sure that the COM port's Port Access Level is set to Level-1 and that at least one Login ID is set to Level-1. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. A reset is required if the Communication Port's Port Use option is set to Net Link (see Table 3-4, General System Options). **Level-2** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information and run tests only; they cannot change configuration options. **Level-3** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information only; they cannot change configuration options or run tests.
Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a Telnet session is disconnected after a specified period of keyboard inactivity. **Enable** – Terminates the session after the Disconnect Time expires. **Disable** – Does not terminate Telnet session during inactivity.

Table 3-15. Telnet and FTP Session Options (3 of 3)

Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Sets the amount of keyboard inactive time allowed before a user session is disconnected. *Display Conditions* – This option does not appear when Inactivity Timeout is disabled. **1 – 60** – Up to an hour can be set.
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 Receive 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 3-16).

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 3-16. SNMP NMS Security Options (1 of 2)

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

Table 3-16. SNMP NMS Security Options (2 of 2)

Access Type
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Specifies the type of access allowed for an authorized NMS when IP address validation is performed. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **Read** – Allows read-only 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 3-17).

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 3-17. SNMP Traps and Trap Dial-Out Options (1 of 5)

SNMP Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the FrameSaver unit sends trap messages to the currently configured SNMP trap manager(s). **Enable** – Sends trap messages. **Disable** – Does not send trap messages.
Number of Trap Managers
Possible Settings: **1 – 6** Default Setting: **1**
Specifies the number of SNMP management systems that will receive SNMP trap messages from the FrameSaver unit. An NMS IP Address must be configured in the NMS *n* IP Address configuration option for each trap manager to receive trap messages. **1 – 6** – Specifies the number of trap managers (inclusive).

Table 3-17. SNMP Traps and Trap Dial-Out Options (2 of 5)

NMS *n* IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address that identifies the SNMP manager(s) to receive SNMP traps. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **001.000.000.000 – 223.255.255.255** – Adds to or changes the IP address for the trap manager. **Clear** – Fills the NMS IP address with zeros.
Destination
Possible Settings: **AutoRoute, Modem, COM, *PVCname*** Default Setting: **AutoRoute**
Specifies the initial route used to reach the specified Trap Manager. When proprietary RIP is active, only one unit in the network needs to specify an interface or management link as the initial destination. All other units can use the default setting. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **AutoRoute** – Uses proprietary RIP from other FrameSaver devices to learn the route for sending traps to the specified Trap Manager, or the Default IP Destination when no route is available in the routing table (see Table 3-12, 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 3-19, Modem Port Options). **COM** – Uses the COM port. This selection is only available when Port Use is set to Net Link (see Table 3-18, Communication Port Options). ***PVCname*** – Uses the defined management *linkname* (the name given the Management PVC). This selection only appears when at least one Management PVC is defined for the node.
General Traps
Possible Settings: **Disable, Warm, AuthFail, Both** Default Setting: **Both**
Determines whether SNMP trap messages for warmStart and/or authenticationFailure events are sent to the currently configured trap manager(s). **Disable** – Does not send trap messages for these events. **Warm** – Sends trap messages for warmStart events only. **AuthFail** – Sends trap messages for authenticationFailure events only. **Both** – Sends trap messages for both warmStart and authenticationFailure events.
Enterprise Specific Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether trap messages for enterpriseSpecific events are sent to the currently configured trap manager(s). **Enable** – Sends trap messages for enterpriseSpecific events. **Disable** – Does not send trap messages for enterpriseSpecific events.

Table 3-17. SNMP Traps and Trap Dial-Out Options (3 of 5)

Link Traps
Possible Settings: **Disable, Up, Down, Both** Default Setting: **Both**
Determines whether SNMP linkDown or linkUp traps are sent to the currently configured trap manager(s). A linkDown trap indicates that the unit recognizes a failure in one of the interfaces. A linkUp trap indicates that the unit recognizes that one of its interfaces is active. Use the Link Traps Interface and the DLCI Traps on Interface configuration options to specify which interface will monitor linkUp and linkDown traps messages. **Disable** – Does not send linkDown or linkUp trap messages. **Up** – Sends trap messages for linkUp events only. **Down** – Sends trap messages for linkDown events only. **Both** – Sends trap messages for linkUp and linkDown events.
Link Traps Interfaces
Possible Settings: **Network, DSX-1, T1s, Ports, DBM, OCU, 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. **DBM** – For units with an ISDN DBM installed, generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on the DBM only. **OCU** – For units with an OCU-DP APM installed, generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on the OCU-DP interfaces 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.
DLCI Traps on Interfaces
Possible Settings: **Network, Ports, DBM, All** 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.

Table 3-17. SNMP Traps and Trap Dial-Out Options (4 of 5)

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.
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.
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**
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.

Table 3-17. SNMP Traps and Trap Dial-Out Options (5 of 5)

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 five 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 Communication Port

Select Communication Port from the Management and Communication menu to display or change the communication port configuration options (see Table 3-18).

Main Menu → Configuration → Management and Communication → Communication Port

Table 3-18. Communication Port Options (1 of 4)

Port Use
Possible Settings: **Terminal, Net Link** Default Setting: **Terminal**
Assigns a specific use to the COM port. NOTE: If the Default IP Destination is set to COM (see Table 3-12, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. **Terminal** – The COM port is used for the asynchronous terminal connection. **Net Link** – The COM port is the network communications link to the IP network or IP device port.
Data Rate (Kbps)
Possible Settings: **9.6, 14.4, 19.2, 28.8, 38.4, 57.6, 115.2** Default Setting: **19.2**
Specifies the rate for the COM port in kilobits per second. **9.6 – 115.2 kbps** – Sets the communication port speed.
Character Length
Possible Settings: **7, 8** Default Setting: **8**
Specifies the number of bits needed to represent one character. NOTE: Character length defaults to 8 and cannot be changed if Port Use is set to Net Link. **7** – Sets the character length to seven bits. **8** – Sets the character length to eight bits. Use this setting if using the COM port as the network communication link.
Parity
Possible Settings: **None, Even, Odd** Default Setting: **None**
Provides a method of checking the accuracy of binary numbers for the COM port. A parity bit is added to the data to make the "1" bits of each character add up to either an odd or even number. Each character of transmitted data is approved as error-free if the "1" bits add up to an odd or even number as specified by this configuration option. **None** – Provides no parity. **Even** – Makes the sum of all 1 bits and its corresponding parity bit always even. **Odd** – Makes the sum of all 1 bits and its corresponding parity bit always odd.

Table 3-18. Communication Port Options (2 of 4)

Stop Bits
Possible Settings: **1, 2** Default Setting: **1**
Determines the number of stop bits used for the COM port. **1** – Provides one stop bit. **2** – Provides two stop bits.
Ignore Control Leads
Possible Settings: **Disable, DTR** Default Setting: **Disable**
Specifies whether DTR is used. **Disable** – Treats control leads as standard operation. **DTR** – Ignores DTR. This may be necessary when connecting to some PAD devices.
Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether a user ID and password (referred to as the login) is required in order to log on to the asynchronous terminal connected to the COM port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Enable** – Requires a login to access the menu-driven user interface. **Disable** – Does not requires a login.
Port Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies level of user access privilege for an asynchronous terminal connected to the COM port. If a login is required for the port, the effective access level is determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. NOTE: The effective access level is always the lowest one assigned to either the port or the user. For example, if the Port Access Level assigned is Level-2, but the User Access Level is Level-3, then only level-3 access will be permitted for the port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Level-1** – Allows full access and control of the device including monitoring, diagnostics, and configuration. The user can add, change, and display configuration options, and perform device testing. **Level-2** – Allows limited access and control of the device. The user can monitor and perform diagnostics, display status and configuration option information. **Level-3** – Allows limited access with monitoring control only. The user can monitor and display status and configuration screens only.

Table 3-18. Communication Port Options (3 of 4)

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

Table 3-18. Communication Port Options (4 of 4)

Link Protocol
Possible Settings: **PPP, SLIP** Default Setting: **PPP**
Specifies the link-layer protocol to be used. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). *Display Conditions* – This option only appears when Port Use is set to Net Link. **PPP** – Point-to-Point Protocol. **SLIP** – Serial-Line Internet Protocol.
RIP
Possible Settings: **None, Proprietary, Standard_out** Default Setting: **None**
Specifies which Routing Information Protocol (RIP) is used to enable routing of management data between devices. *Display Conditions* – This option only appears when Port Use is set to Net Link. **None** – No routing is used. **Proprietary** – A proprietary variant of RIP version 1 is used to communicate routing information between devices to enable routing of IP traffic. **Standard_out** – The device will send standard RIP messages to communicate routing information about other FrameSaver units in the network. Standard RIP messages received on this link are ignored. NOTE: The router must be configured to receive RIP on the port connected to the COM port, configured as the management interface (e.g., Cisco: config-t, router RIP, int serial*x*, IP RIP Receive version 1, ctl-z WR). To create this management interface, make sure that Node or COM port IP Information has been set up (see *Configuring Node IP Information*).

Configuring the Modem Port

Select Modem Port from the Management and Communication menu to configure the modem port (see Table 3-19).

Main Menu → Configuration → Management and Communication → Modem Port

Table 3-19. 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 3-12, 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.
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.
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. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Enable** – Requires a login to access the menu-driven user interface. **Disable** – Does not require a login.

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

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. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Level-1** – Allows full access and control of the device including monitoring, diagnostics, and configuration. The user can add, change, and display configuration options, 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). *Display Conditions* – 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.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Determines the amount of lapsed time before disconnecting a user session in minutes. *Display Conditions* – 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.

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

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. *Display Conditions* – This option only appears when Port Use is set to Net Link. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the modem port, which you can view or edit. **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. *Display Conditions* – This option only appears when Port Use is set to Net Link. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the 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. *Display Conditions* – This option only appears when Port Use is set to Net Link. **PPP** – Point-to-Point Protocol. **SLIP** – Serial-Line Internet Protocol.
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. *Display Conditions* – 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.

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

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. *Display Conditions* – This option only appears when Port Use is set to Net Link. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the 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.
RIP
Possible Settings: **None, Proprietary, Standard_out** Default Setting: **None**
Specifies which Routing Information Protocol (RIP) is used to enable routing of management data between devices. *Display Conditions* – This option only appears when Port Use is set to Net Link. **None** – No routing is used. **Proprietary** – A proprietary variant of RIP version 1 is used to communicate routing information between devices to enable routing of IP traffic. **Standard_out** – The device will respond to standard RIP requests to communicate routing information.

Dial Backup Modules

4

This chapter provides information for the following:

- *Verifying ISDN DBM Operation*
  - *Manually Forcing Backup (Disruptive)*
  - *Manually Placing a Call (Nondisruptive)*
  - *Verifying ISDN Lines*
  - *Verifying That Backup Can Take Place*
  - *Checking the DBM Interface Status*
  - *Viewing DBM Call Performance Statistics*
- *Identifying ISDN DBM Problems*
- *ISDN DBM Tests*
  - *ISDN PVC Tests*
  - *PRI Physical Tests*

See Chapter 7, *Operation and Maintenance*, for card identity information, backup LED and alarm conditions, device and other DBM operation-related messages. This information is generally integrated in the FrameSaver unit's operation.

Dial Backup Overview

The FrameSaver unit supports various LMI types, provides switching capability, and performs continuous monitoring of the frame relay physical and logical links. When combined with an ISDN DBM for frame relay backup rather than a router, better, faster, and easier backup can be achieved.

Backup provides continuing service in case of a network, LMI, or PVC failure. Being a frame relay aware product, the system continually monitors frame relay physical and logical links to detect these failures. If a PRI DBM is installed, up to 23 remote sites can be backed up simultaneously, using a single B-channel per remote site. If a BRI DBM is installed, up to two remote sites can be backed up simultaneously.

Remote sites usually back up to the central site unit since data flows from remote sites to the central site in most network topologies. When this approach is followed, remote site configuration is greatly simplified so that remote site units are generally plug-and-play and most of the configuration is done at the central site.

When backing up to a destination node, an alternate network like ISDN can be used, or the service provider may provide access to ISDN lines through its own network. Either way, the ISDN DBM supports a variety of backup schemes.

Here is **how backup works**:

1. When a network, LMI, or PVC failure is detected, the system generates an alarm, which triggers an SNMP Trap.
2. If the system is configured for automatic backup and an alternate destination circuit has been configured, the originating DBM places a call and the answering device at the other end prepares to receive the call.
3. Once Caller ID is verified, a connection is established between the DBMs, the NAM switches data to the backup link, the alternate path.

   All reconfiguration and redirection occurs automatically within the unit, entirely transparent to the connected DTE.

For **circuit restoration**:

1. When the system detects that normal service has been restored, the unit clears the alarm and SNMP Trap.
2. Data is switched back to its original path and the backup link is disconnected.

   A backup link is disconnected when:

   — One of the devices in the backup link physically disconnects from the ISDN.

   — The backup link LMI has timed out.

   — All alternate DLCIs on the backup link become inactive.

   If the backup link is disconnected but a failure is still detected, the device continues to try to reestablish the connection until the failure is no longer detected or until backup is no longer needed.

See *Setting Up Dial Backup* for assistance configuring the dial backup feature.

Getting Started

Before you set up dial backup, obtain the following information:

- Verification of the type of ISDN switch.
  - For a BRI DBM: NI-1
  - For a PRI DBM: NI-2, ATT 4ESS, or ATT 5ESS
- Verification of the type of ISDN service.
  - For a **BRI DBM**: Capability Package B for 1B-service or Capability Package (I) for 2B Service for an ISDN BRI DBM – Supports up to two circuit-switched B-channels, BRI-B1 and BRI-B2, each with one Service Profile Identification (SPID) number and one local phone number.
  - For a **PRI DBM**: 23B with one phone number and Circuit Switched Data capability.
- Verification of CNIS (calling number identification service) for answering unit.
- Number of digits used for the Outbound Phone Number or Inbound Calling ID (the ISDN Link Profile formats).

  Example:
  A 10-digit format with the area code included may be used for the Inbound Calling ID (8135309999), while a 7-digit format without the area may be used for the Outbound Phone Number (5309999).
- Actual phone number(s) for the DBM.
- For a BRI DBM, obtain the SPID (service profile identification) numbers.

  Order BusyCall Forwarding if more than one phone number will be used so that calls will be forwarded to the second B-channel when the primary B-channel is busy.

Setting Up Dial Backup

When configuring units with ISDN backup capability, one unit's DBM must be configured to originate backup and the other unit's DBM must be configured to answer a backup call.

The following guidelines apply:

- **Central site** configuration guidelines:
  - — Configure a Link Profile for each remote site.
  - — Set up the ISDN DBM physical interface, configuring it to answer calls from remote sites. (A PRI DBM is already configured to answer calls.)
  - — If a BRI DBM is installed, change Automatic Backup Configuration to Disabled. (A PRI DBM is already set to Disabled.)
  - — Manually create alternate DLCIs on the ISDN Backup Link.
  - — After the primary DLCIs have been automatically discovered or manually configured, specify ISDN DLCIs as alternate DLCIs for the PVC connection.

- **Remote site** configuration guidelines:
  - — Set up the ISDN DBM physical interface, configuring it to place backup calls to the central site. (A BRI DBM is already configured to originate calls.)
  - — If a PRI DBM is installed, change Automatic Backup Configuration to Enabled. (A BRI DBM is already set to Enabled.)
  - — 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.

See *Verifying ISDN DBM Operation* when setup is complete.

See Chapter 7, *Operation and Maintenance*, to view information about the DBM card, and DBM-related LEDs, messages, statuses, and performance statistics. This information is generally integrated with FrameSaver unit information.

Setting Up the DBM Physical Interface

▶ Procedure

1. Configure the DBM interface.

   Main Menu →Configuration →ISDN →Physical

2. Enable or disable the interface, and enter the Service Profile IDs (SPIDs) and local phone numbers.

   — If the DBM at the central site is a BRI DBM, change the Originate or Answer option setting to Answer.

   — If the DBM at a remote site is a PRI DBM, change the Originate or Answer option setting to Originate.

3. Save the configuration.

See Table 4-1, ISDN BRI DBM Physical Interface Options, or Table 4-2, ISDN PRI DBM Physical Interface Options for configuration information.

Setting Up Automatic Backup Configuration

When the DBM is enabled, the Auto-Configuration feature allows you to select automatic configuration for backup, as well as for DLCI record configuration and connection within the unit.

Main Menu →Auto-Configuration

Automatic Backup Configuration 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.

If this feature is . . .	Then . . .
Enabled	Appropriate DLCIs are automatically configured on the first ISDN link, and all network primary destination PVC connections and management PVCs are updated to include alternate destination DLCIs with the same number as the network DLCIs. This is the default setting for an ISDN BRI DBM.
Disabled	No automatic configuration takes place on the DBM interface and no alternate destinations are created for PVCs. This is the default setting for an ISDN PRI DBM.

Since a central site DBM generally needs ISDN links for multiple remote sites and a remote site DBM only needs one ISDN link to the central site DBM, this feature should be disabled for a central site DBM (configured to answer backup calls) but enabled for a remote site DBM (configured to originate a backup call).

The default settings for the DBM are based upon the assumption that the central site DBM is equipped with an ISDN PRI DBM, and a remote site DBM is equipped with an ISDN BRI DBM. However, the setting can be changed at any time from this menu.

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

Prompt	**Appears When . . .**	**Description**
Delete All Alternate Destinations from PVC Connections?	Automatic Backup Configuration is disabled.	If Yes (y) is selected, all Alternate Destination information is removed from PVC connections and Management PVCs, and all DLCIs used exclusively for alternate destinations are deleted. If No (n) is selected, 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 settings.
Add Alternate Destinations to Current PVC Connections?	Automatic Backup Configuration is enabled.	If Yes (y) is selected, DLCI records are configured on the first ISDN link and Alternate Destination information is added to current PVC connections and management PVCs. If No (n) is selected, no previously configured PVC connections are changed, and newly discovered DLCIs will be configured according to the new discovery mode and automatic backup settings.

Changes must be saved to take effect.

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 will be allowed to occur, see *Setting the Criteria for Automatic Backup*.

See *Setting Up Auto-Configuration* in Chapter 7, *Operation and Maintenance*, to see an example of the screen.

Setting Up ISDN Link Profiles

When the system is equipped with an ISDN DBM, ISDN link profiles must be set up for each device at the other end of an alternate (backup) link.

- For the central site DBM, a link profile is set up for each remote device.
- For a remote site DBM, a link profile is set up for the central site.

If there is a failure in the primary link or DLCI for which you are creating an alternate link, the DBM performs based upon the ISDN Originate or Answer option setting and the ISDN Link Profile Link Status configuration option settings. In addition to backup, any time a Primary Destination or Source DLCIs for this link profile has been configured, the specified link profile will become active.

If ISDN Physical option Originate or Answer is set to . . .	And ISDN Link Profile Link Status Option is set to. . .	Then the DBM will . . .
Originate	Auto	Dial the Outbound Phone Number that you have specified for this link.
Answer	Auto	Wait for a call from one of the Inbound Calling IDs that you have specified for this link. When the primary link recovers, the call will be disconnected.
Originate or Answer	Disable	Terminate any existing ISDN call(s) associated with this link profile and will not originate any future calls for this link profile.

When no ISDN Link Profiles have been configured, **`No ISDN Link Profiles`** displays. Otherwise, up to 10 previously configured profiles display on one screen, in the order they were defined. ISDN Link Profiles are only displayed for links with nonnull link names.

When creating an ISDN Link Profile and the maximum number of link profiles have been configured, **`Limit of ISDN Link Profiles Reached`** displays at the bottom of the screen. When this occurs, another link profile must be deleted before a new link profile can be created.

See Table 4-1, ISDN BRI DBM Physical Interface Options, or Table 4-2, ISDN PRI DBM Physical Interface Options for configuration information. See Table 4-3, ISDN Link Profile Options, for link profile configuration information.

If setting up a central site unit, see *Creating and Modifying ISDN Link Profiles* and *Manually Creating Alternate DLCIs on ISDN Links at the Central Site*.

If setting up a remote site unit, see *Creating and Modifying ISDN Link Profiles* to add the phone number for the central site.

Creating and Modifying ISDN Link Profiles

Once the Automatic Backup Configuration feature automatically configures an ISDN Link Profile, a name and phone number must be added to the profile.

▶ Procedure

1. Select Link Profiles, then New or Modify.

   Main Menu → Configuration → ISDN → Link Profiles

   If setting up a central site unit, select New, and create a link profile for each remote device.

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). For the first ISDN Link Profile, the default setting is HQ_Site. All other link profile Names are blank.

   When setting up a remote site unit, the Name does not have to be changed.

   — Link Status set to Auto.

   — Phone numbers entered:

Originating System	Answering System
Outbound phone number. Valid characters can include: ■ Numbers (0–9) ■ Special characters * and # ■ Spaces ■ parenthesis ( )	Inbound Calling ID1 and ID2. These are the phone numbers of units that calls will be accepted from. Valid characters can include: ■ Numbers (0–9)

   NOTE:

   Remember to include local dial-out numbers (i.e., 9, then the number).

   — Maximum Link Rate (Kbps) set to the appropriate speed, if necessary.

3. Save the configuration.

See Table 4-3, ISDN Link Profile Options, for configuration information.

If setting up a central site unit, see *Manually Creating Alternate DLCIs on ISDN Links at the Central Site*.

Manually Creating Alternate DLCIs on ISDN Links at the Central Site

This can be done automatically using the Automatic Backup Configuration feature (see *Setting Up Automatic Backup Configuration*). However, a central site generally needs to manually configure DLCI records on multiple ISDN frame relay links and create multiple link profiles. Only one link profile is created when using the Automatic Backup Configuration feature.

▶ Procedure

To manually configure DLCI Records for the link:

1. Select DLCI Records for the ISDN link.

   Main Menu →Configuration →ISDN →DLCI Records

2. Select the desired ISDN Link Profile (an ISDN Link Name), then select New or Modify.

3. Configure the ISDN link DLCI like any other DLCI record.

4. Save the configuration.

Setting the Criteria for Automatic Backup

You can specify when auto backup is allowed to occur on units configured to originate calls. 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

▶ Procedure

To set the criteria 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 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.

3. Save the configuration.

See Table 4-4, 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

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.

See Table 3-17, SNMP Traps and Trap Dial-Out Options, in Chapter 3, *Configuration*, for configuration information.

ISDN DBM Configuration Tables

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

The following configuration option tables are included:

- Table 4-1. ISDN BRI DBM Physical Interface Options
- Table 4-2. ISDN PRI DBM Physical Interface Options
- Table 4-3. ISDN Link Profile Options
- Table 4-4. Auto Backup Criteria Options

Configuring the ISDN DBM Interface

Select Physical from the ISDN menu to configure the physical characteristics for the DBM Interface.

Main Menu → Configuration → ISDN → Physical

When configuring a BRI DBM, refer to Table 4-1.
When configuring a PRI DBM, refer to Table 4-2.

ISDN BRI DBM

Refer to the following configuration options if an ISDN BRI DBM is installed.

Table 4-1. 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.
Originate or Answer
Possible Settings: **Originate, Answer** Default Setting: **Originate**
Specifies whether the unit's DBM will originate or answer dial backup calls. The DBM at one end of the circuit must be configured to originate calls, while the other must be configured to answer calls. **Originate** – Places dial backup calls; the recommended setting for a remote site DBM. **Answer** – Answers dial backup calls; the recommended setting for a central site DBM.
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.

ISDN PRI DBM

Refer to the following configuration options if an ISDN PRI DBM is installed.

Table 4-2. 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.
Originate or Answer
Possible Settings: **Originate, Answer** Default Setting: **Answer**
Specifies whether the access unit’s DBM will originate or answer dial backup calls. The DBM at one end of the circuit must be configured to originate calls, while the other must be configured to answer calls. **Originate** – Places dial backup calls; the recommended setting for a remote site DBM. **Answer** – Answers dial backup calls; the recommended setting for a central site DBM.
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.

Table 4-2. ISDN PRI DBM Physical Interface Options (2 of 3)

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.
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. *Display Conditions* – 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.

Table 4-2. ISDN PRI DBM Physical Interface Options (3 of 3)

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. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **Enable** – Generates and sends PRMs. **Disable** – Does not generate and send PRMs.
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. *Display Conditions* – 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

Select ISDN Link Profiles from the ISDN menu to set up the ISDN Link Profiles (see Table 4-3).

Main Menu →Configuration →ISDN →ISDN Link Profiles

Table 4-3. ISDN Link Profile Options (1 of 2)

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. **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. **Disable** – The frame relay link is out of service. No data will be transmitted or received on the interface.
Outbound Phone Number
Possible Settings: **0 – 9**, *****, **#**, space, _ , **–**, (, or) Default Setting: none
Specifies the phone number to call (the called party ID). Up to 36 digits can be entered. *Display Conditions* – This option only appears when Originate or Answer is set to Originate (see Table 4-1, ISDN BRI DBM Physical Interface Options, or Table 4-2, ISDN PRI DBM Physical Interface Options).

Table 4-3. ISDN Link Profile Options (2 of 2)

Inbound Calling ID 1 or 2
Possible Settings: **0** – **9** Default Setting: none
Specifies the phone number to accept calls from (calling party IDs). Up to 18 digits can be entered. *Display Conditions* – This option only appears when Originate or Answer is set to Answer (see Table 4-1, ISDN BRI DBM Physical Interface Options, or Table 4-2, ISDN PRI DBM Physical Interface Options). NOTE: 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). CAUTION: All calling party IDs must be unique across all of the enabled DBM call profiles. This ensures that the DBM installs the correct backup configuration on answering, since the calling party ID is used to identify the remote unit and to determine which PVC mappings to use.

Configuring the Criteria for Automatic Backup

Follow this menu selection sequence to specify whether and when automatic backup is allowed (see Table 4-4).

Main Menu → Configuration → Auto Backup Criteria

Table 4-4. Auto Backup Criteria Options

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. 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 3-13, 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 3-2, System Frame Relay and LMI Options). **Enable** – Reroutes traffic over the backup (alternate) interface. **Disable** – Does not reroute traffic over the backup interface.
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. *Day* 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. *Display Conditions* – 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.

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 call screening to avoid accidental or intentional disruption of network traffic. The answering DBM only accepts calls from valid calling number identifiers.

When the ISDN DBM interface is enabled, 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.

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 Physical Interface* for more information about ISDN DBM configuration options.

Upgrading ISDN DBM Software

A separate download to update PRI DBM functionality is not necessary; a PRI upgrade is incorporated in the unit's program code (see *Upgrading System Software* in Chapter 7, *Operation and Maintenance*). However, if the FrameSaver unit has a BRI DBM, the program code must be upgraded separately.

Upgrading ISDN BRI DBM Software

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 R*xxxxxx*.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

Verifying ISDN DBM Operation

This section includes:

- *Manually Forcing Backup (Disruptive)*
- *Manually Placing a Call (Nondisruptive)*
- *Verifying ISDN Lines*
- *Verifying That Backup Can Take Place*
- *Checking the DBM Interface Status*
- *Viewing DBM Call Performance Statistics*

See Chapter 7, *Operation and Maintenance*, to view information about the DBM card, and DBM-related LEDs, messages, statuses, and performance statistics. This information is generally integrated with FrameSaver unit information.

Manually 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*).

2. Have someone at the far end disconnect the network cable. The originating unit should initiate backup.

   To determine the answering or originating side, see the Originate or Answer configuration option for the ISDN physical interface options (see *Configuring the ISDN DBM Interface* in Chapter 3, *Configuration)*.

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.

Manually Placing a Call (Nondisruptive)

Use this procedure to test the ISDN path to each remote site. This procedure will not put the system into backup. This is accomplished by creating unique PVCs, with the ISDN Link as the Primary Destination.

▶ Procedure

To set up the originating and answering units for this test:

1. Make sure the ISDN Link Profiles are set up correctly at both the originating and answering devices (see *Setting Up ISDN Link Profiles*).

   Main Menu → Configuration → ISDN → Link Profiles

2. Create a unique test DLCI Record on the ISDN interface at each end (e.g., Line Test).

   Main Menu → Configuration → ISDN → DLCI Records

3. Create a new Management PVC at each end using the DLCI numbers created in Step 2.

   Main Menu → Configuration → Management and Communication → Management PVCs

   The ISDN Link should be configured as the Primary Destination Link and DLCI/EDLCI.

   — For the originating device, the call is placed once the configurations are saved.

   — For the answering device, it will be receiving a call.

   NOTE:

   As long as no other backup is taking place, the Backup (BKP) LED remains off during this procedure since the ISDN link is being used as the primary destination, not the alternate (backup) destination.

4. When the test is complete, delete the test Management PVC and DLCI Records.

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* in this chapter, and Table 7-7, Health and Status Messages in Chapter 7, *Operation and Maintenance*, 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 *DBM Call Performance Statistics* in this chapter, and Table 7-7, Health and Status Messages, and *Viewing LEDs and Control Leads*, in Chapter 7, *Operation and Maintenance*, for additional information.

Checking the DBM Interface Status

Select DBM Interface Status from the Status menu to see the status of the DBM interface.

Main Menu →Status →DBM Interface Status

DBM Interface Status Screen Example

```
main/status/dbm                                                          9191
Device Name: Node A                                          5/26/2000 23:32


                             DBM INTERFACE STATUS

 Line Status:            Invalid Call ID - 8135551212

 Link:                       Colorado
 Link Operating Mode:        Active
 Call Status:                Connected
 Last Cause Value:           Call Awarded and Being Delivered In Est Chnl-7
 Previous Last Cause Value:  Call Awarded and Being Delivered In Est Chnl-7
 Maximum Link Rate (Kbps):   64K      (Configured)
 Remote Call ID:             8135302000
 ISDN Channel:               B1
 Negotiated Rate (Kbps):     64K




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

Table 4-5. DBM Interface Status (1 of 2)

Field	Status	What It Indicates
Line Status		The overall status of the ISDN line.
	Active	■ The ISDN line is active and no error conditions exist.
	Disabled	■ The ISDN interface has been disabled. *Main Menu →Configuration → ISDN →Physical*
	Inactive	■ The ISDN line is disconnected or an ISDN network alarm condition exists.
	Invalid SPID	■ The switch has rejected one of the configured SPIDs *(ISDN BRI DBM only)*.
	Invalid Local Number	■ The phone number configured for a B-channel is an invalid local number.
	Invalid Call ID – *call ID*	■ The incoming call was rejected because the Inbound Calling ID did not match the number in any of the enabled ISDN Link Profiles. The rejected Inbound Calling ID appears at the end of the message, if provided by the switch.
Link	*ISDN Link Name*	The selected ISDN backup link for which status will be displayed.

Table 4-5. DBM Interface Status (2 of 2)

Field	Status	What It Indicates
Link Operating Mode		The status of the ISDN DBM.
	Disabled [1]	■ The ISDN Link Profile is disabled.
	Idle [1]	■ An ISDN link is not currently needed, so there is no ISDN connection.
	Testing	■ A network-initiated test is running on the DBM interface.
	Active	■ The ISDN link is required for frame relay traffic and needs an active ISDN connection.
Last Cause Value	Various ITU cause messages	Refer to Last Cause Value Messages for additional information.
Previous Last Cause Value		
Remote Call ID	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.
ISDN Channel	BRI DBM: B1, B2 PRI DBM: B1, B2, . . . B23	The ISDN B-channel being used for the call on this link.
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.

[1] If Link Operating Mode is Disabled or Idle, the Remote Call ID, ISDN Channel, and Negotiated Rate fields will not appear.

Last Cause Value Messages

The following Last 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 4-6. Last 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 4-6. Last 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 4-6. Last 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.
No Circuit/Channel Available	34	No circuit/channel is currently available to handle the call.	Wait and try again.

Table 4-6. Last Cause Value Messages (4 of 6)

Message	Cause No.	What It Indicates	What To Do
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.
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.

Table 4-6. Last Cause Value Messages (5 of 6)

Message	Cause No.	What It Indicates	What To Do
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.
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.

Table 4-6. Last Cause Value Messages (6 of 6)

Message	Cause No.	What It Indicates	What To Do
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.

Viewing DBM Call Performance Statistics

These statistics are available for ISDN calls and call attempts (see Table 4-7).

Main Menu → Status → Performance Statistics → DBM Call

DBM Call Performance Statistics Screen Example

```
main/status/dbm                                                              9191
Device Name: Node A                                                5/26/2000 23:32

                         DBM CALL PERFORMANCE STATISTICS

                 Total Call Attempts:                          4
                 Total Calls Originated:                       4
                 Total Calls Answered:                         0
                 Total Calls Rejected (Security):              0
                 Total Calls Rejected (Other):                 0
                 Average Call Duration (mins):                 8
                 Longest Call Duration (mins):                12
                 Total Call Duration (mins):                  30








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

Select the ClrDBMStats function key to clear or reset the DBM call performance statistics.

Table 4-7. 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.
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.

For other performance statistics, see *Performance Statistics* in Chapter 7, *Operation and Maintenance*.

Identifying ISDN DBM Problems

The following table identifies symptoms of possible ISDN DBM problems.

Table 4-8. ISDN DBM Symptoms

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 *Setting Up ISDN Link Profiles*). ■ For a BRI DBM, verify that the SPIDs and local area codes and phone numbers are correct (see *Configuring the ISDN DBM Interface*). ■ 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.

For additional information when identifying ISDN DBM problems:

- See *System and Test Status Messages* in Chapter 7, *Operation and Maintenance*,
- See *Checking the DBM Interface Status* and Table 4-6, Last Cause Value Messages, to check the physical interface.
- See *Viewing DBM Performance Statistics* to check the statistics that have been collected on backup calls and call attempts.
- See *Alarms* in Chapter 8, *Troubleshooting*, for additional information about conditions that cause a system alarm and generate SNMP traps.
- See *ISDN DBM Tests* for information about tests that are available when an ISDN DBM is installed.

ISDN DBM Tests

The Test menu allows you to run loopbacks and test patterns on the FrameSaver unit and its ISDN DBM interface. You must have security Access Level of 1 or 2 to run tests.

The following tests can be run for an ISDN DBM:

- PVC Tests on the ISDN link
  - PVC Loopback
  - Send and Monitor Pattern
  - Connectivity
- PRI Physical Tests
  - Local Line Loopback
  - Local Payload Loopback
  - Remote Send Line Loopback
  - Send and Monitor a user-selected Pattern

  Currently, there are no physical tests for a BRI DBM interface.

These tests are started and monitored the same as network tests.

See *Test Status Messages* in Chapter 7, *Operation and Maintenance*, for information about the status of a test. See *PVC Tests* and *Physical Tests* in Chapter 8, *Troubleshooting*, for additional information about these tests.

ISDN PVC Tests

PVC tests can be run on ISDN DBM frame relay links. Only one PVC test can be run on the same DLCI, and no physical test can be run on the same interface while a PVC test is running. An example of the PVC Tests screen is shown, with the multiplexed DLCI 550 selected.

PVC Tests Screen Example

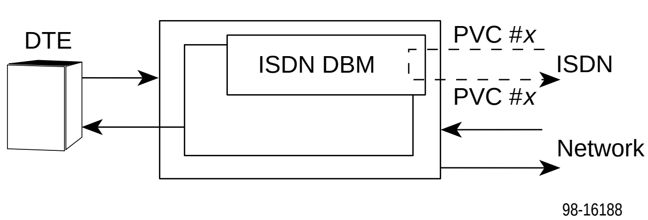
```
main/test/isdn_pvc                                                        9191
Device Name: Node A                                                 5/26/2000 23:32

                                ISDN-FLA PVC TESTS


    DLCI Number: 550

   Test (Non-Disruptive)     Command    Status     Result

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




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

ISDN 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 → ISDN PVC Tests

ISDN PVC Loopback



Send and Monitor Pattern, and Connectivity

See *Send Pattern*, *Monitor Pattern*, and *Connectivity* in Chapter 8, *Troubleshooting, for information*. For an ISDN link, only the menu selection is different.

PRI Physical Tests

Physical tests can be performed on the PRI DBM interface, but there are no physical tests for a BRI DBM interface. Physical tests require the participation of your network service provider.

Main Menu → Test → PRI Physical Tests

Physical Tests Screen Example

```
main/test/pri                                                              9191
Device Name: Node A                                               5/26/2000 23:32

                              PRI PHYSICAL TESTS

 Test                        Command    Status      Result

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


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

  Pattern Tests
    Pattern: user-defined   0101
    Send Pattern:            Stop       Active   0:00:00 - Errors 99999+
    Monitor Pattern:         Stop       Active   0:00:00 - Errors 99999+

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

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

See *Line Loopback*, *Payload Loopback*, and *Send Line Loopback* in Chapter 8, *Troubleshooting*, for information. These tests are the same for a PRI DBM's interface as for the network interface.

Application Modules

5

This chapter provides information about the following:

See Chapter 7, *Operation and Maintenance*, for alarm conditions, device and other APM operation-related messages. This information is generally integrated in the FrameSaver unit's operation.

APM Overview

FrameSaver SLV MSA units support five Application Modules (APMs), which can be installed in a 2-slot or 5-slot housing, Slots 02 to 05.

- The Synchronous Data APM supports:
  - Four ports, each supporting EIA-530A, V.35, RS449, or V.11/X.21.
  - Rates of Nx56 or Nx64.
  - Standard RS232-like (RFC 1659) MIB.
  - Enterprise MIB for testing, statistics, and some configuration functions.

  See the *9109 Sync Data Application Module (APM) Installation Instructions* for additional information.

- The E&M Voice APM supports:
  - E&M Type I, II, IV, or V circuits.
  - µ-law PCM coding of analog voice line.
  - Enterprise MIB for testing and some configuration functions.

  See the *9109 E&M Analog Voice Application Module (APM) Installation Instructions* for additional information.

- The FXO Voice APM supports:
  - FXO circuits.
  - µ-law PCM coding of analog voice line.
  - Enterprise MIB for testing and some configuration functions.

  See the *9109 FXO Analog Voice Application Module (APM) Installation Instructions* for additional information.

- The FXS Voice APM supports:
  - FXS circuits.
  - µ-law PCM coding of analog voice line.
  - Enterprise MIB for testing and some configuration functions.

  See the *9109 FXS Analog Voice Application Module (APM) Installation Instructions* for additional information.

- The OCU-DP APM supports:
  - Either two or six ports.
  - Speeds of 56 kbps and 64 kbps, as well as 4-wire Switched 56.
  - Enterprise MIB for testing and some configuration functions.

  See the *9109 OCU-DP Application Module (APM) Installation Instructions* for additional information.

  To see faceplate LEDs and screens, see *Viewing APM LEDs and Control Leads*.

Hot Swapping Cards

NAMs and APMs, and their matching I/O cards, can be removed from their housing without powering off the system, and without having to reconfigure the cards each time they are moved.

- *NAM Insertion/Removal.* The NAM can be removed without powering off the system; however, all system functionality is lost when it is removed. When removed and inserted into another housing, the NAM applies its configuration from the previous housing to its current housing.
  - If the NAM is moved from a 2-slot housing to a 5-slot housing, the operator can use the configuration of the APM in Slot 02 of the previous housing. APMs in Slots 03 – 05 will be configured with the factory default settings.
  - If the NAM is moved from a 5-slot housing to a 2-slot, the factory default configuration options will be loaded.
- *APM Insertion/Removal.* An APM's configuration travels with the NAM. The NAM senses when an APM has been inserted or removed and automatically makes appropriate changes to screens, configuration options, and MIB objects.
  - When an APM is inserted in a previously unassigned slot, the system configures the APM using the factory default configuration.
  - When the same type of APM is inserted into a previously assigned slot, the system uses the configuration of the APM that previously occupied the slot so the APM does not have to be reconfigured.
  - When another type of APM is inserted into a previously assigned slot, an alarm and trap are generated for the slot. If accepted, the factory default configuration is loaded for the new APM type. If rejected, the new APM is ignored and the previous configuration is retained.

NOTE:

You do not have access to screens and configuration options that are not valid for the given configuration, nor can you preconfigure or predelete the configuration for an APM prior to inserting it in the housing. To see configuration options for an inserted APM, you must exit the configuration screen, then reenter it.

APM Insertion

When an APM is inserted into a housing, one of the following three conditions occurs:

If the slot previously . . .	Then . . .
Was unassigned	The configuration options for this new APM will be set to factory defaults and will be accessible from the MIB and the asynchronous terminal.
Contained the same type of APM	The existing configuration options will be used and will be accessible from the MIB and the asynchronous terminal.
Contained a different type of APM	The system will generate a Module Misconfiguration alarm and trap for the selected slot. The screens and field choices applicable to this APM will not be displayed until you accept the APM upon loading or saving a configuration, or via an enterprise MIB. When you accept the new APM, the previous APM's configuration is deleted, the new APM's configuration options are set to factory defaults, and the screens and field choices applicable to the new APM will be displayed. If you reject the APM, the configuration options for the previous APM can be edited, but all other configuration options and screens will not display fields or choices or MIB objects applicable to either the previous or the current APM.

APM Removal

When an APM is removed from its slot, you can still edit applicable configuration options.

If viewing a Status or Test screen when an APM is removed:

- The message **`APM Removed`** will display after the screen is refreshed and all fields relating to the APM will be cleared.
- Only the Esc (previous menu), Main Menu, and Exit virtual functions will be available when no other valid slots are available for selection.
- MIB objects applicable to the removed APM, and attempts to perform a **get** or **set** of those objects will display the message **`No Such Name`**.

Viewing APM Information

When an APM is installed in a 2-slot housing, the Identity screen includes information about the APM, along with the System and NAM information. When installed in a 5-slot housing, a submenu appears.

Main Menu → Status → Identity

For APMs installed in a 5-slot housing, the submenu includes the following:

— **System & NAM** – Provides information about the system, the FrameSaver NAM/unit, and DBM, if installed.

— **APM** – Provides information about the APM in each slot.

Whether appearing with the system information, or selected from a submenu, the following information is provided about an APM:

View this field . . .	To find the . . .
APM Type	Type of expansion APM that is installed in each slot: Sync Data, E&M Voice, FXS Voice, FXO Voice, OCU (2), or OCU (6). ■ **`Empty`** indicates that no APM is installed in the slot. ■ **`Failed`** indicates that the APM is not operational, or it has been removed from the slot. ■ **`Misconfig`** indicates that the APM in the slot is not configured as defined in the NAM's configuration table. ■ **`Unsupport`** indicates that an unsupported APM is installed in the slot; the NAM does not recognize the APM.
Serial Number	APM's 7-character serial number.
Software Revision	Software version currently being used by the APM. Format *nn.nn.nn* consists of a 6-digit number that represents the major and minor revision levels. If the flash memory is currently being downloaded, **`In Progress`** appears.
Hardware Revision	System's hardware version. Format *nnnn-nnx* consists of a 4-digit number, followed by 2 digits and 1 alphabetic character.

See *Displaying System Information* in Chapter 7, *Operation and Maintenance*, for System & NAM information.

Viewing APM LEDs and Control Leads

The APM's faceplate includes LEDs (light-emitting diodes) that provide status on the card and its interfaces. The Display LEDs and Control Leads feature allows you to monitor a remote APM, which is useful when troubleshooting control lead problems.

To access the Display LEDs and Control Leads screen:

Main Menu →Status →Display LEDs and Control Leads

Voice Port APM Example

```
main/status/leds                                                         9191
Device Name: Node A                                          5/26/2000 23:32

                        DISPLAY LEDS & CONTROL LEADS

                         SLOT: 2  –  FXS Voice APM

                              Voice Ports
                                  OK











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

Synchronous Data Port APM Example

```
main/status/leds                                                         9191
Device Name: Node A                                           5/26/2000 23:32

                          DISPLAY LEDS & Control Leads

                        SLOT: 2 – Sync Data Port APM

                  Port-1     Port-2     Port-3     Port-4
                  OK         OK         OK         OK
                  TXD        TXD        TXD        TXD
                  RXD        RXD        RXD        RXD
                  DTR        DTR        DTR        DTR
                  CTS        CTS        CTS        CTS

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

OCU-DP APM Example

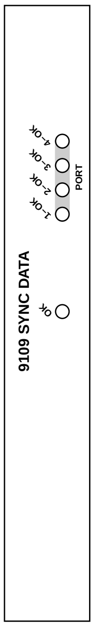
```
main/status/leds                                                         9191
Device Name: Node A                                           5/26/2000 23:32

                       DISPLAY LEDS & CONTROL LEADS

                        SLOT: 2 – OCU (6) APM

                                  OCU-DP
                                  1-TST
                                  2-TST
                                  3-TST
                                  4-TST
                                  5-TST
                                  6-TST

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

See *APM LED Descriptions* to understand the meaning of the LEDs, and to see the appropriate faceplates.

See *Viewing LEDs and Control Leads* in Chapter 7, *Operation and Maintenance*, for additional information.

APM LED Descriptions

When an APM is installed, see Table 5-1 for a Synchronous Data APM's LEDs, Table 5-2 for a Voice APM's LED, and Table 5-3 for an OCU-DP APM's LEDs.



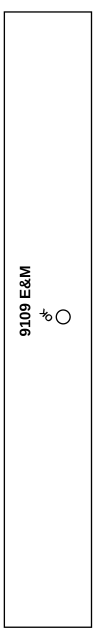
00-15154-01

Table 5-1. Synchronous Data APM LEDs

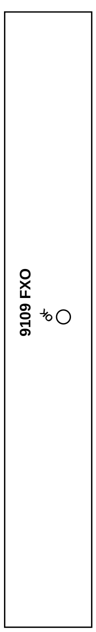
Label	Indication	Color	What It Means
General			
OK	Power and Operational Status	Green	ON – APM has power and is operational. OFF – APM is in a local self-test, or there is a failure.
Synchronous Data Ports			
1-OK 2-OK 3-OK 4-OK	Operational Status	Green	ON – The interchange circuits for the port are in the correct state to transmit and receive data. OFF – The port is idle. Occurs if the port is disabled, if an EDL OOF or EER condition is present, if a DCLB is active, or if the port is configured to monitor DTR and/or RTS and the lead(s) is not asserted.

Table 5-2. Voice APM LED

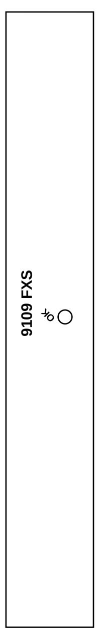
Label	Indication	Color	What It Means
OK	Power and Operational Status	Green	ON – APM has power and is operational. OFF – APM is in a local self-test, or there is a failure.



00-15141-01



00-15648-01



00-15139-01

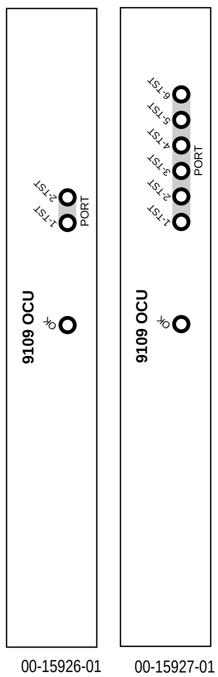


Table 5-3. OCU-DP APM LEDs

Label	Indication	Color	What It Means
General			
OK	Power and Operational Status	Green	ON – APM has power and is operational. OFF – APM is in a local self-test, or there is a failure.
OCU-DP Ports (2 or 6 Port APMs)			
1-TST 2-TST 3-TST 4-TST 5-TST 6-TST	Operational Status	Yellow	ON – A test is in progress. OFF – No test is active on the port, including all test pattern generation, and any loopback that may be active on the local loop or the OCU-DP APM.

APM Configuration Option Tables

The following configuration option tables are included in this chapter:

- Table 5-4. FXS Voice APM Options
- Table 5-5. FXO Voice APM Options
- Table 5-6. E&M Voice APM Options
- Table 5-7. OCU-DP APM Options

For a Sync Data APM, see *Configuring Sync Data APM Ports* for information.

Configuring APM Ports

Configure the following ports on the NAM and any APMs that are installed in your system.

- Synchronous data Port-2 on the NAM or a Sync Data APM
- Voice port on FXS, FXO, and E&M APMs

Once you have a port configured, you can copy that configuration to other ports of the same type (see *Copying Port Configurations*).

Copying Port Configurations

When you have similar card and port types, you can use the Copy Ports feature to copy a configured port to another port. For example, you can configure Port-1 on a Sync Data APM, then copy that configuration to the rest of the synchronous data ports on that APM. Or, if two FXO APMs are installed, you can configure the FXO port in one slot, then copy that configuration to an FXO APM in another slot.

Based upon the slot selected, the type of card in that slot is displayed (e.g., FXS Voice). When copying the configuration of one port to another, the ports being copied to can be enabled or disabled.

NOTES:

Only ports of the same type will be available for selection and affected by the copy process (e.g., Sync Data APM ports, or Port-2 on the FrameSaver NAM when its Port Use option is set to Synchronous Data).

For OCU-DP APMs, you can use the Copy Ports feature ports between 2-Port and 6-port versions of the OCU-DP APM.

▶ Procedure

1. Select the Copy function key from one of the following menu selections to access the Copy Ports screen.

   Main Menu → Configuration → Data Ports → Physical

   Main Menu → Configuration → Voice Ports

   Main Menu → Configuration → OCU-DP Ports

2. Select the slot and port that you want to copy (**From:**).

3. Select the slot and port that you want to configure using the Copy Ports feature (**To:**), or select All.

   — If you select a slot and port, the **`Perform Copy Then Increment`** prompt appears. Once the copy process is complete, the next highest port appears for selection (e.g., copying Port-1 to Port-2 brings up Port-3 for selection).

   — If you select All, the **`Perform Copy`** prompt appears.

4. Press Enter to begin the copy process.

   — If a specific port was selected, only the selected port in the selected slot will be updated.

   — If All was selected, all ports on the APM in the selected slot will be updated.

Configuring Sync Data APM Ports

See *Configuring a User Data Port* in Chapter 3, *Configuration*, to configure synchronous data port(s) on the FrameSaver NAM or a Sync Data APM.

Main Menu → Configuration → Data Ports → Physical

Select the slot where the Sync Data APM is located, and the port you want to configure. Use the Copy Ports feature for an easy way to configure the other ports on the APM (see *Copying Port Configurations*).

Configuring FXS Analog Voice APM Ports

Select Voice Ports from the Configuration menu, then select the slot where the FXS APM is located (see Table 5-4) to configure the 9109 FXS analog voice APM port.

Configuration →Voice Ports

Table 5-4. FXS Voice APM Options (1 of 4)

Port Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether the FXS voice port is in use, and can be configured and assigned to a time slot on the T1 interface to transmit and receive voice frequency signals. *Display Conditions* – This option only appears when Port Status is set to Enable. **Enable** – The port is active, and can be configured and assigned to a time slot. **Disable** – The port is not active, cannot be configured, and does not take up a time slot. ■ No alarms or traps configured for the port will be generated. ■ Existing cross-connect assignments associated with the port will be cleared. The message **`This action will clear any Cross Connections for the Port. Are You Sure? No`** appears. If you select: **No** – The operation is cancelled. (Pressing either the Esc or Ctrl-a key acts as a No.) **Yes** – Port status is disabled and any cross connections are cleared.
Operating Mode
Possible Settings: **FXS, FXSDN, FXSDN/WINK, PLAR, DPO** Default Setting: **FXS**
Selects the operating mode for the FXS voice port. *Display Conditions* – This option only appears when Port Status is set to Enable. **FXS** – Enables the Foreign Exchange Station (FXS) mode, supporting a bidirectional connection to a telephone device, PBX, or key system trunk. This mode uses 4-state signaling (A&B). **FXSDN** – Enables Foreign Exchange Station Software-Defined Network (FXSDN) mode for operation on software-defined networks. This mode is used by Class 4 switches and uses 2-state signaling (A=B). A ring-back signal may need to be provided to the calling end, which is controlled by the Ring-Back Tone option. **FXSDN/WINK** – Enables the mode FXSDN with WINK which is similar to FXSDN, but in addition provides an indication to the central office (CO) when the station equipment is ready to receive signaling information. This consists of detecting an off-hook signal from the CO, which initiates a configurable “wink delay” followed by a configurable off-hook signal back to the CO. **PLAR** – Private Line Automatic Ring-down (PLAR) allows “hotline” point-to-point dedicated connection of two phones. When one phone goes off-hook, the other phone starts ringing. **DPO** – The Dial Pulse Originating (DPO) mode is similar to FXS, except for supporting out-going, one-way trunks from a PBX (direct outward dialing) or key system, or station instrument. No ringing is provided in this mode.

Table 5-4. FXS Voice APM Options (2 of 4)

Signaling Type
Possible Settings: **Loop-Start, Loop-Start/Fwd Disc, Ground-Start, Ground-Start-Immediate, Ground-Start-Automatic, d3, d4** Default Setting: **Loop-Start**
Determines the type of signaling for the FXS voice port. *Display Conditions* – This option only appears when: ■ Port Status is set to Enable. ■ Operating Mode is not set to DPO. NOTE: If you change the value of the Operating Mode option so that the Signaling Type option contains an invalid value, then the invalid value will be forced to the first valid setting for this option. **Loop-Start** – Enables the signaling used for basic telephone service stations, simple PBX trunks, or key systems. Loop Start only appears if Operating Mode is set to FXS, FXSDN, or FXSDN/WINK. **Loop-Start/Fwd Disc** – Enables the signaling used for automated answering equipment. This selection only appears if Operating Mode is set to FXS, FXSDN, or FXSDN/WINK. **Ground-Start** – Enables the signaling used for two-way PBX trunks. Helps to prevent “glaring”, i.e., call collision. This selection only appears if Operating Mode is set to FXS, FXSDN, or FXSDN/WINK. **Ground-Start-Immediate** – Enables the signaling used for fast response time to the PBX or station. This selection only appears if Operating Mode is set to FXS. **Ground-Start-Automatic** – Enables the signaling used for fast response time to the central office. This selection only appears if Operating Mode is set to FXS. **d3** – The APM meets the pre-1988 specifications for PLAR circuits. This selection only appears if Operating Mode is set to PLAR. **d4** – The APM meets the post-1988 specifications for PLAR circuits. This selection only appears if Operating Mode is set to PLAR.
Terminating Impedance (ohms)
Possible Settings: **600, 900** Default Setting: **600**
Determines the terminating impedance (in ohms) for the port. *Display Conditions* – This option only appears when Port Status is set to Enable. **600** – The terminating impedance is 600 ohms. **900** – The terminating impedance is 900 ohms.

Table 5-4. FXS Voice APM Options (3 of 4)

Wink Delay (10 ms)
Possible Settings: **1 – 99** Default Setting: **15**
Determines the amount of delay before the wink signal is generated towards the network, and when an off-hook signal from the CO is detected in increments of 10 milliseconds. *Display Conditions* – This option only appears when: ■ Port Status is set to Enable. ■ Operating Mode is set to FXODN/WINK. **10 to 990** – The valid range is from 10 to 990 ms, in 10 ms increments. The settings are numbers between 1 and 99, representing such increments. The default is 20, for a wink delay of 150 ms.
Wink Duration (10 ms)
Possible Settings: **1 – 99** Default Setting: **20**
Determines the duration of the wink signal generated towards the network when an off-hook signal for the CO is detected and after the wink delay has elapsed in increments of 10 milliseconds. *Display Conditions* – This option only appears when: ■ Port Status is set to Enable. ■ Operating Mode is set to FXODN/WINK. **10 to 990 ms** – The valid range is from 10 to 990 ms, in 10 ms increments. The settings are numbers between 1 and 99, representing such increments. The default is 20, for a wink duration of 200 ms.
Rx Gain (dB)
Possible Settings: **–10.00, –9.5, –9.0, –8.5, . . ., 0.0, +0.5, +1.0, +1.5, +2.0** Default Setting: **0.0**
Determines the receive path analog signal amplification, or gain, on the FXS voice port in decibels. This is the gain (increased signal level) or attenuation (decreased signal level) applied to the signal. *Display Conditions* – This option only appears when Port Status is set to Enable. **–10.00 to +2.0** – Increases or decreases the signal level. The more positive the number, the greater the signal level.

Table 5-4. FXS Voice APM Options (4 of 4)

Tx Attenuation (dB)
Possible Settings: **–10.00, –9.5, –9.0, –8.5, . . ., 0.0, . . ., +4.0, +4.5, +5.0** Default Setting: **0.0**
Determines the amount of attenuation, in dB, that the FXS voice port applies to the analog signal presented by the user's analog equipment. Positive TX Attenuation settings reduce the level of the encoded analog signals sent towards the telephone network and negative settings introduce gain. When connecting permissive mode modems and fax machines, a setting of +3 dB should result in a compliant, encoded analog of less than –12 dBm. The proper setting of this strap is crucial to ensuring compliance with Part 68, FCC Rules and Industry Canada's CS-03 Specification. *Display Conditions* – This option only appears when Port Status is set to Enable. **–10.00 to +5.0** – Increases or decreases the signal level. The more negative the number, the greater the signal level (opposite of Rx Gain settings).
Ring-Back Tone
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Allows generation of an audible tone toward the network in response to an incoming call request, normally referred to as a ring-back. This feature is invoked only when the central office (CO) does not provide it, as with a Class 4 ESS switch. This tone indicates to the calling party that the called line has been reached and ringing has started. Use the ring-back tone when you have a PLAR application. *Display Conditions* – This option only appears when Port Status is set to Enable. **Enable** – Generates a ring-back tone toward the network in response to an incoming call request. **Disable** – Does not generate a ring-back tone toward the network in response to an incoming call request.
Trunk Cond in CGA
Possible Settings: **Busy, Idle** Default Setting: **Busy**
Determines the trunk condition or state that the port is forced into as a result of the Carrier Group Alarm (CGA). *Display Conditions* – This option only appears when Port Status is set to Enable. **Busy** – Forces the port to Busy during the Carrier Group Alarm. **Idle** – Forces the port to Idle during the Carrier Group Alarm.

Configuring FXO Analog Voice APM Ports

Select Voice Ports from the Configuration menu, then select the slot where the FXO APM is located (see Table 5-5) to configure the 9109 FXO analog voice APM port.

Configuration →Voice Ports

Table 5-5. FXO Voice APM Options (1 of 3)

Port Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether the FXO voice port is in use, and can be configured and assigned to a time slot on the T1 or DSX interface in order to transmit and receive voice frequency signals. *Display Conditions* – This option only appears when Port Status is set to Enable. **Enable** – The port is active, and can be configured and assigned to a time slot. **Disable** – The port is not active, cannot be configured, and does not take up a time slot. ■ No alarms or traps configured for the port will be generated. ■ Existing cross-connect assignments associated with the port will be cleared. The message `This action will clear any Cross Connections for the Port. Are You Sure? No` appears. If you select: **No** – The operation is cancelled. (Pressing either the Esc or Ctrl-a key acts as a No.) **Yes** – Port status is disabled and any cross connections are cleared.
Operating Mode
Possible Settings: **FXO, FXODN, FXODN/WINK, DPT** Default Setting: **FXO**
Selects the operating mode for the FXO voice port. *Display Conditions* – This option only appears when Port Status is set to Enable. **FXO** – Enables the Foreign Exchange Office (FXO) mode, supporting a bidirectional connection to a PBX phone line. This mode uses 4-state signaling (A&B). **FXODN** – Enables Foreign Exchange Office Software-Defined Network (FXODN) mode for operation on software-defined networks. This mode is used by Class 4 switches and uses 2-state signaling (A=B). **FXODN/WINK** – Enables the mode FXODN with WINK which is similar to FXODN, but in addition provides an indication toward the network interface when the attached analog equipment is ready to receive signaling information. This consists of detecting an off-hook signal from the network interface, which initiates a configurable “wink delay” followed by a configurable off-hook signal back to the network interface. **DPT** – The Dial Pulse Terminating (DPT) mode is similar to FXO, except for supporting in-coming, one-way trunks to a PBX (direct inward dialing) or key system.

Table 5-5. FXO Voice APM Options (2 of 3)

Signaling Type
Possible Settings: **Loop-Start, Loop-Start/Fwd Disc, Ground-Start** Default Setting: **Loop-Start**
Determines the type of signaling for the FXO voice port. *Display Conditions* – This option only appears when: ■ Port Status is set to Enable. ■ Operating Mode is not set to DPT. **Loop-Start** – Enables the signaling used for basic telephone service stations, simple PBX trunks, or key systems. **Loop-Start/Fwd Disc** – Enables the signaling used for automated answering equipment. **Ground-Start** – Enables the signaling used for two-way PBX trunks. Helps to prevent “glaring”, i.e., call collision.
Terminating Impedance (ohms)
Possible Settings: **600, 900** Default Setting: **600**
Determines the terminating impedance (in ohms) for the port. *Display Conditions* – This option only appears when Port Status is set to Enable. **600** – The terminating impedance is 600 ohms. **900** – The terminating impedance is 900 ohms.
Wink Delay (10 ms)
Possible Settings: **1 – 99** Default Setting: **15**
Determines the amount of delay before the wink signal is generated towards the network, and when an off-hook signal from the CO is detected in increments of 10 milliseconds. *Display Conditions* – This option only appears when: ■ Port Status is set to Enable. ■ Operating Mode is set to FXODN/WINK or DPT. **10 to 990** – The valid range is from 10 to 990 ms, in 10 ms increments. The settings are numbers between 1 and 99, representing such increments. The default is 15, for a wink delay of 150 ms.
Wink Duration (10 ms)
Possible Settings: **1 – 99** Default Setting: **20**
Determines the duration of the wink signal generated towards the network when an off-hook signal for the CO is detected and after the wink delay has elapsed in increments of 10 milliseconds. *Display Conditions* – This option only appears when: ■ Port Status is set to Enable. ■ Operating Mode is set to FXODN/WINK or DPT. **10 to 990 ms** – The valid range is from 10 to 990 ms, in 10 ms increments. The settings are numbers between 1 and 99, representing such increments. The default is 20, for a wink duration of 200 ms.

Table 5-5. FXO Voice APM Options (3 of 3)

Rx Gain (dB)
Possible Settings: **–10.00, –9.5, –9.0, –8.5, . . ., 0.0, +0.5, +1.0, +1.5, +2.0** Default Setting: **0.0**
Determines the receive path analog signal amplification, or gain, on the FXO voice port in decibels. This is the gain (increased signal level) or attenuation (decreased signal level) applied to the signal. *Display Conditions* – This option only appears when Port Status is set to Enable. **–10.00 to +2.0** – Increases or decreases the signal level. The more positive the number, the greater the signal level.
Tx Attenuation (dB)
Possible Settings: **–10.00, –9.5, –9.0, –8.5, . . ., 0.0, . . ., +4.0, +4.5, +5.0** Default Setting: **0.0**
Determines the amount of attenuation, in dB, that the FXO voice port applies to the analog signal presented by the user's analog equipment. Positive TX Attenuation settings reduce the level of the encoded analog signals sent towards the telephone network and negative settings introduce gain. When connecting permissive mode modems and fax machines, a setting of +3 dB should result in a compliant, encoded analog of less than –12 dBm. The proper setting of this strap is crucial to ensuring compliance with Part 68, FCC Rules and Industry Canada's CS-03 Specification. *Display Conditions* – This option only appears when Port Status is set to Enable. **–10.00 to +5.0** – Increases or decreases the signal level. The more negative the number, the greater the signal level (opposite of Rx Gain settings).
Trunk Cond in CGA
Possible Settings: **Busy, Idle** Default Setting: **Busy**
Determines the trunk condition or state that the port is forced into as a result of the Carrier Group Alarm (CGA). *Display Conditions* – This option only appears when Port Status is set to Enable. **Busy** – Forces the port to Busy during the Carrier Group Alarm. **Idle** – Forces the port to Idle during the Carrier Group Alarm.

Configuring E&M Analog Voice APM Ports

Select Voice Ports from the Configuration menu, then select the slot where the E&M APM is located (see Table 5-6) to configure the 9109 E&M analog voice APM port.

Configuration → Voice Ports

Table 5-6. E&M Voice APM Options (1 of 2)

Port Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether the E&M voice port is in use, and can be configured and assigned to a time slot on the T1 or DSX-1 interface in order to transmit and receive voice frequency signals. *Display Conditions* – This option only appears when Port Status is set to Enable. **Enable** – The port is active, and can be configured and assigned to a time slot. **Disable** – The port is not active, cannot be configured, and does not take up a time slot. ■ No alarms or traps configured for the port will be generated. ■ Existing cross-connect assignments associated with the port will be cleared. The message **`This action will clear any Cross Connections for the Port. Are You Sure? No`** appears. If you select: **No** – The operation is cancelled. (Pressing either the Esc or Ctrl-a key acts as a No.) **Yes** – Port status is disabled and any cross connections are cleared.
Operating Mode
Possible Settings: **E&M, Transmit Only** Default Setting: **E&M**
Selects the operating mode for the E&M voice port. *Display Conditions* – This option only appears when Port Status is set to Enable. **E&M** – Enables normal earth and magnetic (E&M) mode. **Transmit Only** – Enables the mode used to support 4-wire private-line modems that do not require E&M signaling.
Rx Gain (dB)
Possible Settings: **–17.0, –16.5, –16.0, –15.5, –15.0 . . ., 0.0, . . ., +15.0, +15.5, +16.0** Default Setting: **0.0**
Determines the receive path analog signal amplification on the E&M voice port in decibels. This is the gain (increased signal level) or attenuation (decreased signal level) applied to the signal before it is presented to the user's analog equipment. *Display Conditions* – This option only appears when Port Status is set to Enable. **–17.0 to +16.0** – Increases or decreases the signal level. The more positive the number, the greater the signal level.

Table 5-6. E&M Voice APM Options (2 of 2)

Tx Attenuation (dB)
Possible Settings: **–17.0, –16.5, –16.0, –15.5, –15.0 . . ., 0.0, . . ., +15.0, +15.5, +16.0** Default Setting: **0.0**
Determines the amount of attenuation, in dB, that the E&M voice receive port applies to the analog signal presented by the user's analog equipment transmit port. Positive TX Attenuation settings reduce the level of the encoded analog signals sent towards the telephone network, and negative settings will introduce gain. The proper setting of this strap is crucial to ensuring compliance with Part 68, FCC Rules and Industry Canada's CS-03 Specification. *Display Conditions* – This option only appears when Port Status is set to Enable. **–17.0 to +16.0** – Increases or decreases the signal level. The more positive the number, the greater the signal level.
Trunk Cond in CGA
Possible Settings: **Busy, Idle** Default Setting: **Busy**
Determines the trunk condition or state that the port is forced into as a result of the Carrier Group Alarm (CGA). *Display Conditions* – This option only appears when Port Status is set to Enable. **Busy** – Forces the port to Busy during a CGA. **Idle** – Forces the port to Idle during a CGA.

Configuring OCU-DP APM Ports

Select OCU-DP Ports from the Configuration menu, then select the slot where the OCU-DP APM is located (see Table 5-7) to configure a port on an 9109 OCU-DP APM.

Configuration →OCU-DP Ports

Select the port to be configured (Port 1 – 6). Use the Copy Ports feature for an easy way to configure the other ports on the APM (see *Copying Port Configurations*).

Table 5-7. OCU-DP APM Options

Port Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether the OCU-DP port is in use, and can be configured and used to transmit and receive data. **Enable** – The port is active, and can be configured used to **Disable** – The port is not active, cannot be configured, and cannot transmit/receive data. ■ No alarms or traps configured for the port will be generated. ■ Existing cross-connect assignments associated with the port will be cleared. The message `This action will clear any Cross Connections for the Port. Are You Sure? No` appears. If you select: **No** – The operation is cancelled. (Pressing either the Esc or Ctrl-a key acts as a No.) **Yes** – Port status is disabled and any cross connections are cleared.
Port Rate
Possible Settings: **56K, 64KCC, Switched_56** Default Setting: **56K**
Selects the rate for the port. *Display Conditions* – This option only appears when Port Status is set to Enable. **56K** – The setting for 56 kbps. **64KCC** – The setting for 64 kbps Clear Channel. **Switched_56** – The rate for 4-wire Switched 56.
Loopback Detection
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the FrameSaver unit will detect loopback activation codes coming from the network. *Display Conditions* – This option only appears when Port Status is set to Enable. **Enable** – Loopback code detection is enabled. **Disable** – Loopback code detection is disabled.

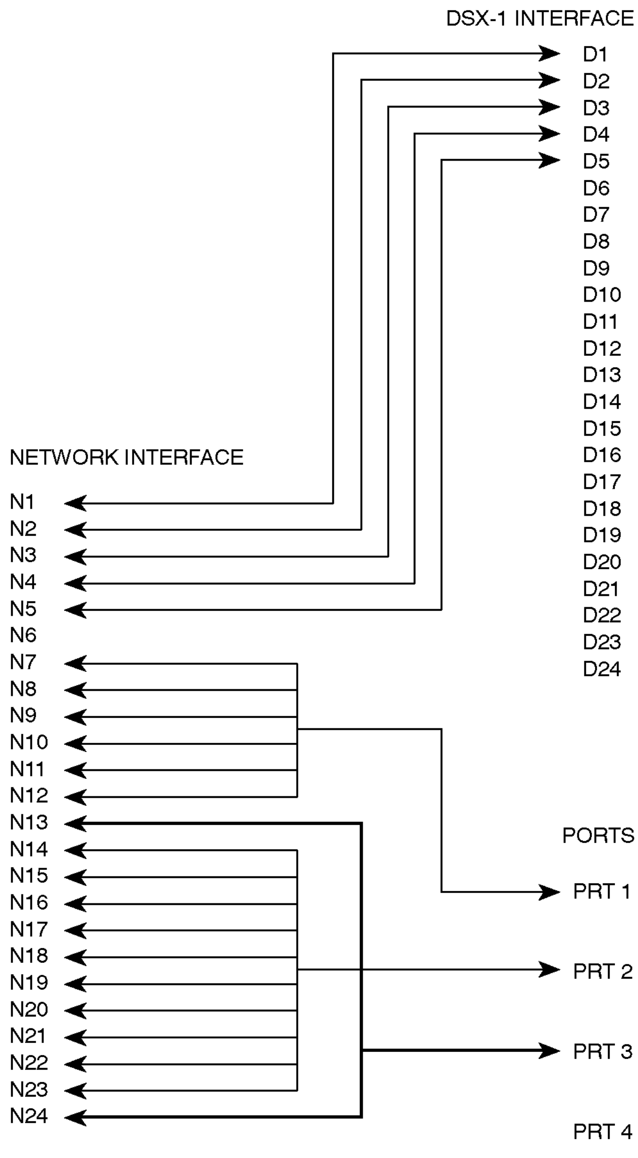
Assigning APM Ports to Network or DSX-1 Time Slots

The following APM ports can be assigned to network or DSX-1 time slots:

- Voice Port Assignments
- Synchronous Data Port Assignments
- OCU-DP Port Assignments

See *Assigning Synchronous Data Ports to Network or DSX-1 Time Slots* in Chapter 3, *Configuration*, when configuring a Sync Data APM. An example of data channel allocation is shown below.

Channel Allocation Example



The same procedure is used to assign voice, synchronous data, and OCU-DP ports to selected time slots.

▶ Procedure

To assign APM ports to network or DSX-1 time slots:

1. Select the appropriate screen for the APM.

   Configuration →Time Slot Assignment/Cross Connect → Voice Port Assignments

   Configuration →Time Slot Assignment/Cross Connect → Sync Data Port Assignments

   Configuration →Time Slot Assignment/Cross Connect → OCU-DP Port Assignments

2. At the **`Assign To`** field, select **`Net1`** to assign the APM port to Network 1 interface time slots, or **`DSX-1`** to assign the port to DSX-1 interface time slots.

3. Move the cursor to the next time slot to be changed (underlined). Use the spacebar or type in the desired slot and port.

   Repeat this step until all desired time slots are assigned.

4. Save the configuration.

See *Assigning Time Slots/Cross Connections* in Chapter 3, *Configuration*, for additional information.

Assigning Voice Ports to Network or DSX-1 Time Slots

Use the Voice Port Assignments screen to view the status of all DS0 assignments on the Network or DSX-1 interface, or to assign voice ports to selected time slots.

Assigning Synchronous Data Ports to Network or DSX-1 Time Slots

Use the Sync Data Port Assignment screen to view the status of all DS0 assignments on the Network 1 or DSX-1 interface, or to assign synchronous data ports to selected time slots.

All ports on the Sync Data APM are synchronous ports, and Synchronous Data Port-to-Synchronous Data Port assignments are not supported.

See *Assigning Synchronous Data Ports to Network or DSX-1 Time Slots* in Chapter 3, *Configuration*, for additional information.

Assigning OCU-DP Ports to Network or DSX-1 Time Slots

Use the OCU-DP Port Assignments screen to view the status of all DS0 assignments on the network or DSX-1 interface, or to assign OCU-DP data ports to network or DSX-1time slots.

Checking Voice APM Status

Select Voice Status from the Status menu to see the status of the analog voice cards that are installed.

Main Menu → Status → Voice Status

Enter the desired voice APM's slot number. Status information varies depending upon the type of voice APM installed.

Table 5-8. Voice APM Status (1 of 3)

View this field . . .	To find the . . .
E&M Voice APM	
Port Status	Status of the port.
Assigned To	Interface the port is assigned to.
Operating Mode	Operating mode of the voice port that was configured using the Operating Mode configuration option on the Voice Ports screen. See Table 5-6. E&M Voice APM Options for configuration information.
Signaling Type	Type of signaling used by the voice port that was configured using the switches on the E&M APM. See Table 5-6. E&M Voice APM Options for configuration information.
Call Progress	Current condition of the port.
TX ABCD bits	Current value of the ABCD bits that are being transmitted to the T1 interface.
RX ABCD bits	Current value of the ABCD bits that are being received from the T1 interface.
E-Lead State	Current status of the E-lead (On or Off).
M-Lead State	Current status of the M-lead (On or Off).
Trunk Cond CGA	Displays the status of trunk conditioning (On for CGA, Off for no CGA).
FXO Voice APM	
Port Status	Status of the port.
Assigned To	Interface the port is assigned to.
Operating Mode	Operating mode of the voice port that was configured using the Operating Mode configuration option on the Voice Ports screen.
Signaling Type	Type of signaling used by the voice port that was configured using the Signaling Type configuration option on the Voice Ports screen. See Table 5-5. FXO Voice APM Options on configuration information.
Call Progress	Current condition of the port.

Table 5-8. Voice APM Status (2 of 3)

View this field . . .	To find the . . .
FXO Voice APM (Cont'd)	
TX ABCD bits	Current value of the ABCD signaling bits that are being transmitted to the T1 interface.
RX ABCD bits	Current value of the ABCD signaling bits that are being received from the T1 interface.
T-R Control	Current status of the tip and ring leads: ■ Loop. Tip and Ring are connected together. ■ Rgnd. Ring lead is attached to ground. ■ Open. Ring lead is not connected to either the Tip lead or the ground. ■ Lpgnd. Tip and Ring are connected together, and are connected to ground.
T-R Receive	Status of what the attached device is doing with the Tip and Ring leads of the FXO port. ■ RbTo. Attached device has battery applied to the Ring lead and the Tip lead is opened. ■ RbTg. Attached device has battery applied to the Ring lead and the Tip lead is grounded. ■ TbRg. Attached device has battery applied to the Tip lead and the Ring lead is grounded. ■ Ring. Attached device is applying Ringing voltage between Tip and Ring. ■ ToRo. Attached device has both Tip and Ring leads open. ■ TgRo. Attached device has the Tip lead grounded and the Ring lead open. ■ TgR*. Attached device has the Tip lead grounded and the Ring lead state is unknown. ■ ToR*. Attached device has the Tip lead open and the Ring lead state is unknown. ■ RoT*. Attached device has the Ring lead open and the Tip lead state is unknown.
Trunk Cond CGA	Displays the status of trunk conditioning (On during CGA, Off for no CGA).

Table 5-8. Voice APM Status (3 of 3)

View this field . . .	To find the . . .
FXS Voice APM	
Port Status	Status of the port.
Assigned To	Interface the port is assigned to.
Operating Mode	Operating mode of the voice port that was configured using the Operating Mode configuration option on the Voice Ports screen. See Table 5-4. FXS Voice APM Options for configuration information.
Signaling Type	Type of signaling used by the voice port that was configured using the Signaling Type configuration option on the Voice Ports screen. See Table 5-4. FXS Voice APM Options for configuration information.
Call Progress	Current condition of the port.
TX ABCD bits	Current value of the ABCD signaling bits that are being transmitted to the T1 interface.
RX ABCD bits	Current value of the ABCD signaling bits that are being received from the T1 interface.
T-R Control	Current status of the tip and ring leads: ■ RbTo. A –48 VDC battery is applied to the Ring lead and the Tip lead is opened. ■ RbTg. A –48 VDC battery is applied to the Ring lead and the Tip lead is grounded. ■ TbRg. A –48 VDC battery is applied to the Tip lead and the Ring lead is grounded. ■ Ring. Ringing voltage is applied between Tip and Ring.
T-R Receive	Status of what the attached device is doing with the Tip and Ring leads of the FXS port. ■ Loop. Tip and Ring are connected together. ■ Rgnd. Ring lead is grounded by attached device. ■ Open. Ring lead is not connected to either the Tip lead or the ground.
Trunk Cond CGA	Displays the status of trunk conditioning (On for CGA, Off for no CGA).

APM Performance Statistics

In addition to the Performance Statistics collected for all interfaces (see *Performance Statics* in Chapter 7, *Operation and Maintenance*), DDS Line statistics are available when an OCU-DP APM is installed.

Viewing DDS Line Performance Statistics

When an OCU-DP APM is installed, select DDS Line from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → DDS Line

Table 5-9. DDS Line Performance Statistics

Statistic	What It Indicates
No Signal Count	Number of times a No Signal (NS) condition has occurred.
Out of Service Count	Number of times an Out-of-Service (OOS) condition has occurred.
Out of Frame Count	Number of times an Out-of-Frame (OOF) condition has occurred.
Excessive BPV Count	Number of times an excessive bipolar violation (BPV) condition has occurred. This is a count of BPVs that qualify as being excessive. The count is incremented when at least one invalid BPV occurs every 20 ms over a 2-second period.
BPV Count	Number of errors received when a BPV condition has occurred. This is a total count of invalid BPV errors.

[1] Elapsed time is also shown for all statistics except the BPV Count in the hours:minutes:seconds format. This is the total amount of time that the FrameSaver unit has experienced the condition since the unit's last power cycle.

To clear OCU-DP APM performance statistics, use the ClrDDSStats function key.

APM Tests

In addition to the tests available for the network interfaces and user data ports (see *Tests Available* in Chapter 8, *Troubleshooting*), Voice Port and OCU-DP physical tests are available when an APM is installed.

The following tests can be run for an APM:

- **Sync Data APM** – All the PVC and physical tests available to a user data port are available to synchronous data ports on the APM. See *Tests Available* in Chapter 8, *Troubleshooting*, for synchronous data port test information.

- **Analog Voice APM Physical Tests** – These tests include:

  — Digital Loopback

  — Analog Loopback

  — Send Test Tone

  — Force and Monitor Signaling (Tx ABCD bits, Rx ABCD bits, and Tip & Ring Leads)

- **OCU-DP APM Physical Tests** – These tests include:

  — Nonlatching Loopback (local and remote) – 56K and Switched 56

  — Latching Loopback (local and remote) – 64K clear channel (CC)

  — OCU Loopback

  — DS-0 Loopback

  — Line Loopback

  — Data Loopback

  — Pattern Tests (All-zeros, All-ones, 63, 511, and 2047)

Analog Voice APM Physical Port Tests

Tests are available to run on voice APM ports for any installed and enabled APM. These tests include:

- Digital Loopback
- Analog Loopback
- Send Test Tone
- Force and Monitor Signaling

▶ Procedure

To start and stop a voice port loopback:

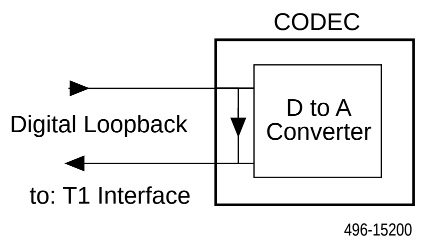
1. Follow this menu selection sequence:

   Main Menu → Test → Voice Port Tests

2. Select the APM slot number and port to be tested.
3. To send the test tone, highlight **`Start`** in the Command column and press Enter. The Status changes to Active. The length of time that the test has been running is shown in the Results column.
4. To stop the test, press Enter to send the **`Stop`** command. Start reappears and the status of the test changes back to Inactive.

Digital Loopback

A Digital Loopback loops the digital voice signal received from the T1 interface back to the same interface, just before the signal reaches the digital-to-analog converter on the voice port.

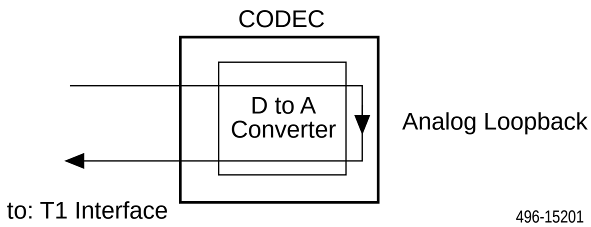


The following tests cannot be running when a Digital Loopback is started:

- DRS or Quient Test Tone
- Analog Loopback

Analog Loopback

An Analog Loopback loops the analog voice signal received from the T1 interface back to the same interface, after the signal passes through the digital-to-analog (D to A) converter on the voice port.

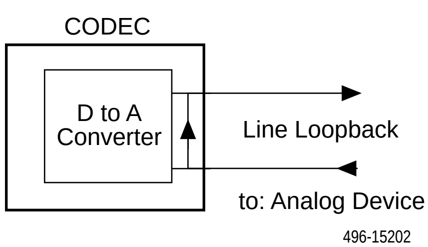


The following tests cannot be running when an Analog Loopback is started:

- DRS or Quient Test Tone
- Digital Loopback
- Line Loopback

Line Loopback

This test is only available for an E&M APM. A Line Loopback loops the analog voice signal received from the analog line/device connected to the port back to the same line/device, before passing through the digital-to-analog (D to A) on the voice port.



The following tests cannot be running when a Line Loopback is started:

- DRS or Quient Test Tone
- Analog Loopback

Send Test Tone

A test tone can be sent to the T1 interface or the user data port. Select one of the following types of test tones:

- **DRS** – Digital Reference Signal, a 1004 Hz, 0.0 dBm tone (the default).
- **Quiet** – No signal is sent.

▶ Procedure

To start and stop a test tone:

1. Follow this menu selection sequence:

   Main Menu → Test → Voice Port Tests

2. Select the APM slot number and port to be tested.
3. Move the cursor to Send ___ to T1 Interface or Send ___ to User, and select the type of tone to be sent, DRS or Quiet.
4. To send the test tone, highlight **`Start`** in the Command column and press Enter. The Status changes to Active. The length of time that the test has been running is shown in the Results column.
5. To stop the test, highlight **`Stop`** under Command and press Enter. The Status changes to Inactive.

The following tests cannot be running when a test tone is started:

- Any loopbacks on the same port
- Another type of test tone (other than the one currently running) on the same interface

Force and Monitor Signaling

Force and Monitor Signaling enables the sending and receiving of various signals to/from the T1 interface to which the APM port is assigned.

▶ Procedure

To force and monitor signaling:

1. Follow this menu selection sequence:

   Main Menu → Test → Voice Port Tests

2. Select the APM slot number and port to be tested.
3. Press the PgDn function key to go to page 2.
4. Enter the desired setting for each field (see Table 5-10).
5. To send the test tone, highlight **`Start`** in the Command column and press Enter. The Status changes to Active. The length of time that the test has been running is shown in the Results column.
6. To monitor the test, look at the values displayed under Monitor Signaling.
7. To stop the test, highlight **`Stop`** under Command and press Enter. The Status changes to Inactive.

See Table 5-10 for the appropriate settings of the Force and Monitor Signaling fields.

Table 5-10. Force and Monitor Signaling (1 of 3)

To force these fields . . .	To these settings . . .
For ESF framing: ABCD bits (Tx and Rx) *For D4 framing:* AB bits (Tx and Rx)	User-specified value
Set Tip and Ring Leads To *(FXO APM only)*	**Loop** – Tip and Ring are connected together. **Rgnd** – Ring lead is attached to ground. **Open** – Ring lead is not connected to either the Tip lead or the ground. **Lpgnd** – Tip and Ring are connected together, and Tip is connected to ground.
Set Tip and Ring Leads To *(FXS APM only)*	**RbTo** – A –48 VDC battery is applied to the Ring lead and the Tip lead is open. **RbTg** – A –48 VDC battery is applied to the Ring lead and the Tip lead is grounded. **TbRg** – A –48 VDC battery is applied to the Tip lead and the Ring lead is grounded. **Ring** – Ringing voltage applied between Tip and Ring.

Table 5-10. Force and Monitor Signaling (2 of 3)

To force these fields . . .	To these settings . . .
Set E-lead To *(E&M APM only)*	On Off
For ESF framing: ABCD bits (Tx and Rx) *For D4 framing:* AB bits (Tx and Rx)	Whatever value is currently set.
Tip and Ring Leads State *(FXO APM only)*	**ToRo** – Attached device has both Tip and Ring leads open. **TgRo** – Attached device has Tip lead grounded and Ring lead open. **TgR*** – Attached device has Tip lead grounded and Ring lead state is unknown. **ToR*** – Attached device has Tip lead open and Ring lead state is unknown. **RoT*** – Attached device has Ring lead open and Tip lead state is unknown. **RbTo** – A battery is applied to the Ring lead and the Tip lead is open. **RbTg** – A battery is applied to the Ring lead and the Tip lead is grounded. **TbRg** – A battery is applied to the Tip lead and the Ring lead is grounded. **Ring** – Ringing voltage applied between Tip and Ring.
Tip and Ring Leads State *(FXS APM only)*	**RbTo** – Ring Lead connected to nominal –48VDC battery and Tip lead open. **RbTg** – Ring Lead connected to nominal –48VDC battery and Tip lead grounded. **TbRg** – Tip Lead connected to nominal –48VDC battery and Ring lead grounded. **Ring** – Ringing voltage applied between Tip and Ring.
Tip and Ring Leads Control State *(FXO APM only)*	**Loop** – Tip and Ring are connected together. **Rgnd** – Ring lead is attached to ground. **Open** – Ring lead is not connected to either the Tip lead or the ground. **Lpgnd** – Tip and Ring are connected together, and Tip is connected to ground.

Table 5-10. Force and Monitor Signaling (3 of 3)

To force these fields . . .	To these settings . . .
E-lead State *(E&M APM only)*	On Off
M-lead State *(E&M APM only)*	On Off

OCU-DP Physical Port Tests

Each enabled port on an OCU-DP APM can be tested. These tests include:

- Nonlatching Loopback
- Latching Loopback
- OCU Loopback
- DS-0 Loopback
- Line Loopback
- Data Loopback

If the customer premises equipment (CPE) is running at 64K clear channel (CC), a Latching Loopback can be sent. If running at 56K and Switched 56, a Nonlatching Loopback is run. The procedure for running a Latching Loopback and a Nonlatching Loopback or other loopbacks is different.

Follow this procedure to start and stop a Nonlatching Loopback (LB) or other OCU-DP loopback. See Latching Loopback for that procedure.

▶ Procedure

To start and stop a Nonlatching Loopback or other OCU-DP loopback:

1. Follow this menu selection sequence:

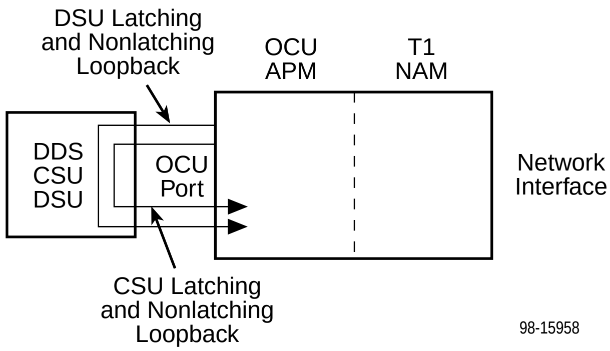
   Main Menu → Test → OCU-DP Tests

2. Select the APM slot number and port to be tested.
3. If running a Nonlatching, select the type of loopback:
   — For Local: CSU or DSU
   — For Remote: CSU, DSU, or OCU
4. To start the test, highlight **`Start`** in the Command column and press Enter. The Status changes to Active. The length of time that the test has been running is shown in the Results column.
5. To stop the test, highlight **`Stop`** under Command and press Enter. The Status changes to Inactive.

Nonlatching Loopback

A Nonlatching Loopback is a network-initiated test of the local loop between the selected port and the attached customer premises equipment (CPE) running at 56K or Switched 56.

Once a Nonlatching Loopback is started, the FrameSaver unit remains in loopback until it receives the loopback-release sequence from the network.



Latching Loopback

A Latching Loopback is a network-initiated loopback that allows the testing of a local loop between the selected port and the attached customer premises equipment (CPE) running at 64K clear channel (CC).

Once a Latching Loopback is started, the FrameSaver unit remains in loopback until it receives the loopback-release sequence from the network. The latching loopback code is a control sequence (as opposed to a bipolar violation sequence); therefore, user data may cause the FrameSaver unit to activate the loopback.

▶ Procedure

To send and stop a Latching Loopback:

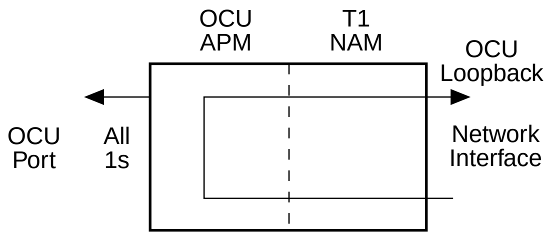
1. Follow this menu selection sequence:

   Main Menu → Test → OCU-DP Tests

2. Select the APM slot number and port to be tested.
3. In the Latching LB row, select the type of loopback:
   — For Local: CSU or DSU
   — For Remote: CSU, DSU, or OCU
4. Select the **Up** code to put the remote device in loopback.
5. To start the test, highlight **Send** in the Command column and press Enter. The code will be sent for up to 10 seconds, or until an acknowledgement is received. The length of time that the test has been running is shown in the Results column.
6. To stop the test, send the **Down** code to take the remote device out of loopback.

OCU Loopback

The OCU Loopback loops the data received from the T1 interface for the selected port back to the T1 interface.

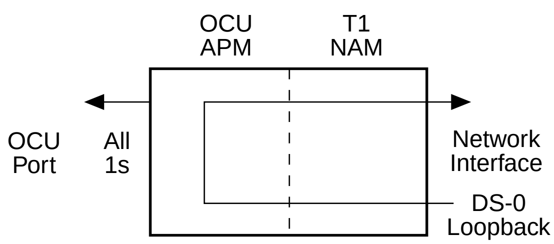


98-15959

A Line Loopback is the only test allowed to run at the same time as an OCU Loopback.

DS-0 Loopback

The DS-0 Loopback loops the data received from the T1 interface for the selected port back to the T1 interface.

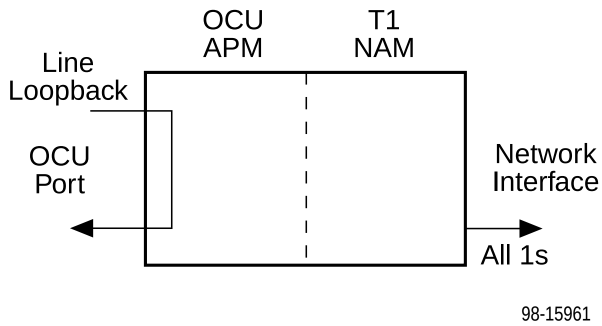


98-15960

A Line Loopback is the only test allowed to run at the same time as an DS-0 Loopback.

Line Loopback

The Line Loopback tests the local loop between the OCU port and the attached CPE. The loopback occurs on the APM near the local loop interface, toward the local loop.

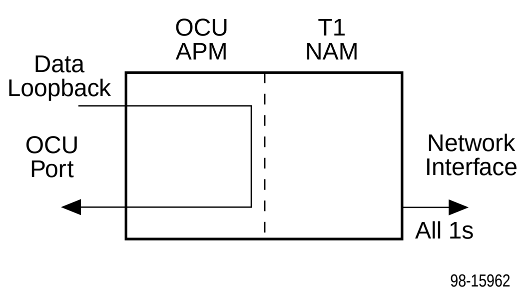


The following tests are the only tests allowed to run at the same time as a Line Loopback:

- OCU Loopback
- DS-0 Loopback
- Line Loopback on the cross-connected T1 interface
- Payload Loopback on the cross-connected T1 interface

Data Loopback

The Data Loopback tests the APM circuitry and the local loop connecting the port to the CPE. The loopback occurs on the APM near the backplane connection, toward the local loop.



The following tests are the only tests allowed to run at the same time as a Data Loopback:

- Line Loopback on the cross-connected T1 interface
- Payload Loopback on the cross-connected T1 interface

Security and Logins

6

This chapter includes the following:

When an ISDN DBM is installed, ISDN access can be controlled. See *Controlling ISDN Access* in Chapter 4, *Dial Backup Modules*, for additional information.

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

   NOTE:

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

3. Save your changes.

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 Telnet or FTP Access

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

Limiting Telnet Access

Telnet access can be limited by:

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

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

▶ Procedure

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

1. Select the Telnet and FTP Session options.

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

2. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Disable Telnet access	Telnet Session to Disable.
Require a login	Login Required to Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login*.
Assign an access level	Session Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the Telnet session (e.g., if a user has a Level-1 login and Level-2 telnet access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow users to configure the unit, keep the access at Level-1.

3. Save your changes.

See *Configuring Telnet and/or FTP Session Support* in Chapter 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 Management Link:

1. Select the Telnet and FTP Session options.

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

2. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Disable FTP	FTP Session to Disable.
Require a login	Login Required to Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login*. If you want to allow users to configure the unit or perform file transfers, including downloads, keep the access at Level-1. Level-1 access is required to download software to the unit, or to upload or download configuration files. Level-3 is sufficient for NMS access for SLV historical information.
Limit bandwidth for FTP	FTP Max Receive Rate (FrameSaver SLV 9126) or FTP Max Transfer Rate (FrameSaver SLV 9128) 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 Management Link

▶ Procedure

To limit Telnet or FTP access when the session is **on** the TS Management Link:

1. Select the Telnet and FTP Session options.

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

2. Disable Telnet Session and/or FTP Session, as appropriate.

3. Return to the Management and Communication menu, and select Node IP.

4. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Disable access via 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 *n* IP Address to the appropriate IP address.
Specify the access allowed for an authorized NMS when IP address validates is performed	Access Level to Read or Read/Write.

3. Save your changes.

See *Configuring SNMP NMS Security* in Chapter 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 8, *Troubleshooting*, should you be locked out inadvertently.

3. Save your changes.

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

See *Configuring SNMP NMS Security* in Chapter 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

7

This chapter includes the following information:

- *FTP File Transfers*
  - *Upgrading System Software*
  - *Determining Whether a Download is Completed*
  - *Changing Software*
  - *Transferring Collected Data*
- *Turning Off the System Alarm Relay*

If your system has an ISDN DBM and/or APM installed, see the following chapter(s) for additional information:

- For an ISDN DBM, see Chapter 4, *Dial Backup Modules*.
- For an APM, see Chapter 5, *Application Modules*.

Displaying System Information

Use the Identity screen to view identification information about the FrameSaver unit and its installed optional features.

Main Menu → Status → Identity

This information is useful if you are purchasing additional or replacement units and/or making firmware upgrades.

- When an ISDN DBM is installed, the DBM information is on the same screen as the system and NAM information.
- When an APM is installed in a 2-slot housing, the APM information is included on the same screen as the system, NAM, and DBM information.
- When an APM is installed in a 5-slot housing, a submenu appears and you can select one of the following:
  - **System & NAM** – Provides information about the system, the FrameSaver NAM/unit, and DBM, if installed.
  - **APM** – Provides information about the APM in each slot.

See *Viewing APM Information* in Chapter 5, *Application Modules*, for Identity information for APMs.

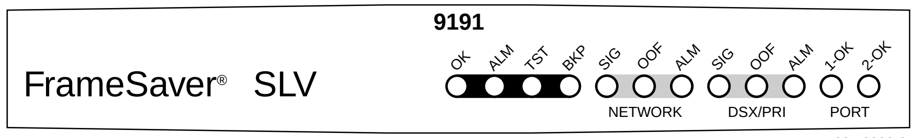
Viewing FrameSaver System Information

The following information is available when Identity is selected and no APM is installed, or System & NAM is selected from the Identity submenu when an APM is installed in a 5-slot housing. See *Viewing APM Information* in Chapter 5, *Application Modules*, for Identity information for APMs.

View this field . . .	To find the . . .
System	
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 (e.g., T1 FR NAM).
Serial Number	Unit's 7-character serial number.
Current Software Revision	Software version currently being used by the unit. Format *nn.nn.nn* consists of a 6-digit number that represents the major and minor revision levels.
Alternate Software Revision	Software version that has been downloaded into the unit, but has not yet been implemented. Format is the same as for the Current Software Revision. ■ **`In Progress`** indicates that the flash memory is currently being downloaded. ■ **`Invalid`** indicates that no download has occurred or the download was not successful
Hardware Revision	Unit's hardware version. Format *nnnn-nnx* consists of a 4-digit number, followed by two digits and one alphabetic character.
ISDN DBM	
DBM Type	The type of dial backup module installed, ISDN-BRI or ISDN-PRI, if applicable. ■ **`Unsupport`** indicates that the DBM is not supported by the FrameSaver unit. ■ **`Failed`** indicates that the DBM is not operational.
Software Revision	Software version currently being used by the system's DBM. Format *nn.nn.nn* 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 *nnnn-nnx* consists of a 4-digit number, followed by 2 digits and 1 alphabetic character.

Viewing LEDs and Control Leads

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



00-16339-01

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.

To access the Display LEDs and Control Leads screen:

Main Menu → Status → Display LEDs and Control Leads

FrameSaver Unit with an ISDN DBM and APM Example

```
main/status/leds                                                             9191
Device Name: Node A                                                5/27/2000 23:32

                          DISPLAY LEDS & Control Leads


              GENERAL     NETWORK 1    DSX-1    Port-1   Port-2
              OK          Sig          Sig      OK        OK
              Alarm       OOF          OOF      TXD       TXD
              Test        Alm          Alm      RXD       RXD
              Backup                            DTR       DTR
                                                CTS       CTS


              ISDN PRI      VOICE PORTS
              Sig           OK
              OOF
              Alm


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

When using this feature:

- Inverse video indicates that the LED is on.
- Normal video indicates that it is off.

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

LED Descriptions

Table 7-1 identifies the alarms that cause the Alarm LED to light. See Table 7-2 for network, DSX-1, or PRI interface LED and Table 7-3 for user data port interface LED information.

Table 7-1. 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 – System has just been reset, or an error or fault has been detected. Error/fault/alarm conditions: ■ Abnormal Station Code ■ Alarm Indication Signal (AIS) ■ APM Card Failed ■ CTS Down ■ DBM BRI Card Failure ■ DBM Download Failed ■ DLCI Down ■ DTR 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 Failure ■ Primary or Secondary Clock Failed ■ Self-Test Failed ■ 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 during power recycling, then goes off, the ISDN BRI DBM may have failed.

Table 7-1. General Status LEDs (2 of 2)

Label	Indication	Color	What It Means
ALM *(cont'd)*	Operational Alarm (Fail)	Red	ON – System has just been reset, or an error or fault has been detected. Error/fault/alarm conditions: ■ Network Communication Link Down ■ CTS Down ■ DTR Down ■ Primary or Secondary Clock Failed OFF – No failures have been detected.
TST	Test Mode	Yellow	ON – Loopback or test pattern in progress, initiated locally, remotely, or from the network. OFF – No tests are active.
BKP	Backup	Yellow	ON – System is in Backup mode; that is, the backup link has been established, and backup is in progress through the specified Alternate Destination Link. OFF – System is not in Backup mode. Blinking ON and OFF – Alternate Destination Link is being established, but no data has been passed.

Table 7-2. 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 7-3. User Data Port LEDs

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

If an APM is installed, see *Viewing APM LEDs* in Chapter 5, *Application Modules*.

Control Lead Descriptions

See Table 7-2, Network, DSX-1, or PRI Interface LEDs, for descriptions of these control leads. See Table 7-3, User Data Port LEDs, to interpret user data port OK control leads. 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 7-4.

Table 7-4. Additional User Data Port Control Leads

Label	Indication	What It Means
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.
CTS	Clear to Send	Shows the current state of the CTS 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 7-5. Device Messages (1 of 5)

Message	What It Indicates	What To Do
Access level is *n*, Read-only.	User's access level is 2 or 3; user is not authorized to change configurations.	No action 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.
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 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 *Changing Software*.

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

Message	What It Indicates	What To Do
File Transfer Failed – Invalid file *(Seen at an FTP terminal.)*	A file transfer was attempted, but it was not successful.	■ Try again, making sure you type the filename correctly. ■ Exit the FTP session, or download another file. See *Changing Software*.
Invalid Character (*x*)	A non-valid printable ASCII character has been entered.	Reenter information using valid characters.
Invalid date: must be mm/dd/yyyy	A non-valid date was entered on the System Information screen.	Reenter the date in the month/day/4-digit year format.
Invalid date and/or time	A non-valid date or time was entered on the System Information screen. The date does not exist (e.g., February 30th).	Reenter the date in the month/day/4-digit year format and/or time in the hour:minutes:seconds format.
Invalid time: must be hh:mm:ss	A non-valid system time was entered on the System Information screen.	Reenter the time in the hour:minutes:seconds format.
Invalid – Already Active	A test was already in progress when it was selected.	No action needed.
Invalid Password	Login is required and an incorrect password was entered; access is denied.	■ Try again. ■ Contact your system administrator to verify your password.
Invalid Test Combination	A conflicting loopback or pattern test was in progress when Start was selected to start another test, or was active on the same or another interface when Start was selected.	■ Wait until other test ends and message clears. ■ Cancel all tests from the Test screen (Path: main/test). ■ Stop the test from the same screen the test was started from.
Limit of ISDN Link Profiles Reached	New was selected from the ISDN Link Profiles screen, but the maximum number of link profiles have been reached.	■ Delete another link profile. ■ Set up the new link profile.
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.

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

Message	What It Indicates	What To Do
Limit of Mgmt PVCs reached	New was selected from the PVC Connection Table and the maximum number of management PVCs has already been created.	■ Do not create the management PVC. ■ Delete another management PVC, and try again.
Limit of PVC Connections reached	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 or ISDN link, which are suitable PVC Destinations.	Configure additional DLCIs for the network or ISDN link and try again.
No DLCIs available for connection	New was selected from the PVC Connection Table, but all configured DLCIs have been connected.	No action needed, or configure more DLCIs and try again.
No DLCIs available for connection	New was selected from the Management PVCs option screen, but all Link/DLCI pairs have been connected.	Configure more network and/or Port-1 Links/DLCIs pairs and try again.
No DLCIs Available for Mgmt PVC	New was selected from the Management PVCs option screen, but all configured DLCIs have been connected.	Configure more network and/or Port-1 DLCIs and try again.
No DLCIs Defined	DLCI Records was selected from an interface's Configuration Edit/Display menu, and no DLCI Records have been created for this interface.	Select New and create a DLCI record.
No more DLCIs allowed	New or CopyFrom was selected from an interface's DLCI Records configuration screen, and the maximum number of DLCI Records had already been reached.	Delete a DLCI, then create the new DLCI Record.

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

Message	What It Indicates	What To Do
No Primary Destination Link DLCIs Available	New or Modify was selected from the PVC Connection Table, but even though DLCIs are available to form a connection, no DLCIs are available on the network or ISDN link, which is a suitable Primary PVC Destination.	Configure additional DLCIs for the network or ISDN link and try again. If a network or ISDN DLCI has been entered as a Source DLCI: 1. Change the Source DLCI to a user data port DLCI. 2. Enter the network or ISDN 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.
Permission Denied *(Seen at an FTP terminal.)*	A file transfer was attempted, but the: ■ User did not have Level 1 security. ■ Wrong file was specified when the **put** command was entered. ■ User attempted to upload a program file from the unit.	■ See your system administrator to get your security level changed. ■ Try again, entering the correct file with the **put** command. ■ Enter the **put** command instead of a **get** command; you can only transfer files to the unit, not from it. See *Upgrading System Software*.
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Resetting Device, Please Wait ...	Yes (or y) was entered in the *Reset COM Port usage* field of the System Paused menu.	No action needed.

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

Message	What It Indicates	What To Do
Test Active	No higher priority health and status messages exist, and a test is running.	■ Contact service provider if test initiated by the network. ■ Wait until the test ends and message clears. ■ Cancel all tests from the Test screen (Path: main/test). ■ Stop the test from the same screen the test was started from.
User Interface Already in Use	Two Telnet sessions are already in use when an attempt to access the menu-driven user interface through the COM 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 unit with the ISDN DBM option and a voice APM installed.

Status Menu Example

```
main/status                                                                9191
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
                             Voice Status
                             Performance Statistics
                             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, and Voice Status will not appear if the unit does not have an FXS, FXO, or E&M analog voice APM installed.

- For an ISDN DBM, see *Checking the DBM Interface Status in* Chapter 4, *Dial Backup Modules*.
- For an APM, see *Checking Voice APM Status in* Chapter 5, *Application Modules*.

NOTE:

Status messages contained in the following sections are in alphabetical order.

System and Test Status Messages

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

Main Menu → Status → System and Test Status

The following information is included on this screen:

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

Self-Test Results Messages

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 7-6. Self-Test Results Message

Message	What It Indicates	What To Do
Failure *xxxxxxxx*	An internal failure occurred (*xxxxxxxx* represents an 8-digit hexadecimal failure code for use by service personnel).	1. Record the failure code. 2. Reset the unit. 3. Contact your service representative.
Passed	No problems were found during power-up or reset.	No action needed.

Health and Status Messages

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

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

Message	What It Indicates
Abnormal Station Code, Slot-*s*, Port-*p* *(OCU-DP APM only)*	An Abnormal Station Code is being received from the network DS0 for the identified OCU-DP interface. This indicates that the far-end unit is disconnected or powered-off.
AIS at DSX-1 *or* AIS at DSX-1, Slot-*s*, Port-*p*	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	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.
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.
APM Card Failed, Slot-*s* *(APM only)*	The FrameSaver unit detects an APM failure for the identified slot.
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.

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

Message	What It Indicates
Back-to-Back Mode is Active	The operating mode has been configured for back-to-back operation (*Main Menu → Control → Change Operating Mode)*. The FrameSaver unit can be connected to another FrameSaver unit without a frame relay switch between them. This feature is useful for product demonstrations or for a point-to-point configuration using a leased line.
Backup Active *(ISDN DBM only)*	Backup has been established and data is flowing over the alternate DLCI.
CTS down to Port-1 Device *or* CTS down to Slot-*s* Port-*p* Device	The Port-1 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.
DBM Download Required *(ISDN BRI DBM only)*	A download attempt was interrupted and failed to complete. The NAM software and DBM software are incompatible.
DDS Network Fail *bbbbbb* Slot-*s* Port-*p* *(OCU-DP APM only)*	The OCU-DP specified interface is receiving a DDS network code of *bbbbbb.* This 6-bit code represents bits 0–7 of the DS0 code as defined in AT&T PUB 62310.
Device Fail *yyyyyyyy*	An internal error has been detected by the operating software.
DLCI *nnnn* Down, *frame_relay_link* [1,2]	The DLCI for the specified frame relay link is down.
DTR down from Port-1 Device *or* DTR down from Slot-*s*, Port-*p* Device	The DTR control lead on the device connected to Slot *s* Port *p* is off.

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

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

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

– *Ss*Port-*p*. The frame relay link associated with data port-*p* in slot-*s*.

– *ISDN Link Name* on a non-network ISDN DBM interface.

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

Message	What It Indicates
EER at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	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.
Internal Modem Failed	The unit's internal modem failed to pass the self-test.
ISDN Active *(ISDN DBM only)*	An ISDN call is active.
ISDN Link Profile Disabled *ISDN Link Name* *(ISDN DBM only)*	An ISDN backup call could not be made because the ISDN link profile specified Link Name is disabled (*Main Menu → Configuration → ISDN → Link Profiles)*.
ISDN Link Profile Invalid, *ISDN Link Name* *(ISDN DBM only)*	The ISDN link profile specified (*ISDN Link Name*) is invalid.
ISDN Network Failed (Active/Idle) *(ISDN DBM only)*	An ISDN network failure was detected when: ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode.
Link Down Administratively, *frame_relay_link* [2]	The specified frame relay link has been disabled by the unit due to LMI Behavior conditions or LMI Protocol on another link is in a failed state.
Link Profile Disabled, *ISDN Link Name* *(ISDN DBM only)*	An ISDN backup call could not be made because the specified link profile was disabled.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– *Ss*Port-*p*. The frame relay link associated with data port-*p* in slot-*s*.
– *ISDN Link Name* on a non-network ISDN DBM interface.

Table 7-7. Health and Status Messages (4 of 6)

Message	What It Indicates
LMI Discovery in Progress, *frame_relay_link* [2]	Local Management Interface protocol discovery is in progress to determine which protocol will be used on the specified frame relay link.
LMI Down, *frame_relay_link* [2]	The Local Management Interface(s) has been declared down for the specified frame relay link.
LOS at 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.
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. 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.
LOS at OCU-DP, Slot-*s* Port-*p* *(OCU-DP APM only)*	A Loss of Signal (LOS) condition is detected on the specified OCU-DP interface. An LOS is declared when a signal has been absent on the local loop for more than two consecutive minutes.
Loss of Loop Timing, Slot-*s* Port-*p* *(OCU-DP APM only)*	The OCU-DP interface in Slot *s*, Port *p* cannot recover timing from the received signal on the local loop.
Module MisConfig, Slot-*s* *(APM only)*	The APM in slot *s* is not the one specified in the NAM's configuration table.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– *Ss*Port-*p*. The frame relay link associated with data port-*p* in slot-*s*.
– *ISDN Link Name* on a non-network ISDN DBM interface.

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

Message	What It Indicates
Module Unsupported, Slot-*s* *(APM only)*	The NAM does not recognize the APM in slot-*s*. Possible reasons include: ■ A newer APM was installed prior to downloading the NAM. ■ An APM was taken from a FrameSaver model other than the current model.
Network Com Link Down	The communication link for the COM port is down, and the COM port is configured for Net Link.
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.
OOF at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	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.
Power Supply Alarm *(5-slot housing only)*	The power supply output voltage has dropped below the specified tolerance level required for the system.
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.

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

Message	What It Indicates
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.
SLV Timeout, DLCI *nnnn*, *frame_relay_link* [1, 2, 3]	An excessive number of SLV communication responses from the remote FrameSaver SLV unit have been missed on the specified multiplexed DLCI; the DLCI is not suitable for user data. When a hardware bypass capable device has been detected at the other end of the PVC and this condition occurs, only user data for EDLCI 0 will be transmitted while this condition exists. 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.
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) *(ISDN PRI DBM only)*	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.
64KCC Loop OOF, Slot-*s* Port *p* *(OCU-DP APM only)*	An Out of Frame (OOF) condition has been detected for the identified OCU-DP interface.

[1] *nnnn* indicates a DLCI number of 16 through 1007.
[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– *Ss*Port-*p*. The frame relay link associated with data port-*p* in slot-*s*.
– *ISDN Link Name* on a non-network ISDN DBM interface.
[3] Does not apply to a TS Management Link DLCI.

Test Status Messages

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

Table 7-8. Test Status Messages (1 of 3)

Message	What It Indicates
DCLB Active, *frame_relay_link* [1]	A Data Channel Loopback (DCLB) is active on the T1 network frame relay link, or the specified port in slot-*s*.
DTE External LB Active, Slot-*s* Port-*p*	An external DTE Loopback is active on the specified port in slot-*s*.
DTE Init. Ext LB Active, Slot-*s* Port-*p*	DTE has initiated an external DTE Loopback on the specified port in slot-*s*.
DTPLB Active, Slot-*s* Port-*p*	A Data Terminal Payload Loopback (DTPLB) is active on the specified port in slot-*s.*
Lamp Test Active	The Lamp Test is active, causing the NAM and APM faceplate LEDs to flash on and off.
Latching CSU LB Active, Network 1 *or* Latching CSU LB Active, Slot-*s* Port-*p (OCU-DP APM only)*	A Latching CSU Loopback test is active on the specified OCU-DP interface in slot-*s.*
Latching DSU LB Active, Network 1 *or* Latching DSU LB Active, Slot-*s* Port-*p (OCU-DP APM only)*	A Latching DSU Loopback is active on the specified interface in slot-*s.*
Latching OCU LB Active, Slot-*s* Port-*p (OCU-DP APM only)*	A Latching OCU Loopback is active on the specified OCU-DP interface in slot-*s.*
LLB Active, Network 1 *or* LLB Active, DSX-1 *or* LLB Active, ISDN PRI *(ISDN PRI DBM only)*	A Line Loopback (LLB) is active on the specified interface.

[1] *frame relay link* is one of the following:
- Net1-FR1. The frame relay link specified for the network interface, Network 1.
- *Ss*Port-*p*. The frame relay link associated with data port-*p* in slot-*s*.
- *ISDN Link Name* on a non-network ISDN DBM interface.

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

Table 7-8. Test Status Messages (2 of 3)

Message	What It Indicates
Monitor Pttn. Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	A Monitor Pattern test (user-selected pattern) is active on the specified DLCI for the specified frame relay link.
Monitor *Pttn* Active, Network 1 *or* Monitor *Pttn* Active, DSX-1 *or* Monitor *Pttn* Active, Slot-*s* Port-*p* *(APM only) or* Monitor *Pttn* Active, ISDN *(ISDN DBM only)*	A Monitor Pattern test (user-selected pattern) is active on the specified interface, or the specified port in slot-*s*. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
Network Initiated ISDN BRI Test Active *(ISDN BRI DBM only)*	An ISDN test has been initiated by the ISDN BRI network and is currently active.
NonLatching CSU LB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A Nonlatching CSU Loopback is active on the specified OCU-DP interface in slot-*s.*
NonLatching DSU LB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A Nonlatching DSU Loopback is active on the specified OCU-DP interface in slot-*s.*
NonLatching OCU LB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A Nonlatching OCU Loopback is active on the specified OCU-DP interface in slot-*s.*
No Test Active	No tests are currently running.
OCU Data LB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	An OCU Data Loopback is active on the specified port in slot-*s.*
OCU DS-0 OCU LB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	An OCU Data Loopback is active on the specified OCU-DP interface in slot-*s.*
OCU LLB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	An OCU Line Loopback is active on the specified OCU-DP interface in slot-*s.*
PLB Active, Network 1 *or* PLB Active, DSX-1 *or* PLB Active, ISDN PRI *(ISDN PRI DBM only)*	A Payload Loopback (PLB) is active on the specified interface*.*

[1] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– *Ss*Port-*p*. The frame relay link associated with data port-*p* in slot-*s*.
– *ISDN Link Name* on a non-network ISDN DBM interface.

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

Table 7-8. Test Status Messages (3 of 3)

Message	What It Indicates
PVC Loopback Active, DLCI *nnnn*, *frame_relay_link* [1,2]	A PVC Loopback is active on the specified DLCI for the frame relay link.
RLB Active, DSX-1 *or* RLB Active, Network 1	A Repeater Loopback (RLB) is active on the specified interface.
Send Pattern Active, DLCI *nnnn*, *frame_relay_link* [1,2]	A Send Pattern test (user-selected pattern) is active on the specified DLCI for the specified frame relay link.
Send *Pttn* Active, Network 1 *or* Send *Pttn* Active, DSX-1 *or* Send *Pttn* Active, Slot-*s* Port-*p* *(OCU-DP APM only) or* Send *Pttn* Active, ISDN *(ISDN DBM only)*	A Send Pattern test (user-selected pattern) is active on the specified interface, or the specified port or interface in slot-*s*. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
Voice ALB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A voice Analog Loopback (ALB) is active on the specified OCU-DP interface in slot-*s.*
Voice DLB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A voice Digital Loopback (DLB) is active on the specified OCU-DP interface in slot-*s.*
Voice DRS Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A voice Digital Reference (DRS) test tone is active on the specified OCU-DP interface in slot-*s.*
Voice Forced Signal Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A voice forced signaling condition is active on the specified OCU-DP interface in slot-*s.*
Voice LLB Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A voice Line Loopback (LLB) is active on the specified OCU-DP interface in slot-*s.*
Voice Quiet Active, Slot-*s* Port-*p* *(OCU-DP APM only)*	A voice quiet test tone is active on the specified OCU-DP interface in slot-*s.*

[1] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– *Ss*Port-*p*. The frame relay link associated with data port-*p* in slot-*s*.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[2] *nnnn* 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                                                       9191
Device Name: Node A                                              5/26/2000 23:32

                     frame relay link LMI REPORTED DLCIs         Page 1 of 2



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

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

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

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

Table 7-9. 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		LMI-reported status of the DLCI:
	Active	■ Whether the DLCI is active (capable of carrying data) in the frame relay network,
	Inactive	■ Whether it is inactive in the frame relay network,
	Deleted [1]	■ Whether it has been deleted by the frame relay network, or
	New [1]	■ Whether it has been created by the frame relay network.
CIR (bps)	0–64000	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 for the FrameSaver unit shows an alternate destination for backup, as well as a primary destination.

PVC Connection Status Screen Example

```
main/status/connections                                                    9191
Device Name: Node A                                             5/26/2000 23:32

                                                                    Page 1 of 2
                           PVC CONNECTION STATUS

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

 Port-1  201          Net1-FR1   300    0      Active
 Port-1  202          Net1-FR1  1001    0      Active
 Port-1  100          Net1-FR1  1001    0      Active
 Port-1  204          Net1-FR1  1001    1      Active
 Mgmt PVC Mgm205      Net1-FR1  1001    2      Active
 Port-1  206          Net1-FR1  1001    3      Active
 Port-1  207          Net1-FR1  1001    4      Active
 Port-1  208          Net1-FR1   500    5      Active     HQ_Site  400       Inactive
 Port-1  209          Net1-FR1   502    0      Inactive   HQ_Site  302   0   Active
 Port-1  210          Net1-FR1   504    0      Inactive   HQ_Site  304   0   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. This is what is shown in the screen example above. It shows a remote site unit backing up to the central site (HQ_Site).

For units without ISDN backup capability, an alternate 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 7-10. PVC Connection Status

Field	Status	What It Indicates
Link		Identifies the cross-connection of DLCIs configured for the unit.
	Net1-FR1	■ Source/destination is frame relay link 1 on Network 1
	S*s*Port-*p*	■ Source/destination is the frame relay link on the specified port in slot-*s*
	Mgmt*PVCName*	■ User data port – Port-1 or Port-2 ■ Virtual circuit is a management link that terminates in the unit, where *Name* 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.
Status		Identifies whether the physical interfaces, LMIs, and DLCIs are all enabled and active for this PVC connection.
	Active [1]	■ The PVC is currently active.
	Inactive	■ The PVC is inactive because: – Alarm conditions and network and SLV communication status indicate that data cannot be successfully passed. – The unit has disabled the interface or frame relay link due to internal operating conventions. – Activation of an alternate virtual circuit is not warranted; that is, no alarm condition on the primary destination link has been detected.

[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 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                                               9191
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        Slot 2 - Sync Data APM    Slot 3 - FXS Voice APM
   Slot 4 - E&M Voice APM    Slot 5 - FXO Voice APM

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

This screen also provides information on the slot assignment for each APM type. The following designations can be displayed:

- **Empty** – The slot is empty.
- **Misconfig** – The slot contains a misconfigured APM.
- **Unsupported** – The slot contains an unrecognized APM.
- **Failed** – The slot contained an APM that was removed or is no longer operational.
- **Sync Data APM** – The slot contains a 4-port synchronous data APM.
- **E&M Voice APM** – The slot contains an 8-port E&M Analog Voice APM.
- **FXO Voice APM** – The slot contains an 8-port FXO Analog Voice APM.
- **FXS Voice APM** – The slot contains an 8-port FXS Analog Voice APM.
- **OCU (2) APM** – The slot contains a 2-port OCU-DP APM.
- **OCU (6) APM** – The slot contains a 6-port OCU-DP APM.

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.
Ss*Pp*	The voice, Sync Data Port, or OCU-DP APM port or interface in slot-*s* is assigned to the network interface time slot (01 to 24). **NOTE:** For a Sync Data Port APM, Port Use must be set to Synchronous Data.
D*s-p*/*tt*	The DSX-1 time slot *tt* is assigned to the network interface time slot (01 to 24).
D*s-p*/*tt*r	The DSX-1 time slot *tt* is assigned to the network interface time slot (01 to 24), using Robbed Bit Signaling (r).
RsvdSs	The time slot is currently assigned to an APM in slot-*s*, which is either: ■ Failed (APM Card Failed condition) ■ Removed or not installed ■ Replaced by an APM that is not compatible with the configuration.

See Chapter 5, *Application Modules*, for additional information about APMs.

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                                                9191
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       Slot 2 - Sync Data APM    Slot 3 - FXS Voice APM
   Slot 4 - E&M Voice APM   Slot 5 - FXO Voice APM

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

This screen also provides information on the slot assignment for each APM type. The following designations can be displayed:

- **Empty** – The slot is empty.
- **Misconfig** – The slot contains a misconfigured APM.
- **Unsupported** – The slot contains an unrecognized APM.
- **Failed** – The slot contained an APM that was removed or is no longer operational.
- **Sync Data APM** – The slot contains a 4-port synchronous data APM.
- **E&M Voice APM** – The slot contains an 8-port E&M Analog Voice APM.
- **FXO Voice APM** – The slot contains an 8-port FXO Analog Voice APM.
- **FXS Voice APM** – The slot contains an 8-port FXS Analog Voice APM.
- **OCU (2) APM** – The slot contains a 2-port OCU-DP APM.
- **OCU (6) APM** – The slot contains a 6-port OCU-DP APM.

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

The Cross Connect Status Field (bottom) . . .	Indicates the . . .
Unassgn	The time slot is unassigned.
SsP*p*	The voice, Sync Data Port, or OCU-DP APM port or interface in slot-*s* is assigned to the DSX-1 interface time slot (01 to 24). **NOTE:** For a Sync Data Port APM, Port Use must be set to Synchronous Data.
Net1/*tt*	Network interface 1, time slot *(tt)* is assigned to DSX-1 time slot (01 to 24) using Clear Channel.
Net1/*tt*r	Network interface 1, time slot *(tt)* is assigned to DSX-1 time slot (01 to 24) using Robbed Bit Signaling (r).
RsvdSs	The time slot is currently assigned to an APM in slot-*s*, which is either: ■ Failed (APM Card Failed condition) ■ Removed or not installed ■ Replaced by an APM that is not compatible with the configuration.

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                                                      9191
Device Name: Node A                                                5/26/2000 23:32

                             PERFORMANCE STATISTICS


                             Service Level Verification
                             DLCI
                             Frame Relay
                             ESF Line
                             DDS Line
                             DBM Call
                             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 an ISDN DBM installed. See *Viewing DBM Call Performance Statistics in* Chapter 4, *Dial Backup Modules*.

DDS Line statistics only appear when an OCU-DP APM is installed. See *Viewing DDS Line Performance Statistics in* Chapter 5, *Application Modules*.

When you want to observe and estimate the frequency or duration of a specific condition (e.g., gathering information for reporting a problem to the network), determine whether a statistic is incrementing.

▶ **Procedure**

To determine whether a statistic is incrementing:

1. Record the accumulated value for the statistic of interest (the beginning value).
2. Press **r** for Refresh to see if it changes.
3. If the statistic is incrementing, record the ending value and the amount of time between the beginning and ending values.

   Continue to Refresh the screen until you have a sense of how serious the problem might be.

Clearing Performance Statistics

If you have a Level-1 security access level, performance statistics counters can be reset to the baseline when using a directly-connected asynchronous terminal. This feature is useful when troubleshooting problems.

Statistic counters are not actually cleared using this feature. True statistic counts are always maintained so SLAs can be verified, and they can be viewed from an SNMP NMS. However, since statistics can be cleared locally, the statistics viewed via the menu-driven user interface may be different from those viewed from the NMS.

▶ **Procedure**

To clear all statistics:

Performance Statistics → Clear All Statistics

▶ **Procedure**

To clear specific sets of statistics:

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

  Performance Statistics → Service Level Verification
  Performance Statistics → DLCI

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

  Performance Statistics → Frame Relay

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

  Performance Statistics → ESF Line

- Use the ClrDDsStats function key to reset the OCU-DP APM's DDS line performance statistics.

  Performance Statistics →DDS Line

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

  Performance Statistics →DBM Call

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 7-11. Service Level Verification Performance Statistics (1 of 2)

Statistic	What It Indicates
Far End DLCI	Number of the multiplexed DLCI or VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) at the other end of the connection. If the far-end circuit is a DLCI, the DLCI number (16–1007) appears. If a VPI/VCI, the number is displayed as *xx,yyy,* xx being the VPI number (0–15) and *yyy* being the VCI number (32–2047). **None** appears if the unit has not communicated with the other end.
Far End IP Addr	IP Address of the device at the other end of the multiplexed DLCI connection. **None** appears if the FrameSaver unit has not communicated with the other end, or if the device at the other end of the multiplexed DLCI does not have an IP Address configured.
Inbound Dropped Frames [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 3-3, Service Level Verification Options) must be enabled for these statistics to appear.

[1] Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.

Table 7-11. 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 3-3, Service Level Verification Options) must be enabled for these statistics to appear. **NA** appears instead of a statistical count if FDR/DDR (Frame Delivery Ratio/Data Delivery Ratio) information is not being received from the far-end device .
Dropped SLV Responses	The number of SLV inband sample messages sent for which a response from the far-end device has not been received.
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 3-3, Service Level Verification Options) over the previous 15-minute period. If SLV Packet Size is changed, a new average is not available until a new sample has been received. **Unknown** appears if communication with the far-end device over the last 15 minutes has not been successful.
Max RdTrip Latency	Same as average (Avg RdTrip Latency), but storing the maximum value of latency over the previous 15-minute interval. **Unknown** appears if communication with the far-end device over the last 15 minutes has not been successful.

[1] Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.

DLCI Performance Statistics

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

Main Menu → Status → Performance Statistics → DLCI

Table 7-12. 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 system 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 system discovered that the DLCI was active in the network.
Tx/Rx Characters	Number of data octets (8-bit bytes) sent/received for the selected DLCI on the interface.
Tx/Rx Frames	Number of frames sent/received for the DLCI on the interface.
Tx/Rx Frames Within CIR	Number of frames sent/received for the DLCI on the interface that are within the committed information rate that had been configured.
Tx/Rx Frames Exceed CIR	Number of frames sent/received for the DLCI on the interface that exceed the committed information rate that had been configured.
Tx/Rx Frames With DE	Number of frames sent/received for the DLCI on the interface that have the discard eligible bit set.

[1] Only appears for the network interface.

Table 7-12. DLCI Performance Statistics (2 of 2)

Statistic	What It Indicates
Tx BECN Frames	Number of Backward Explicit Congestion Notifications (BECNs) sent over the interface. BECNs are sent to notify users of data traffic congestion in the opposite direction of the frame carrying the BECN indicator.
Rx BECN Frames	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.
Rx FECN Frames	Number of Forward Explicit Congestion Notifications (FECNs) received for the selected DLCI on the interface. The network sends FECNs to notify users of data traffic congestion in the same direction of the frame carrying the FECN indicator.

Frame Relay Performance Statistics

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

Main Menu → Status → Performance Statistics → Frame Relay

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

Table 7-13. 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 7-13. 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 7-13. 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 7-13. 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.

ESF Line Performance Statistics Screen Example

```
          main/status/performance/esf                                           9191
          Device Name: Node A                                        5/26/2000 23:32
                               Network 1 ESF LINE PERFORMANCE STATISTICS
          Current Interval Timer                                     ESF Error Events
          Near=123    Far = 124                                   Near = 15   Far = 12

                                  ---ES--   --UAS--   --SES--   --BES--   --CSS--   -LOFC--
                        Time     Near Far  Near Far  Near Far  Near Far  Near Far  Near Far
            Current: 10:37        0   0     0   0     0   0     0   0     0   0     0   0
Line 10      Int 01: 10:35        0   0     0   0     0   0     0   0     0   0     0   0
             Int 02: 10:20        0   0     0   0     0   0     0   0     0   0     0   0
             Int 03: 10:05        0   0     0   0     0   0     0   0     0   0     0   0
Line 13      Int 04: 09:50        0   0     0   0     0   0     0   0     0   0     0   0
             Int 05: 09:35        0   0     0   0     0   0     0   0     0   0     0   0
             Int 06: 09:20        0   0     0   0     0   0     0   0     0   0     0   0
Line 16      Int 07: 09:05        0   0     0   0     0   0     0   0     0   0     0   0

Line 18      Worst Interval:     24  24    14  14    14  14    09  09    18  16    44  44
          Near  Tot(valid 96):  00010     00000     00000     00000       002       003
          Far   Tot(valid 96):  00010     00000     00000     00000       002       003
          --------------------------------------------------------------------------------
          Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
           Refresh   PgDn   PgUp   ClrFarStats   ClrNearStats
          Select: 01, 02, 03, 04, 05, 06, 07, 08, 09 ...
```

For the ESF line performance statistics, the following performance statistics are kept for each 15-minute interval over the past 24-hour period. A Near set and a Far set are kept for each statistic. The Far set is based on information kept by the unit at the other end of the local loop and is only available when ANSI performance report messages are enabled in the unit.

Summary information that appears near the top of the screen includes:

- **Near/Far Current Interval Timer** – Contains the number of seconds that have elapsed in the current 15-minute interval for the near or far information, which can show a value up to 900 seconds.

- **Near/Far ESF Error Events** – Maintains a count of ESF error events, as specified by AT&T TR 54016, which counts CRC and OOF events. A maximum of 65,535 error events can be counted. Once 65535 is reached, it stays at that number until the network issues a reset command.

The following performance statistics are collected for ESF line conditions.

Table 7-14. 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.

Modem Operation

This section includes the following:

- *Manually Disconnecting the Modem*
- *Verifying Modem Operation*

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

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*).

FTP File Transfers

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

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

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

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

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 6, *Security and Logins*), you are prompted to enter them. If not, press Enter.

   The FTP prompt appears.

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

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

Upgrading System Software

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

NOTE:

Upgrades can be performed through the network using a Management PVC, or through the COM port if Port Use is set to Net Link (see Table 9-15, Communication Port Options).

▶ Procedure

To download software:

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

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

NOTE:

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

⚠ WARNING:

A *put* to current.cfg will replace all currently-configured configuration options, including the node's IP Address. Always put configuration files to a customer configuration area so it can be modified before the file is loaded into the current configuration.

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

Determining Whether a Download Is Completed

To see whether a download has completed, check the Identity screen (selected from the Status menu). 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 Select Software Release screen shows the currently loaded software version and the new release that was just transferred.

   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. The **`Are you sure?`** prompt appears.

3. Enter Yes. 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 (identification) 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 in 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 Receive Rate (Kbps) option (see Table 3-15, Telnet and FTP Session Options in Chapter 3, *Configuration*).

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.

NOTE:

Use your NMS application to FTP and view statistics and packet data. Data files are not in user-readable format.

▶ Procedure

To retrieve data:

1. Perform Steps 1 through 3 in *Upgrading System Software* on page 7-49 to initiate and set up an FTP session.
1. Initiate an FTP session to the device from which SLV statistics will be retrieved.
2. Type **cd data** to change to the data directory.

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

3. Close the FTP session.

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

Turning Off the System Alarm Relay

For FrameSaver units mounted in a 5-slot housing, an alarm system relay is provided. This relay activates a light or buzzer when an alarm condition is detected in the FrameSaver unit.

Once the alarm relay is connected, enabling the System Alarm Relay option activates this feature (see Table 3-4, 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 *5-Slot Housing Installation Instructions* for information about connecting the alarm relay.

Troubleshooting

8

This chapter includes the following:

If your system has an ISDN DBM and/or APM installed, see the following chapter(s) for additional information:

- For an ISDN DBM, see Chapter 4, *Dial Backup Modules*.
- For an APM, see Chapter 5, *Application Modules*.

Problem Indicators

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

Indicators . . .	**See . . .**
LEDs	*Viewing LEDs and Control Leads* and *LED Descriptions* in Chapter 7, *Operation and Maintenance*, as well as the user interface screen. *Main Menu → Status → Display LEDs and Control LEDs*
Health and Status	Table 7-7, Health and Status Messages in Chapter 7, *Operation and Maintenance*. *Main Menu → Status → System and Test Status* Messages also appear at the bottom of any menu-driven user interface screen.
Performance statistics	*Performance Statistics* in Chapter 7, *Operation and Maintenance*, to help you determine how long a problem has existed.
Alarm conditions that will generate an SNMP trap	*Alarms* on page 8-7.
SNMP traps	Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults.* Traps supported include warm-start, authentication-failure, enterprise-specific (those specific to the unit), link-up, and link-down.
Alarm system relay for units installed in a 5-slot housing	*Configuring General System Options* in Chapter 3, *Configuration*, to enable this feature. *Main Menu → Configuration → System → General*

Resetting the Unit and Restoring Communication

You can reset the access 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 access unit performs a self-test when it is reset.

Resetting the Unit from the Control Menu

Use this procedure to initiate a power-on self-test of the access unit, recycling power.

▶ **Procedure**

To reset the access 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 access unit.

Restoring Communication with a Misconfigured Unit

Misconfiguring the access 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 access unit, then hold the Enter key down until the System Paused screen appears. (See *Resetting the Unit and Restoring Communication* on page 8-4 for other methods of resetting the unit.)

3. Tab to the desired prompt, and type **y** (Yes) at one of the prompts.

If selecting . . .	The following occurs . . .
Reset COM Port usage	■ Port Use is set to Terminal so the asynchronous terminal can be used. ■ Data Rate (Kbps), Character Length, Stop Bits, and Parity are reset to the factory defaults. ■ Access unit resets itself.
Reload Factory Defaults	■ All configuration and control settings are reset to the Default Factory Configuration, overwriting the current configuration. ■ Access 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 access unit resets itself and no configuration changes are made.

Once the access 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.syc in the system's data directory so the data can be uploaded and transferred to a Network Associates Sniffer for analysis.

▶ Procedure

To use this utility:

1. Select the LMI Packet Capture Utility.

   Main Menu → Control → LMI Packet Capture Utility

2. Select an enabled frame relay link, or Capture Interface, either Net1-FR1 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 7, *Operation and Maintenance*, for additional information about this feature.

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 (see Table 8-1). These alarm conditions also generate Health and Status messages seen on the System and Test Status screen.

Main Menu → Status → System and Test Status

If your system has an ISDN DBM and/or APM installed, see the following chapter(s) for additional information:

- For an ISDN DBM, see Chapter 4, *Dial Backup Modules*.
- For an APM, see Chapter 5, *Application Modules*.

Table 8-1. Alarm Conditions (1 of 9)

Alarm Condition	What It Indicates	What To Do
Abnormal Station Code *(OCU-DP APM only)*	An Abnormal Station Code is being received from the network DS0 for the identified OCU-DP interface. This indicates that the far-end unit is disconnected or powered-off.	■ Check the APM's slot location and the affected port. ■ Check the cable to the far-end device. ■ Check that the far-end device is operational.
AIS at DSX-1	For the DSX-1 interface, the attached DTE is transmitting an AIS.	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.	Report the problem to your T1 service provider.
AIS at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	For the ISDN PRI DBM interface, the ISDN network is transmitting an AIS.	Report the problem to your ISDN service provider.
APM Card Failed *(APM only)*	The NAM detects an APM card failure for the identified slot, or the APM card was removed.	■ Check whether the APM was removed from the slot. ■ Remove the APM, then reinstall it. ■ Contact your service representative.

Table 8-1. Alarm Conditions (2 of 9)

Alarm Condition	What It Indicates	What To Do
CTS down to Slot-*s* Port-*n* Device	The CTS control lead on the device's interface is off.	Check DTR and RTS from the port in the specified slot. ■ Verify that the port is enabled. ■ Check DTR from the user data port. ■ Verify that the port is enabled. ■ Check DTR from the user data port.
DBM BRI Card Failed *(ISDN BRI DBM only)*	One or more of the unit's integrated circuit chips has failed to internally loop data through the ISDN BRI DBM's BRI circuit.	■ Reset the unit and try again. ■ Call your service representative for assistance. ■ Return the unit to the factory (see Page A at the front of this guide).
DBM Download Required *(ISDN DBM only)*	A download attempt was interrupted and failed to complete, or the NAM software and DBM software are incompatible.	Call your service representative.
DDS Network Failure *yyyyyy,* Slot-*s* Port-*n* *(OCU-DP APM only)*	The identified OCU-DP interface is receiving DDS network code *yyyyyy* from the network. This is a 6-bit code representing bits 2–7 of the DS0 code defined in AT&T PUB 62310. The least significant bit is to the left.	■ Provide the displayed 6-digit failure code to your service representative. ■ Reset the FrameSaver unit to clear the condition. *Main Menu → Control → Reset Device*
Device Fail *yyyyyyyy*	An internal error has been detected by the operating software.	■ Provide the 8-digit failure code (*yyyyyyyy*) that follows the alarm to your service representative. ■ Reset the NextEDGE unit to clear the condition. ■ Clear the Device Fail message. *Main Menu → Control → Clear Device Fail*

Table 8-1. Alarm Conditions (3 of 9)

Alarm Condition	What It Indicates	What To Do
DLCI *nnnn* Down, *frame_relay_link* [1,2]	The DLCI for the specified frame relay link is down.	Verify that the network LMI is up. If it is, contact your network provider, or your ISDN service provider if an ISDN Link Name is the link.
DTR Down from Slot-*s* Port-*n* Device	The DTR control lead on the device connected to the specified port is off. This message applies to data ports that act as DCEs.	Examine the attached DTE and cable connected to the port in the specified slot. ■ Check that the port cable is securely attached at both ends. ■ Check the status of the attached equipment.
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.
EER at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	For an ISDN PRI DBM interface, Active indicates that a backup call was in progress when the ISDN network failure was detected, and Idle indicates that the call was in idle mode when it was detected. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.	■ Verify that the cable is securely attached at the DBM interface. ■ Contact your ISDN network provider.
Internal Modem Failed	The unit's internal modem failed to pass the self-test.	Reset the FrameSaver unit (*Main Menu → Control → Reset Device)*. If the modem fails again, contact your service representative.

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

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

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

– *Ss*Port-*n*. The frame relay link associated with data port-*n* in slot-*s*.

– *ISDN Link Name* on a non-network ISDN DBM interface.

Table 8-1. Alarm Conditions (4 of 9)

Alarm Condition	What It Indicates	What To Do
ISDN Link Profile Disabled *ISDN Link Name* *(ISDN DBM only)*	An ISDN backup call could not be made because the ISDN link profile specified Link Name is disabled (*Main Menu → Configuration → ISDN → Link Profiles)*.	Enable the ISDN link profile if you want to make a call.
ISDN Link Profile Invalid, *ISDN Link Name* *(ISDN DBM only)*	An ISDN backup call could not be made because the ISDN link profile specified (*ISDN Link Name*) is invalid.	Check that the phone number is correct.
ISDN Network Failed (Active/ Idle) *(ISDN DBM only)*	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.
Link Down Administratively, *frame relay link* [2]	The specified frame relay link has been disabled by the unit due to LMI Behavior conditions or LMI Protocol on another link is in a failed state. This is not an alarm condition so **`System Operational`** appears, as well.	Verify that the network LMI is up. If it is, contact your network provider.
LMI Down, *frame relay link* [2]	The Local Management Interface is down for the specified frame relay link.	For the network interface: ■ If LMI was never up, verify that the LMI Protocol setting reflects the LMI type being used. ■ If LMI was never up: – Verify that the proper time slots have been configured. – Verify that the LMI Protocol setting reflects the LMI type being used. ■ Verify that Frame Relay Performance Statistics show LMI frames being transmitted. If all of the above have been verified and the physical link is not in Alarm, contact your network provider.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– *Ss*Port-*n*. The frame relay link associated with data port-*n* in slot-*s*.
– *ISDN Link Name* on a non-network ISDN DBM interface.

Table 8-1. Alarm Conditions (5 of 9)

Alarm Condition	What It Indicates	What To Do
LMI Down, *frame relay link* [2]	The Local Management Interface is down for the specified frame relay link.	For a user data port: ■ Check that the DTE cable is securely attached at both ends. ■ Verify that Transmit Clock Source and Invert Transmit Clock options are properly configured. ■ Verify that Frame Relay Performance Statistics show LMI frames being received. If no frames are being received: – Check the attached device. – Verify that the LMI Protocol setting reflects the LMI type being used.
LOS at 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.	■ Check that the DSX-1 cable is securely attached at both ends.
	■ No signal being transmitted from the DTE.	■ 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.	■ Check that the network cable is securely attached at both ends.
	■ No signal is being transmitted at the far-end FrameSaver unit.	■ Check far-end FrameSaver unit status.
	■ T1 facility problem.	■ Contact your network provider.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– *Ss*Port-*n*. The frame relay link associated with data port-*n* in slot-*s*.
– *ISDN Link Name* on a non-network ISDN DBM interface.

Table 8-1. Alarm Conditions (6 of 9)

Alarm Condition	What It Indicates	What To Do
LOS at ISDN PRI (Active/ Idle) *(ISDN PRI DBM only)*	Active indicates that a backup call was in progress when the ISDN network failure was detected, and Idle indicates that the call was in idle mode when it was detected. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. ■ Cabling problem. ■ Incompatiblity between the ISDN network and the unit. ■ An ISDN network problem.	■ Check that the ISDN PRI cable is securely attached at both ends. ■ Verify that the attached device is operational. ■ Contact your ISDN service provider.
LOS at OCU-DP, Slot-*s* Port-*n* *(OCU-DP APM only)*	An LOS is declared when a signal has been absent on the local loop for more than two consecutive minutes.	■ Check that the cable for the specified port is securely attached at both ends. ■ Verify that the DCE is powered on.
Loss of Loop Timing, Slot-*s* Port *n* *(OCU-DP APM only)*	The identified OCU-DP interface cannot recover timing from the received signal on the local loop. This typically occurs when the CPE CSU/DSU is misconfigured for the wrong rate (e.g., 19.2 kbps) when the OCU-DP is configured for 56K or Switched 56 operation.	Check that the CPE CSU/DSU rate matches the OCU-DP rate.
Module MisConfig, Slot-*s* *(APM only)*	The APM connected to the NAM is not configured as defined in the NAM's configuration table.	■ Replace the APM with the type of APM specified by the configuration table. ■ Change the current configuration to reflect the type of APM in the slot. To do this, edit the configuration, accept the APM, then save the configuration.
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.

Table 8-1. Alarm Conditions (7 of 9)

Alarm Condition	What It Indicates	What To Do
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.	■ Check that the framing format for the DSX-1 (DTE) interface is correct.
	■ DSX-1 cabling problem.	■ Check that the DSX-1 cable is securely attached at both ends.
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.	■ Check that the framing format for the network interface is correct.
	■ Network cabling problem.	■ Check that the network cable is securely attached at both ends.
	■ T1 facility problem.	■ Contact your network provider.
OOF at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	Active indicates that a backup call was in progress when the ISDN network failure was detected, and Idle indicates that the call was in idle mode when it was detected.	
	■ Cabling problem.	■ Check that the ISDN PRI cable is securely attached at both ends.
	■ Incompatiblity between the ISDN network and the unit.	■ Verify that the attached device is operational.
	■ An ISDN network problem.	■ Contact your ISDN service provider.
Power Supply Alarm *(5-slot housing only)*	Output voltage for the 5-slot housing has dropped below the system's tolerance level.	■ Check that the power cord is securely attached at both ends. ■ Check that the power outlet has power by plugging in equipment that that you know is operational, then check the circuit breaker. ■ Replace the power supply.

Table 8-1. Alarm Conditions (8 of 9)

Alarm Condition	What It Indicates	What To Do
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.	
SLV Timeout, DLCI *nnnn*, *frame relay link* [1, 2]	An excessive number of SLV communication responses from the remote system have been missed on the specified multiplexed DLCI and link. If the frame relay link is Net1-FR1, the timeout is on the network FrameRly1 timeslot assignment. When a hardware bypass-capable device has been detected at the other end of the PVC and this condition occurs, only user data for EDLCI 0 will be transmitted as long as the condition exists.	■ Verify that the network LMI is up. If it is, contact your network service provider. ■ If a DBM is present and Auto Backup is enabled, backup is initiated automatically.
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.

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

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

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

– *Ss*Port-*n*. The frame relay link associated with data port-*n* in slot-*s*.

– *ISDN Link Name* on a non-network ISDN DBM interface.

Table 8-1. Alarm Conditions (9 of 9)

Alarm Condition	What It Indicates	What To Do
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.
Yellow Alarm at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	A yellow alarm signal is received on the DBM interface. Active indicates that a backup call was in progress when the ISDN network failure was detected, and Idle indicates that the call was in idle mode when it was detected.	Report the problem to your ISDN service provider.
64KCC Loop OOF, Slot-*s* Port-*n* *(OCU-DP APM only)*	An Out of Frame (OOF) condition has been detected on the specified OCU-DP interface.	■ Check that the cable is securely attached at both ends. ■ Check that the framing format for the interface is correct. ■ Contact your network provider.

Troubleshooting Tables

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

Device Problems

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

Symptom	Possible Cause	Solutions
No power, or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle to rear panel connection.	Check that the power cord is securely attached at both ends.
	The wall receptacle has no power.	■ Check the wall receptacle power by plugging in some equipment that is known to be working. ■ Check the circuit breaker. ■ Verify that your site is not on an energy management program.
Power-Up Self-Test fails. Only Alarm LED is on after power-up.	The access unit has detected an internal hardware failure.	■ Reset the unit and try again. ■ Contact your service representative. ■ Return the unit to the factory (refer to *Warranty, Sales, Service, and Training Information* on page A of this document).
Cannot access the 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 *Restoring Communication with a Misconfigured Unit* on page 8-5). ■ Contact your service representative.
Device Fail appears on the System and Test Status screen under Self-Test results.	The unit detects an internal hardware failure.	■ Record the 8-digit code from the System and Test Status screen. ■ Reset the unit and try again. ■ Contact your service representative.

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

Symptom	Possible Cause	Solutions
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. DDS network is down. T1 network is down.	■ Reconnect or repair the cable. ■ Call the network service provider.
Receiving data errors on a multiplexed DLCI, but frame relay is okay.	FR Discovery is being used for automatic DLCI and PVC configuration	Change the DLCI Type for each network DLCI from Multiplexed to Standard, turning off multiplexing. The equipment at the other end is not frame relay RFC 1490-compliant or the unit at one end of the PVC does not support the Data Delivery Ratio feature.

Frame Relay PVC Problems

Table 8-3. Frame Relay PVC Problems

Symptom	Possible Cause	Solutions
No receipt or transmission of data.	Cross Connection of the DLCIs are configured incorrectly.	Verify the PVC connections, DLCIs, and CIRs agree with those of the service provider by checking the network-discovered DLCIs.
	DLCI is inactive on the frame relay network.	■ Verify that the DLCI(s) is active on the PVC Connection Status screen. If the DLCI(s) is not active, contact the service provider. ■ Verify the LMI Reported DLCI field on the Interface Status screen.
	DTE is configured incorrectly.	Check the DTE's configuration.
	LMI is not configured properly for the DTE, network, or ISDN link.	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. 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. ■ Check the line's error rate – the physical line quality. Contact the service provider.

Tests Available

The following tests are available to a FrameSaver unit and its optional features.

Test Menu Example

```
main/test                                                              9191
Device Name: Node A                                         5/26/2000 23:32

                                    TEST

                             Network PVC Tests
                             Data Port PVC Tests
                             ISDN PVC Tests

                             Network Physical Tests
                             Data Port Physical Tests
                             DSX-1 Physical Tests
                             PRI Physical Tests
                             Voice Port Physical Tests
                             OCU-DP Physical Tests

                             IP Ping
                             Lamp Test

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

ISDN PVC Tests only appears when the optional ISDN DBM feature is installed, and PRI Physical Tests only appears when the DBM is a ISDN PRI DBM.

Voice Port Physical Tests only appears when an optional FXS, FXO, or E&M analog voice APM is installed, and OCU-DP Physical Tests only appears when an OCU-DP APM is installed.

When a Sync Data APM is installed, all the tests available to a user data port are available to synchronous data ports on the APM.

For additional test information:

- For an ISDN DBM, see *ISDN Tests* in Chapter 4, *Dial Backup Modules*.
- For APMs, see *APM Tests* in Chapter 5, *Application Modules*.

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 system is remotely managed through an inband data stream (PVC). If a test is accidently commanded to execute on the interface providing management access, control is regained when the specified time period expires, automatically terminating the test.

To use this feature, enable the Test Timeout configuration option, and set a duration for the test to run in the Test Duration (min) configuration option (see *Configuring General System Options* in Chapter 3, *Configuration Options*).

NOTE:

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

Starting and Stopping a Test

Use the following procedures 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

To abort an individual test, see the appropriate procedure:

- *Starting and Stopping a PVC or Local Loopback or a Pattern Test*
- *Starting and Stopping a Remote Loopback*
- *Sending and Monitoring a User-Selected Pattern Test*

Starting and Stopping a PVC or Local Loopback or a Pattern Test

Use this procedure to run a PVC Loopback, local loopback, or to send and monitor a pattern test on a frame relay link.

▶ Procedure

To start and stop a PVC or local loopback or a pattern test:

1. Follow this menu selection sequence:

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

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

2. Select the DLCI number to be tested. The cursor is positioned at Start in the Command column of the first available test and is highlighted.

3. Move the cursor to the desired test.

4. To start the test, highlight the **`Start`** command for the desired test 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. For the pattern test, sequence and data error counts are also shown.

5. To stop the test, press Enter to send the **`Stop`** command. Start reappears and the status of the test changes back to Inactive.

Starting and Stopping a Remote Loopback

Use this procedure to run a remote loopback on a physical connection.

▶ Procedure

To start and stop a remote loopback:

1. Follow this menu selection sequence:

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

2. If running a remote loopback on a synchronous data port, enter the slot and port number.

3. Move the cursor to the desired remote loopback.

4. Select the **`Up`** code to put the remote device in loopback.

5. To start the test, highlight the **Send** command and press Enter. The code is sent for 10 seconds, or until an acknowledgement is received.

   The length of time that the test has been running is shown in the Result column.

6. To stop the test, send the **`Down`** code to take the remote device out of loopback.

Sending and Monitoring a User-Selected Pattern Test

Use this procedure to send or monitor a user-defined test pattern on a physical interface or port.

▶ Procedure

To send and monitor a a user-defined pattern test:

1. Follow this menu selection sequence:

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

2. If running a pattern test on a synchronous data port, enter the desired slot and port number.

3. Move the cursor to the Send or Pattern row and select a test pattern.

   To monitor the test, move the cursor to the Monitor row and select the same test pattern.

4. Enter the the desired 2-byte hexadecimal value in the field next to the selected pattern.

5. To send or monitor the selected pattern, 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 sending a pattern, the Inject Err function key appears at the bottom of the screen. Use Inject Err if you want to inject a bit error in the transmitted bit pattern.

   — When monitoring a pattern, the ResetMon function key appears. Use ResetMon to reset the error count to zero.

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. Abort All Tests does not interrupt DTE-initiated loopbacks.

▶ Procedure

To abort all tests on all interfaces:

1. Follow this menu selection sequence:

   Main Menu → Test

2. Select Abort All Tests.

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

PVC Tests

PVC tests can be run on a requested DLCI for a selected interface.

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

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

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

PVC Tests Screen Example

```
main/test/network_pvc                                                       9191
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




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

NOTE:

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

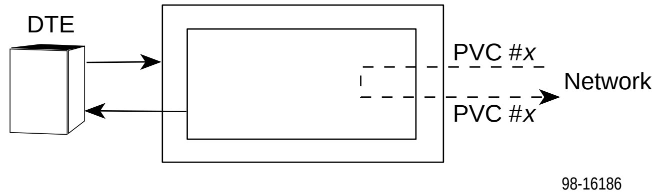
To start and stop PVC tests, see *Starting and Stopping a PVC or Local Loopback or a Pattern Test*.

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.

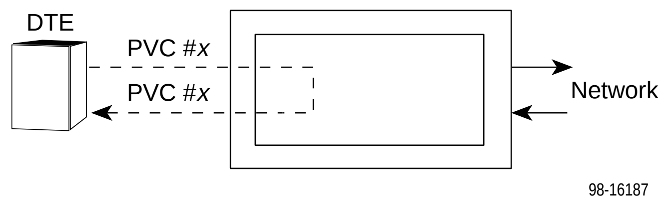
Main Menu → Test → Network PVC Test

Network PVC Loopback



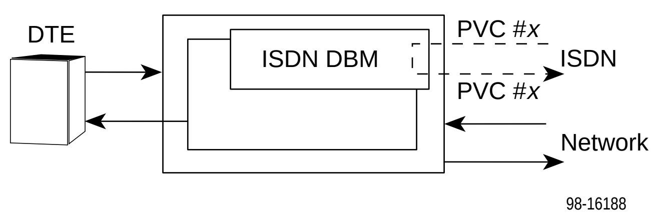
Main Menu → Test → Data Port PVC Tests

Port PVC Loopback



Main Menu → Test → ISDN 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 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 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 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.

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                                                          9191
Device Name: Node A                                             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 only appears when a Monitor Pattern Test is Active. Select ResetMon to reset the monitor pattern error counter.

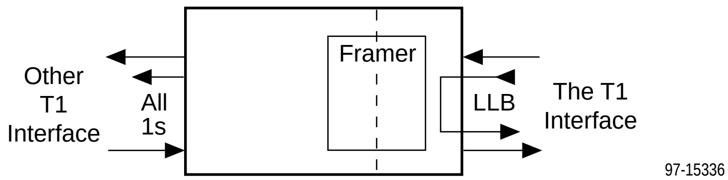
CAUTION:

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 local 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/DSX-1 Physical Tests/ PRI Physical Tests]



To start and stop a Line Loopback, see *Starting and Stopping a PVC or Local Loopback or a Pattern 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.

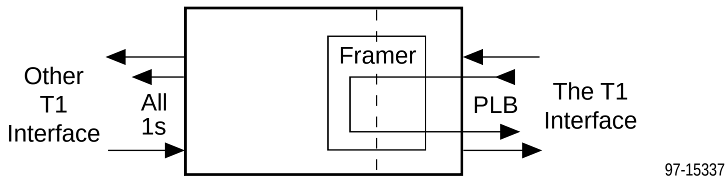
An LLB cannot be started when one of the following tests is active:

- Payload Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this interface.
- Repeater Loopback on any other T1 interface with DS0s assigned to this 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 interface.
- Data Channel Loopback on a frame relay link on this 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/DSX-1 Physical Tests/ PRI Physical Tests]



To start and stop a Payload Loopback, see *Starting and Stopping a PVC or Local Loopback or a Pattern Test*.

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.

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

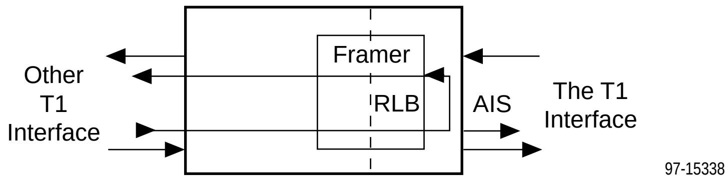
- Line Loopback, Repeater Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this interface.
- Payload or Repeater Loopback on any other T1 interface with DS0s assigned to this interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) 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 interface.
- Data Channel Loopback on the frame relay link on this 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 access unit is operational.

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

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



The T1 NAM will not respond to any messages from the network during this test.

To start and stop a Repeater Loopback, see *Starting and Stopping a PVC or Local Loopback or a Pattern 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.

A 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.
- Data Channel Loopback on a frame relay link on this network interface.

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.

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

To start and stop a Send Line Loopback, see *Starting and Stopping a Remote Loopback*.

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) assigned to this network interface.
- Data Channel Loopback on the frame relay link on this network interface.

User-Selected Pattern Test

Pattern tests enable a FrameSaver unit to either send or monitor a known bit pattern on a physical interface or port. 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	

To send or monitor a selected pattern test, see *Sending and Monitoring a User-Selected Pattern Test*

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

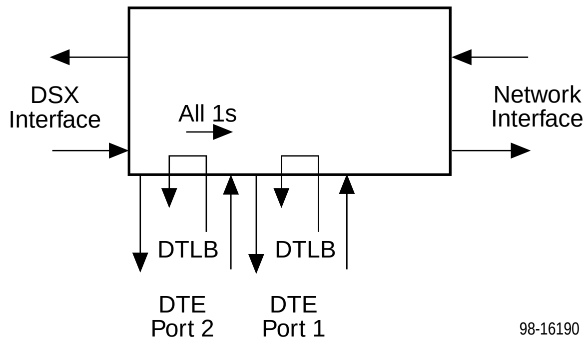
- Any loopback on the same interface.
- Send Pattern Test on any port assigned to this network interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) assigned to this network interface.

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 and monitor data being looped back.



To start and stop a DTE Loopback, see *Starting and Stopping a PVC or Local Loopback or a Pattern Test*.

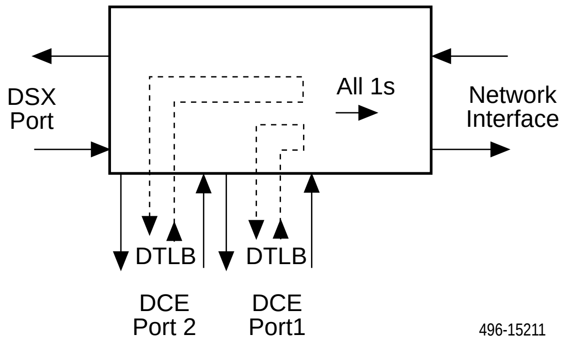
CAUTION:

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.

DTE Payload Loopback

The DTE Payload Loopback (DTPLB) loops the information received on the Network or DSX-1 interface back to the network after it has passed through the port circuitry. Use DTPLB for isolating problems on the DTE line. An attached device or test equipment must generate and monitor data to be looped back.

Main Menu → Test → Data Port Physical Tests



To start and stop a DTE Payload Loopback, see *Starting and Stopping a PVC or Local Loopback or a Pattern Test*.

CAUTION:

The Abort All Tests selection from the Test screen, or the test timeout feature, will not interrupt a DTE Loopback initiated by an attached device since the Local Loopback lead will still be asserted.

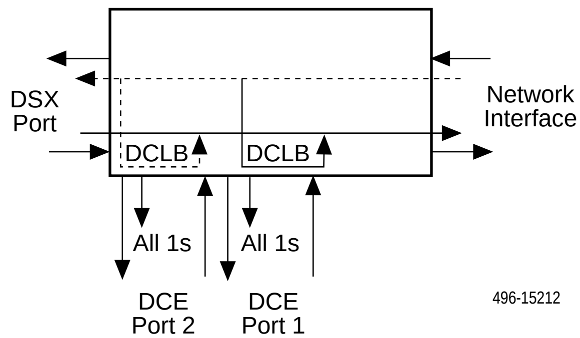
The following tests cannot be running on the same port when a DTE Payload Loopback is initiated:

- A DTE Loopback or Data Channel Loopback on the same port.
- A Send Pattern Test, Send V.54 Loopback, or Send FT1 Loopback on the same port.

Data Channel Loopback

The Data Channel Loopback (DCLB) loops the data for a particular synchronous data port back to the interface after the information has passed all the way through the device (i.e., just before it is sent to the Customer Premises Equipment). Use DCLB to verify the end-to-end integrity of a circuit for a particular port.

Main Menu → Test → Data Port Physical Tests



To start and stop a Data Channel Loopback, see *Starting and Stopping a PVC or Local Loopback or a Pattern Test*.

The following tests cannot be running when a DCLB test is initiated:

- A Line Loopback, Payload Loopback, Repeater Loopback, or Send Pattern Test on the interface to which the port is assigned.
- Send Pattern Test or DTE Payload Loopback on the same port.

Send V. 54 Loopback

The remote V.54 Loopback commands a device to go into the data channel loopback on the associated port.

To start and stop a Send V.54 Loopback, see *Starting and Stopping a Remote Loopback*.

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.

The following tests cannot be running when a V.54 Loopback is initiated:

- A Send Pattern Test, Send Remote Line Loopback, Payload Loopback, or Repeater Loopback on the interface to which the port is assigned.
- DTE Payload Loopback, Send Pattern Test, or Send FT1 Loopback on the same port.

Send FT1 Loopback

The remote FT1 Loopback commands a remote device to go into Data Channel Loopback on the associated port.

To start and stop a Send FT1 Loopback, see *Starting and Stopping a Remote Loopback*.

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.

The following tests cannot be running when an FT1 Loopback is initiated:

- A Send Pattern Test, Send Remote Line Loopback, Payload Loopback, or Repeater Loopback on the interface to which the port is assigned.
- DTE Payload Loopback, Send Pattern Test, or Send V.54 Loopback on the same port.

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

9

This chapter includes:

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
- Multiple maintenance schedules for scheduling more than one maintenance period, with a report for each scheduled task.

- Multiple Circuit IDs for multiple access levels so customers, as well as network service providers, have access to network management information.
- 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

10

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

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

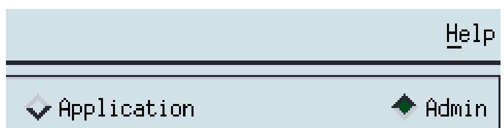
▶ Procedure

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

   — 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.

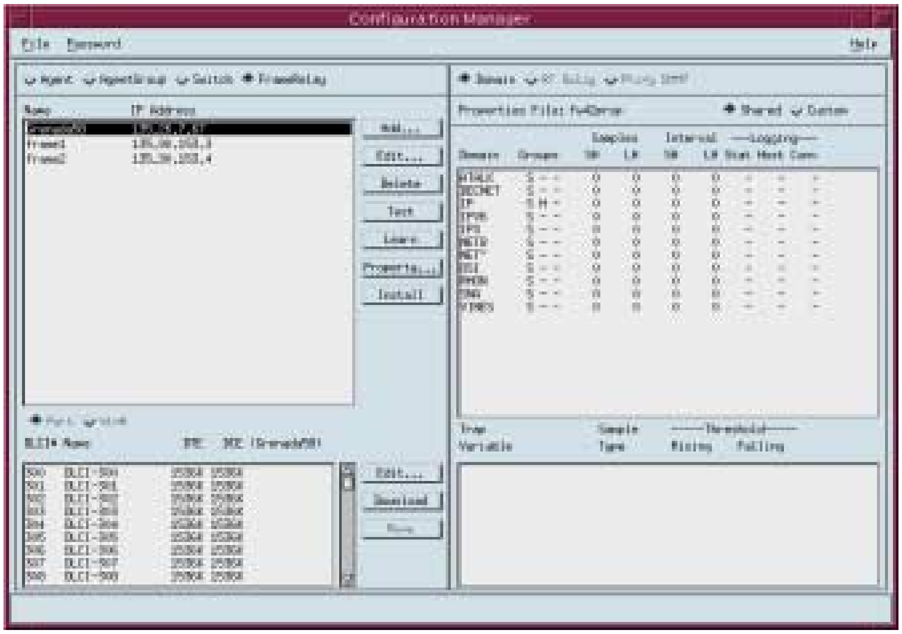
8. Select the Test button (fourth button down, center of the screen) to make sure you can communicate with the agent.

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.

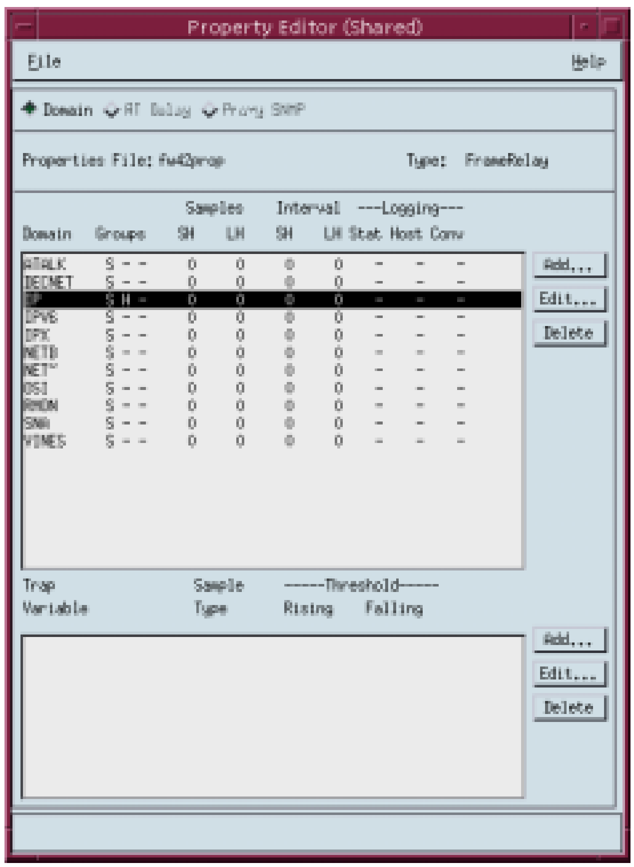
Correcting Domains and Groups

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

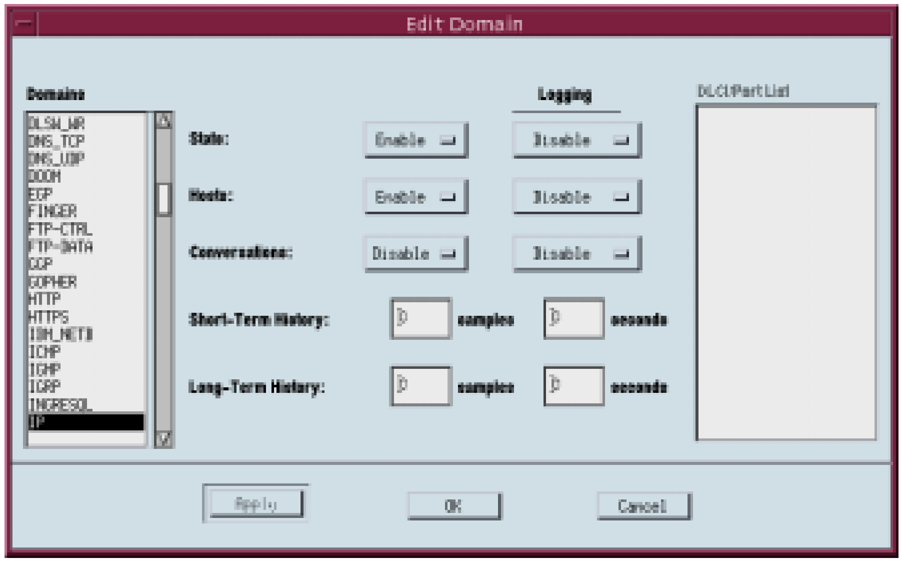
1. Select the the Property... button (down the center of the Configuration Manager main window). The Property Editor window opens.



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.

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



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

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

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

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

Adding SLV Alarms Using a Template

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

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

— Frames Sent (SLVFramesSnt)	— 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.

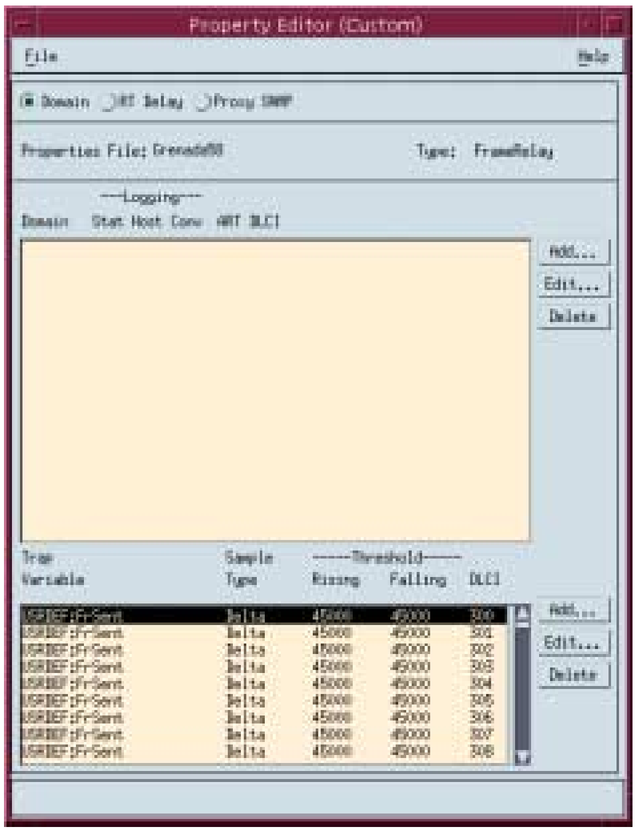
Editing Alarms

▶ 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.

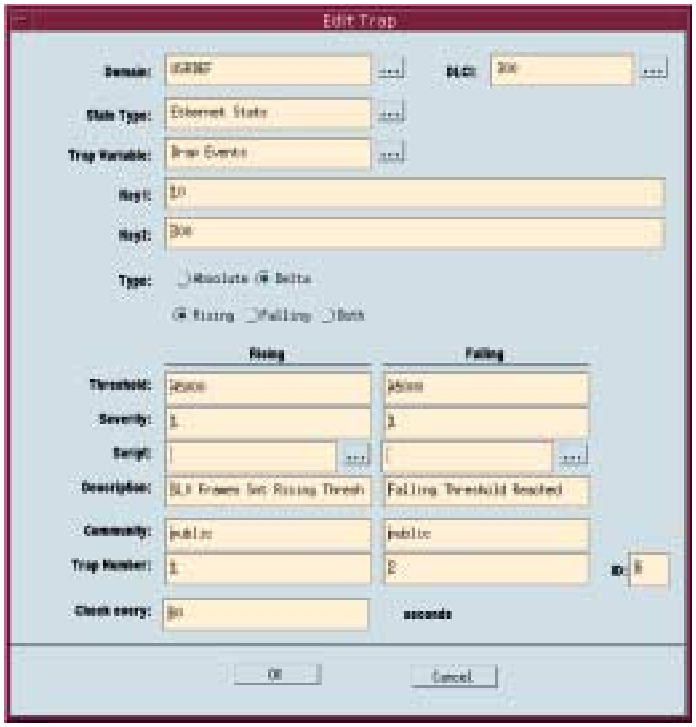
2. Select the Custom radio button from the Properties File area (in the upper right of the window), then Property... (down the center of the screen).

   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.



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

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

Adding SLV Alarms Manually

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

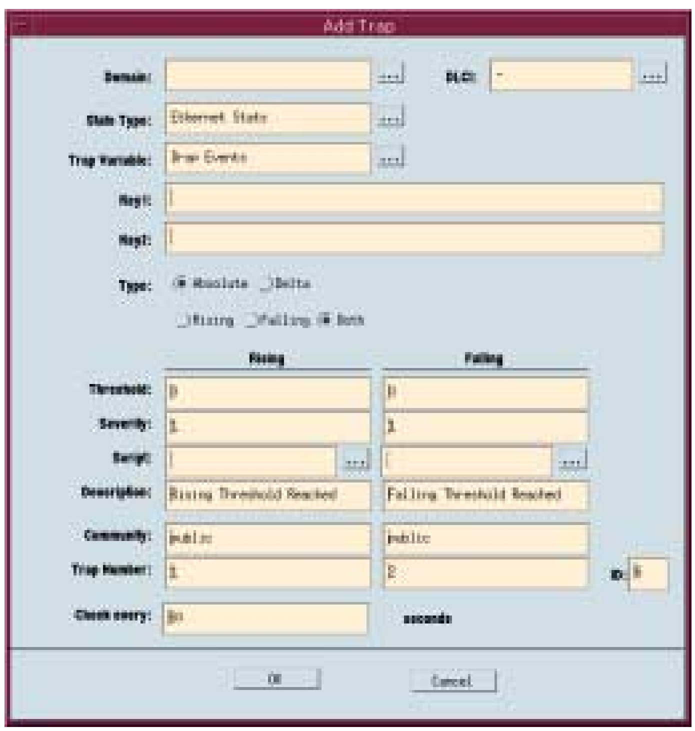
When configuring alarms manually, every alarm must be configured for each DLCI; that is, if there are eight alarms and 20 DLCIs, 160 trap configurations must be created (8 x 20). For this reason, it is recommended that the OpenLane defaults be used. Follow the procedure below to configure alarms manually.

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

▶ Procedure

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

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



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

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

[1] Latency MIB variables should be Absolute; all others should be Delta.
[2] Generally, Rising is selected.

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

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

Creating History Files

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

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

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

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

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

CAUTION:

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

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

▶ Procedure

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

   The variables in the file are listed with their OIDs (Object IDs). The frame relay interface number 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 9191 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 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.

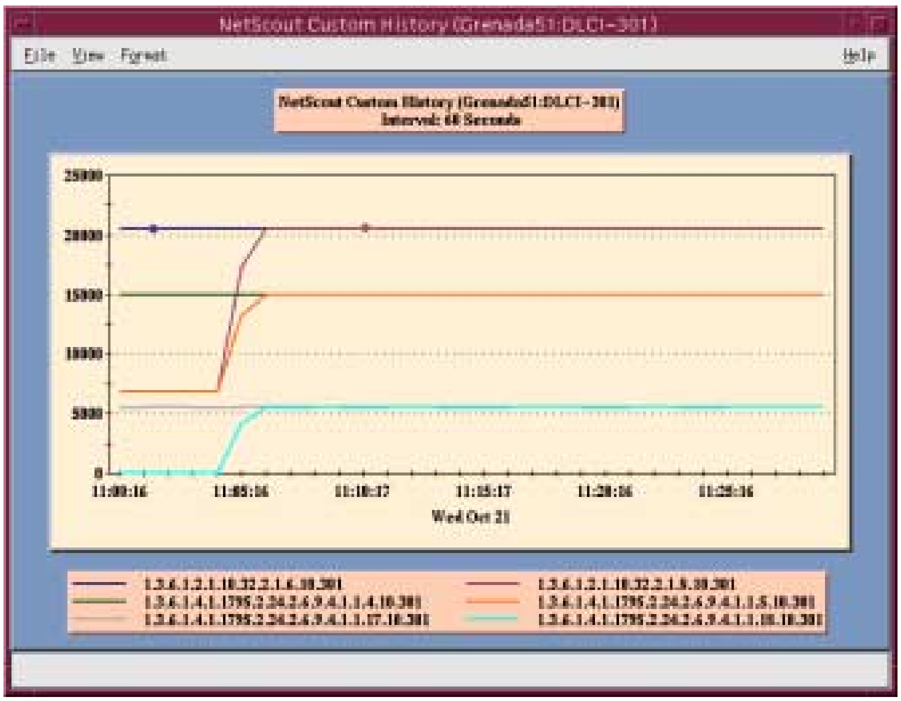
   The appropriate icons appear.

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.

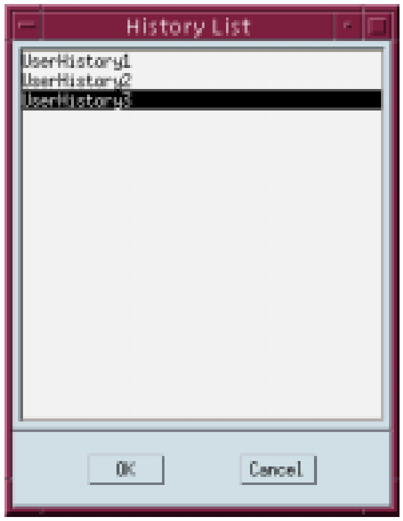
4. Click on the Custom History icon. The NetScout Custom History window opens.

   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.

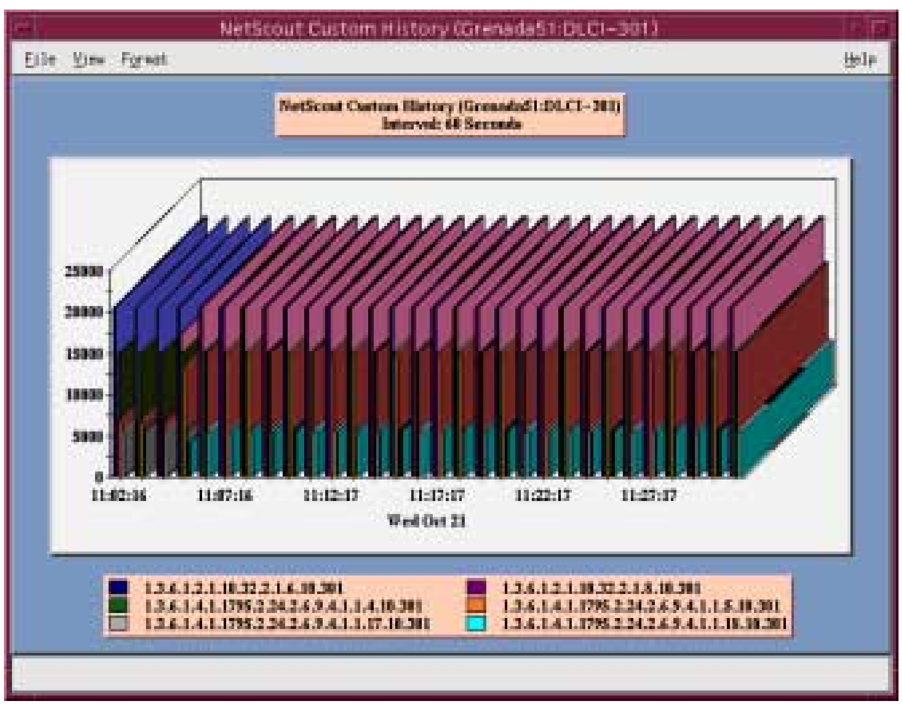
   The newly defined user history variables should appear on this list.



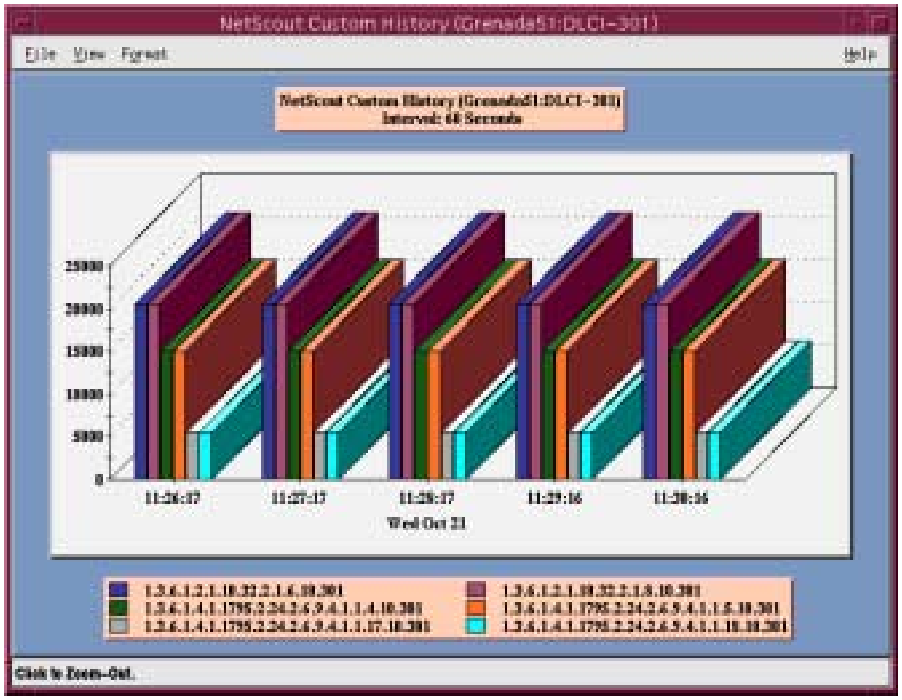
6. Highlight the desired set of user history variables, and select the OK button.

   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

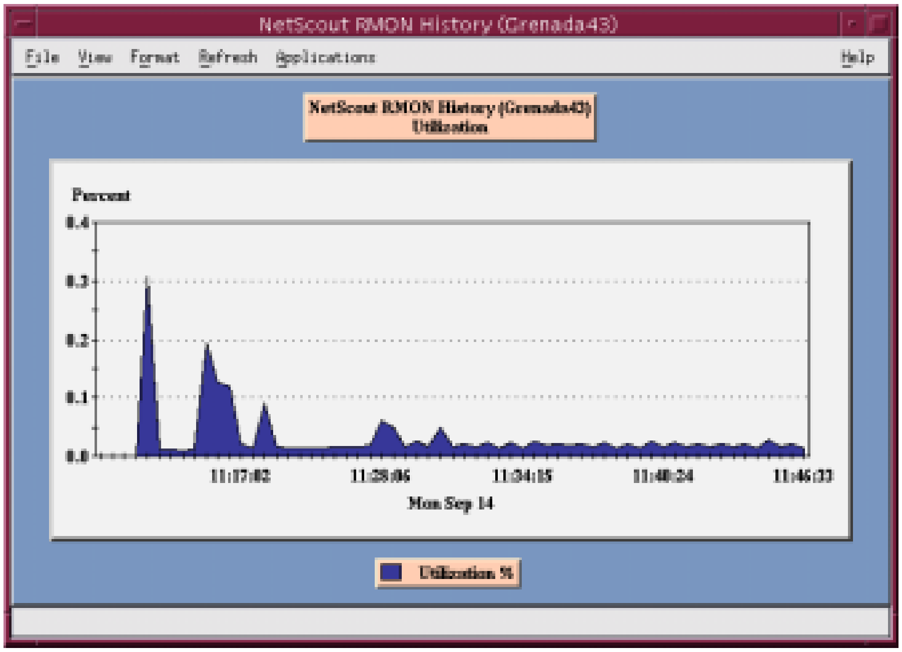
1. Select the Traffic radio button to monitor the newly added agent, or one of its DLCIs.

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

11

FrameSaver units are compatible with Concord Communication's Network Health software. In addition, Network Health has released the first in a series of software modules that integrate FrameSaver SLV enhanced performance statistics into its reporting package (see the FrameSaver SLV report example on page 11-10). 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:

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 11-10, you can compare a DLCI's volume with the network's performance over a specified period of time. Ranges for service level goals can be set for up to five variables: availability, bandwidth, bytes, health exceptions, and latency. These ranges need to be set before reports are scheduled. In addition, all the enhanced network statistics that only an SLV 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.

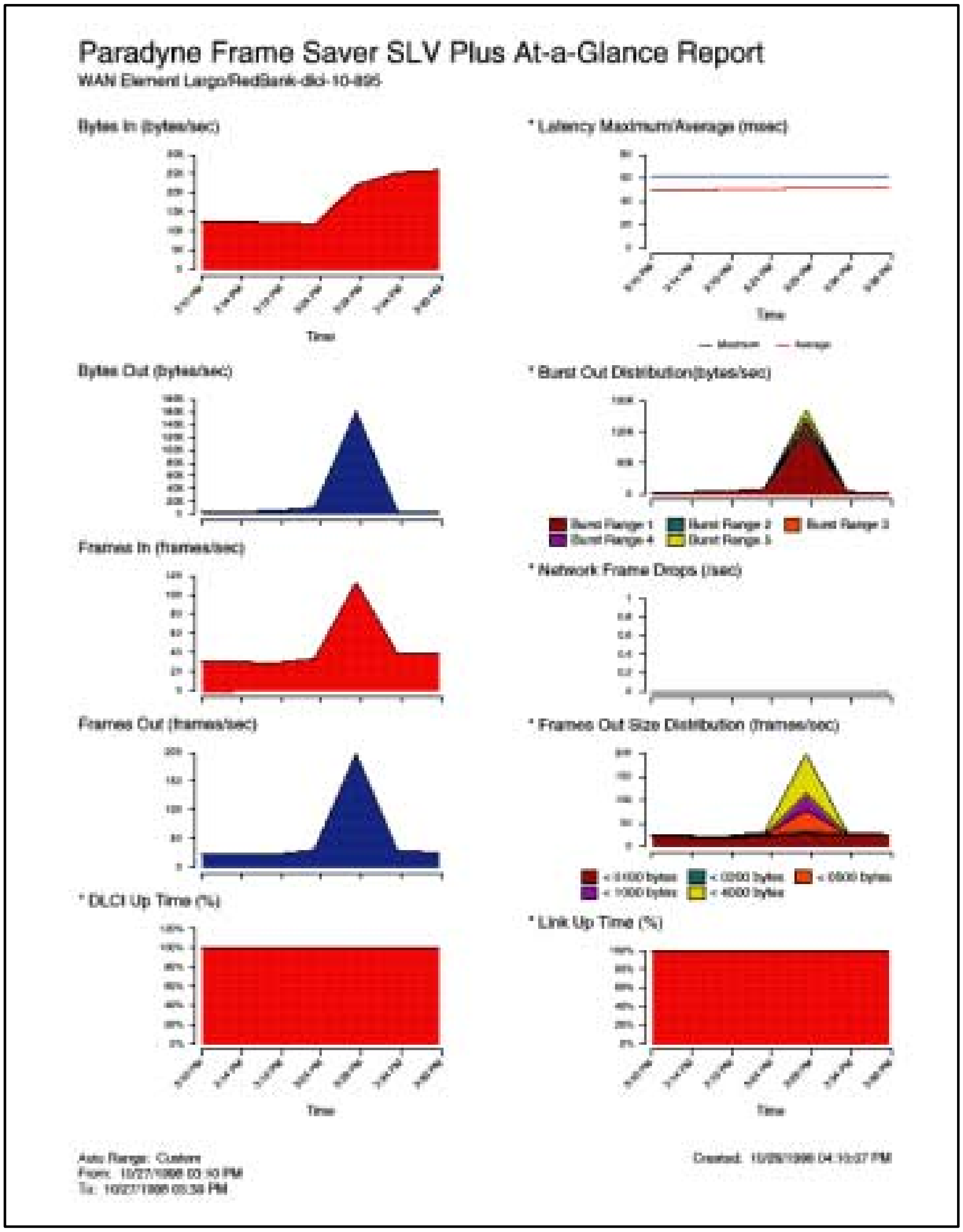
  — **Customer Service Level Report** – Provides service level information for customers. This report is used to provide service level information to service customers to help them determine optimum service levels needed based upon their own traffic data, as well as provide documented evidence for increasing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

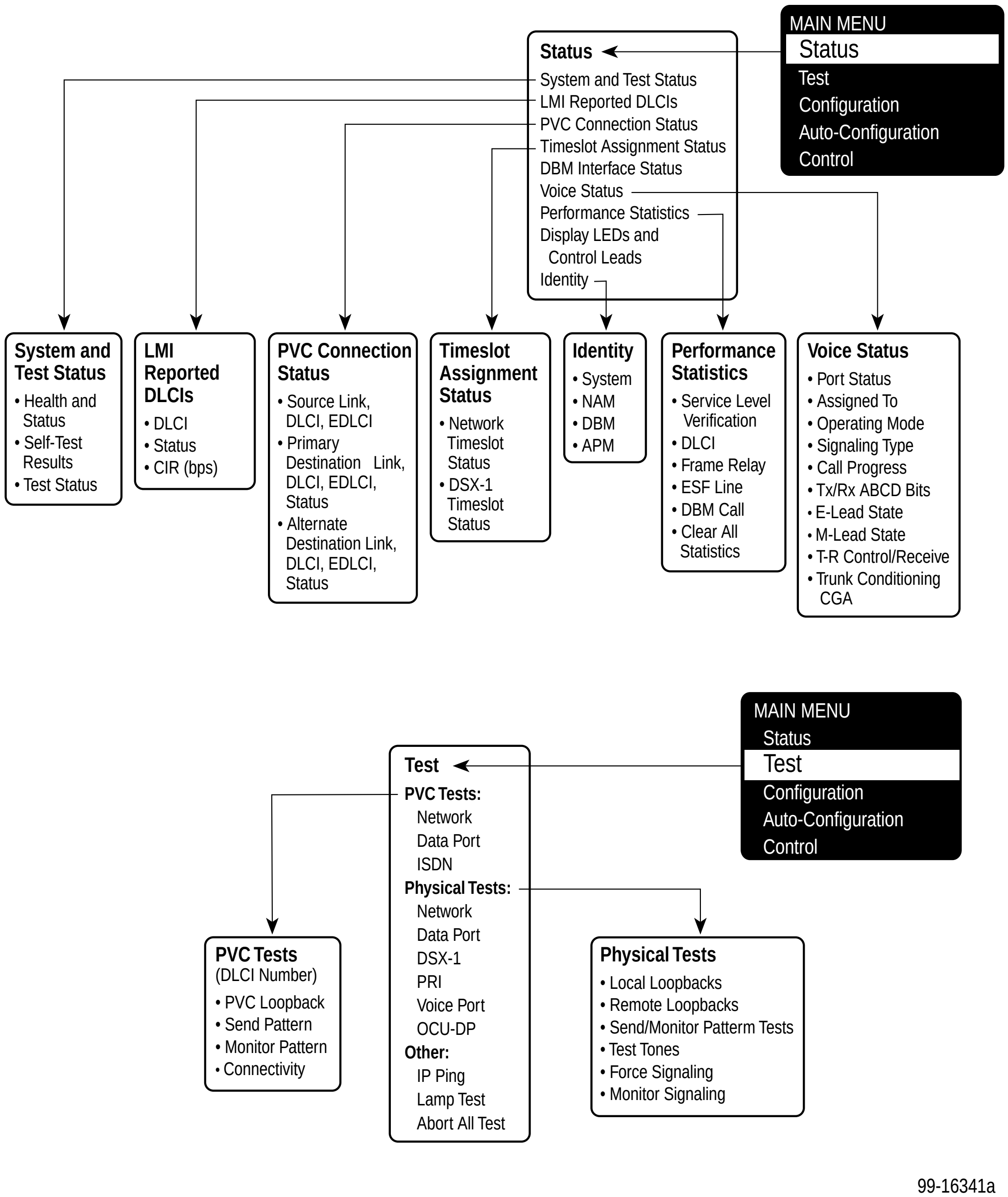
Menu Hierarchy

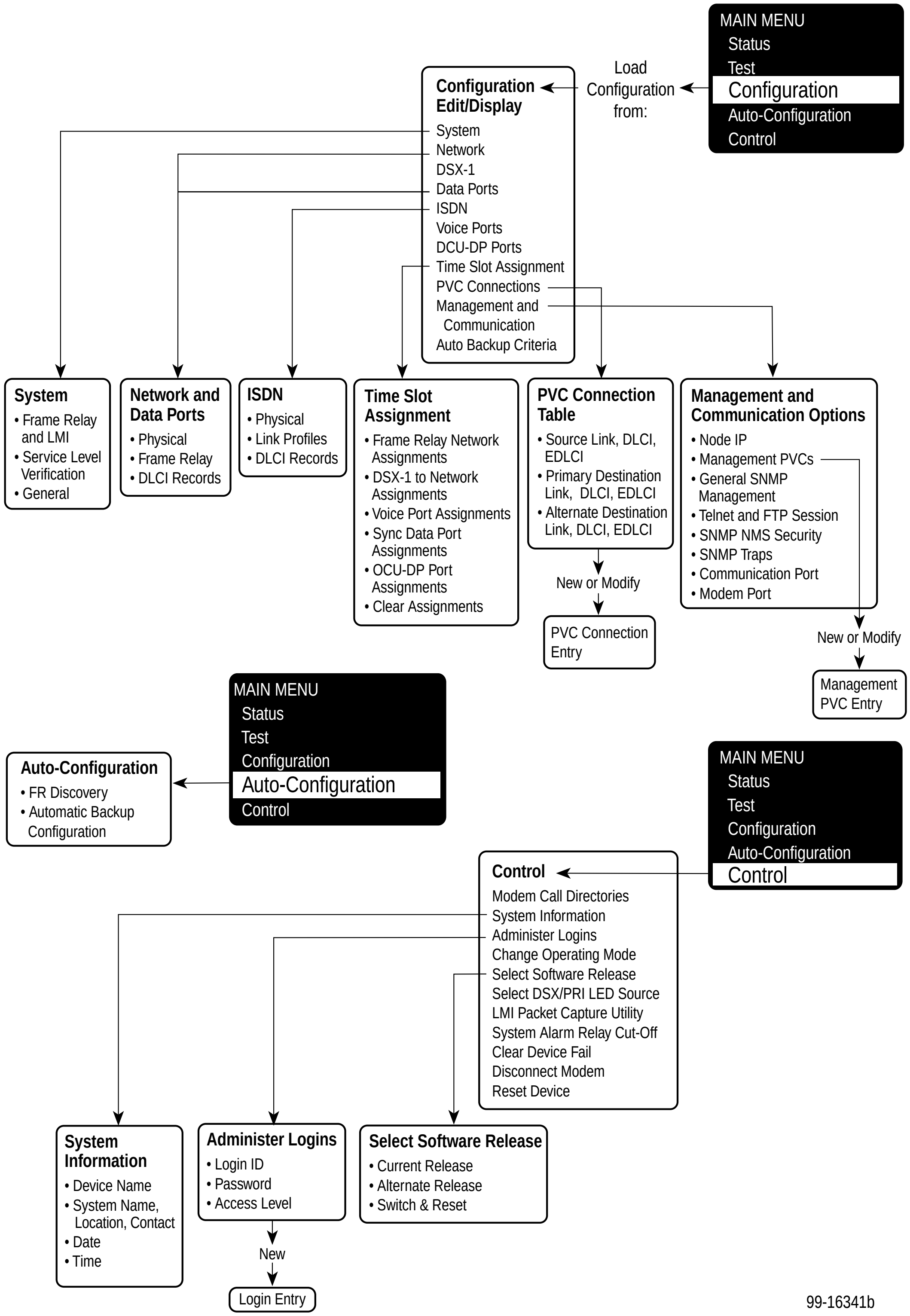
A

Menu

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

Menu Hierarchy




MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Load Configuration from:
Configuration Edit/Display
System
Network
DSX-1
Data Ports
ISDN
Voice Ports
DCU-DP Ports
Time Slot Assignment
PVC Connections
Management and Communication
Auto Backup Criteria
System
• Frame Relay and LMI
• Service Level Verification
• General
Network and Data Ports
• Physical
• Frame Relay
• DLCI Records
ISDN
• Physical
• Link Profiles
• DLCI Records
Time Slot Assignment
• Frame Relay Network Assignments
• DSX-1 to Network Assignments
• Voice Port Assignments
• Sync Data Port Assignments
• OCU-DP Port Assignments
• Clear Assignments
PVC Connection Table
• Source Link, DLCI, EDLCI
• Primary Destination Link, DLCI, EDLCI
• Alternate Destination Link, DLCI, EDLCI
New or Modify
PVC Connection Entry
Management and Communication Options
• Node IP
• Management PVCs
• General SNMP Management
• Telnet and FTP Session
• SNMP NMS Security
• SNMP Traps
• Communication Port
• Modem Port
New or Modify
Management PVC Entry
MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Auto-Configuration
• FR Discovery
• Automatic Backup Configuration
MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Control
Modem Call Directories
System Information
Administer Logins
Change Operating Mode
Select Software Release
Select DSX/PRI LED Source
LMI Packet Capture Utility
System Alarm Relay Cut-Off
Clear Device Fail
Disconnect Modem
Reset Device
System Information
• Device Name
• System Name, Location, Contact
• Date
• Time
Administer Logins
• Login ID
• Password
• Access Level
New
Login Entry
Select Software Release
• Current Release
• Alternate Release
• Switch & Reset
99-16341b

SNMP MIBs and Traps, and RMON Alarm Defaults

B

This appendix includes the following sections:

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
- 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 Service & 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 SLV 9192/9195 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: *[9192/9195]*; 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 9192: 1.3.6.1.4.1.1795.1.14.2.4.6.1
FrameSaver SLV 9195: 1.3.6.1.4.1.1795.1.14.2.4.6.2

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 on the NAM and APMs, the ifDescr, and the ifIndex that Paradyne has assigned to each (see Table B-1).

Table B-1. Paradyne Interface Objects Information (1 of 4)

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

Table B-1. Paradyne Interface Objects Information (2 of 4)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Physical Layer *(cont'd)*			
COM	Communications port	COM Port; T1 FR NAM; Hardware Version: *hhhh-hhh*	101004001
Modem	Modem port	Modem Port; T1 FR NAM; Hardware Version: *hhhh-hhh*	101005001
ISDN BRI DBM	ISDN BRI DBM interface (if applicable)	ISDN BRI DBM; T1 FR NAM; Child Card: ISDN-BRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101110001
ISDN PRI DBM	ISDN PRI DBM interface (if applicable)	ISDN PRI DBM; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101111001
Sync Data Port S*ss*P*n*	Synchronous Data APM, Port 1 – 4 (if applicable)	Synchronous Data Port, Slot: *s*, Port: *n*; Sync Data APM; Hardware Version: *hhhh-hhh*; Serial Number:*sssssss*	1*ss*007001 to 1*ss*007004
Voice FXS S*ss*P1	FXS Voice APM, Port 1 (if applicable)	Voice Port, Slot: *s*, Port: *n*; FXS Voice APM; Hardware Version: *hhhh-hhh*; Serial Number:*sssssss*	1*ss*007001
Voice E&M S*ss*P1	E&M Voice APM, Port 1 (if applicable)	Voice Port, Slot: *s*, Port: *n*; E&M Voice APM; Hardware Version: *hhhh-hhh*; Serial Number:*sssssss*	1*ss*008001
Voice FXO S*ss*P1	FXO Voice APM, Port 1 (if applicable)	Voice Port, Slot: *s*, Port: *n*; FXO Voice APM; Hardware Version: *hhhh-hhh*; Serial Number:*sssssss*	1*ss*009001
DDS OCU S*ss*P*n*	DDS OCU-DP APM, Port 1 – 2 or Port 1 – 6 (if applicable)	DDS OCU Port, Slot: *s*, Port: *n*; OCU [*2 or 6*] APM; Hardware Version: *hhhh-hhh*; Serial Number:*sssssss*	1*ss*012001 to 1*ss*012002 or 1*ss*012006

Table B-1. Paradyne Interface Objects Information (3 of 4)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Frame Relay Logical Layer			
FR UNI	Frame relay logical link on the T1 network interface	*For the DTE side:* Network T1 of FR DTE; T1 FR NAM; Hardware Version: *hhhh-hhh*	101015001
		For the DCE side: Network T1 of FR SERVICE; T1 FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on synchronous data Port-1 of the NAM	*For the user side:* Synchronous Data Port of FR DTE, Slot 1, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	101016001
		For the network side: Synchronous Data Port of FR SERVICE, Slot: 1, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on synchronous data Port-2 of the NAM (if applicable)	*For the user side:* Synchronous Data Port of FR DTE, Slot: 1, Port: 2; T1 FR NAM; Hardware Version: *hhhh-hhh*	101016002
		For the network side: Synchronous Data Port of FR SERVICE, Slot 1, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on a Sync Data APM, Port 1 – 4 (if applicable)	*For the user side:* Synchronous Data Port of FR DTE, Slot: *s*, Port: *n*; Sync Data APM; Hardware Version: *hhhh-hhh*	1*ss*007001 to 1*ss*007004
		For the network side: Synchronous Data Port of FR SERVICE, Slot: *s*, Port: *n*; Sync Data APM; Hardware Version: *hhhh-hhh*	

Table B-1. Paradyne Interface Objects Information (4 of 4)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Frame Relay Logical Layer *(cont'd)*			
FR UNI	Frame relay logical link on a DDS OCU-DP APM, Port 1 – 2 or Port 1 – 6 (if applicable)	*For the user side:* Network DDS of FR DTE, Slot: *s*, Port: *n*; OCU [*2 or 6*] APM; Hardware Version: *hhhh-hhh*	1*ss*012001 to 1*ss*012002 or 1*ss*012006
		For the network side: Network DDS of FR SERVICE, Slot: *s*, Port: *n*; OCU [*2 or 6*] APM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on BRI (if applicable)	*For the user side:* ISDN BRI DBM of FR DTE; Profile: *[Link Name]*; T1 FR NAM; Child Card: ISDN-BRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101018001 101018002
		For the network side: ISDN BRI DBM of FR SERVICE; Profile: *[Link Name]*; T1 FR NAM; Child Card: ISDN-BRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101018001 101018002
	Frame relay logical link on PRI (if applicable)	*For the user side:* ISDN PRI DBM of FR DTE; Profile: *[Link Name]*; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101017001 to 101017120
		For the network side: ISDN PRI DBM of FR SERVICE; Profile: *[Link Name]*; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	

NetScout Indexes to the Interface Table (ifTable)

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

Table B-2. NetScout Interface Objects Information (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 of the NAM	*For the DTE side:* RMON (IN/OUT); Network T1 of FR DTE; T1 FR NAM; Hardware Version: *hhhh-hhh*	1
		For the DCE side: RMON (IN/OUT); Network T1 of FR SERVICE; T1 FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on a DDS network interface of the APM	*For the DTE side:* RMON (IN/OUT); Network DDS of FR DTE, Slot: *s*, Port: *n*; OCU [*2 or 6*] APM; Hardware Version: *hhhh-hhh*	
		For the DCE side: RMON (IN/OUT); Network DDS of FR SERVICE, Slot: *s*, Port: *n*; OCU [*2 or 6*] APM; Hardware Version: *hhhh-hhh*	
Frame Relay 3 Sync Data Port 1	Frame relay logical link on Synchronous Data Port-1 of the NAM	*For the user side:* RMON (IN/OUT); Synchronous Data Port of FR DTE, Slot: *s*, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	3
		For the network side: RMON (IN/OUT); Synchronous Data Port of FR SERVICE, Slot: *s*, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on Synchronous Data Port-1 a Sync Data APM	*For the user side:* RMON (IN/OUT); Synchronous Data Port of FR DTE, Slot: *s*, Port: *n*; Sync Data APM; Hardware Version: *hhhh-hhh*	
		For the network side: RMON (IN/OUT); Synchronous Data Port of FR SERVICE, Slot: *s*, Port: *n*; Sync Data APM; Hardware Version: *hhhh-hhh*	

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

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Frame Relay Logical Layer *(cont'd)*			
Frame Relay 4 Sync Data Port 2	Frame relay logical link on Synchronous Data Port-2 of the NAM	*For the user side:* RMON (IN/OUT); Synchronous Data Port of FR DTE, Slot: *n*, Port: 2; T1 FR NAM; Hardware Version: *hhhh-hhh*	4
		For the network side: RMON (IN/OUT); Synchronous Data Port of FR SERVICE, Slot: *n*, Port: 2; T1 FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on Synchronous Data Port-2 of a Sync Data APM	*For the user side:* RMON (IN/OUT); Synchronous Data Port of FR DTE, Slot: *s*, Port: 2; Sync Data APM; Hardware Version: *hhhh-hhh*	
		For the network side: RMON (IN/OUT); Synchronous Data Port of FR SERVICE, Slot: *s*, Port: 2; Sync Data APM; Hardware Version: *hhhh-hhh*	
RMON Logical Layer			
RMON Frame Relay Logical Interfaces	These values are calculated. ■ For the DTE: (ifIndex –1) * 2 +17 ■ For the DCE: DTE calculated value +1	IN – RMON (IN); [*ifName of the interface*]	17–48
		OUT – RMON (OUT); [*ifName of the interface*]	
RMON Virtual Interfaces	These values are calculated based on the probe's internal circuit index: circuit index +65.	ALL – VIRTUAL PVC [*interface number*] [*DLCI number*] ALL	65–512
RMON Virtual Logical Interfaces	These values are calculated. ■ For the DTE: (virtual interface ifIndex –65) * 2 +513 ■ For the DCE: DTE calculated value +1	IN – VIRTUAL PVC [*interface number*] [*DLCI number*] DTE	513–1023
		OUT – VIRTUAL PVC [*interface number*] [*DLCI number*] DCE	

Standards Compliance for SNMP Traps

This section describes the FrameSaver unit's compliance with SNMP format standards and with its special operational trap features.

All traps have an associated string to help you decipher the meaning of the trap. Strings associated with an interface with a substring containing $ifString have the following format:

'DLCI $dlciNumber of $ifName frame relay link "$linkName".'

— $dlciNumber is the DLCI number. DLCI $dlciNumber only appears when a DLCI is associated with the trap.

— $linkName is the name given to the link. Frame relay $linkName only appears when a frame relay link is associated with the trap.

— $ifName is the string returned for the SNMP ifName variable.

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

The unit supports the following traps:

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

These traps are listed in alphabetical order within each table.

Trap: warmStart

This trap indicates that the FrameSaver unit has been reset and has stabilized.

Table B-3. warmStart Trap

Trap	What It Indicates	Possible Cause
warmStart	FrameSaver unit has just reinitialized and stabilized itself. **Variable-Bindings** devLastTrapString (devHealthAndStatus.mib)	■ Reset command sent. ■ Power disruption. *String:* 'Unit reset.'

Trap: authenticationFailure

Table B-4. authenticationFailure Trap

Trap	What It Indicates	Possible Cause
authenticationFailure	Access to the FrameSaver unit was attempted and failed.	■ SNMP protocol message not properly authenticated. ■ Three unsuccessful attempts were made to enter a correct login user ID/password combination. ■ IP Address security is enabled and a message was received from the SNMP Manager whose address was not on the lost of approved managers. *String:* 'Unauthorized access attempted.'
	Variable-Bindings	
	devLastTrapString (devHealthAndStatus.mib)	

Traps: linkUp and linkDown

These traps are supported on the following interfaces:

- Network, PRI or BRI, 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.

The following variable-bindings support the linkUp and linkDown traps.

Table B-6. linkUp and linkDown Variable-Bindings (1 of 3)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer – Represented by the entry in the MIB II Interfaces Table.		
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 – Loopback *Strings:* '$ifString down.' No alarms exist. (E.g., 'Network T1 down due to loopback.') '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the interface. *String:* '$ifString up.'
Synchronous Data Port (Supported by the media-specific RS232-like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the port. Alarm conditions include: – DTR [1] – RTS [2] – ' ' – Not DTR or RTS, but link is down. *String:* '$ifString $alarmString down.' (E.g., 'Sync Data Port S01P1 DTR and RTS down.') ■ linkUp – No alarms on the port. *String:* '$ifString up.'
[1] The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state. [2] The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state.		

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

Interface	Variable-Bindings	Possible Cause
Physical Sublayer (Cont'd)		
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. *Strings:* '$ifString down.' No alarms exist on the link. '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the interface. *String:* '$ifString up.'
OCU (Supported by the media-specific RS232-like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573)	■ linkDown – One or more alarm conditions are active on the interface. Alarm conditions include: – Loss of Signal – Abnormal Station Code – 64 KCC Loop OOF – DDS Net Failure *xxxxxx* (*xxxxxx* is the failure code) – Loss of Loop Timing ■ linkUp – No alarms on the interface.

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

Interface	Variable-Bindings	Possible Cause
Logical Link Sublayer – Represented by the entry in the MIB II Interfaces Table.		
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. *Strings:* '$ifString down.' No alarms exist on the link due to LMI. '$ifString LMI down.' No alarms exist on the link. (E.g., 'Frame Relay link "Chicago" on T1 Network LMI down.') '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$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. *Strings:* '$ifString LMI down.' '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$ifString up.'

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

Traps: enterprise-Specific

These traps indicate that an enterprise-specific event has occurred. Supported enterprise-specific traps include the following, listed in alphabetical order:

Table B-7. enterprise-Specific Traps and Variable-Bindings (1 of 4)

Trap	Variable-Bindings	Possible Cause
enterpriseAPM-Failed(9)	■ devCfgCardSlot	The system detected the failure of an APM, or the APM was removed from its configured slot. *String:* ‘APM failure on module in slot *s*.’ (Slot *s* is the slot number.)
enterpriseAPM-FailedClear(109)		The system detected the failure of an APM, or the APM was removed from its configured slot. *String:* ‘APM failure cleared on module in slot *s*.’ (Slot *s* is the slot number.)
enterpriseCIR-Change(15)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciCIR (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib)	CIR has changed due to the LMI report. LMI Protocol is set to Standard and the network’s CIR changed. *String:* ‘CIR on $ifString changed to $CIR bps.’
enterpriseConfig-Change(6)	■ devLastTrapString (devHealthAndStatus.-mib)	Configuration has been changed via the menu-driven user interface, an SNMP Manager, or auto-configuration after 60 seconds has elapsed without another change. *String:* ‘Device configuration change.’
enterpriseDevice-Fail(3)	An internal device failure. The variable binding for this trap is devHealthandStatus.	Operating software has detected an internal device failure.
enterpriseDLCI-delete (17)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib.)	The DLCI has been deleted. The network no longer supports the DLCI, and it was removed. *Strings:* ‘$ifString deleted by Auto-DLCI delete.’

Table B-7. enterprise-Specific Traps and Variable-Bindings (2 of 4)

Trap	Variable-Bindings	Possible Cause
enterpriseDLCI-Down(11)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib.)	DLCI Status is set to Inactive; the DLCI is down. *Strings:* '$ifString down.' (Due to LMI or physical failure.) '$ifString administratively shutdown.' (Due to an intentional shutdown.)
enterpriseDLCIUp(12)		DLCI Status is set to Active; DLCI is up again. *String:* '$ifString up.'
enterpriseLinkSpeed-Change(14)	■ ifIndex (RFC 1573) ■ ifSpeed (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib.)	Speed of the frame relay link has been changed by the unit's autorate algorithm. *String:* 'Speed of $ifName changed to $ifString bps.'
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. *String:* 'SLV down on $ifString due to excessive SLV packet loss. Total SLV packets lost is $numLost.'
enterpriseMissedSLV-Up(116)		SLV Timeout Error Event has been cleared. *String:* 'SLV up on $ifString because SLV communication was reestablished. Total SLV packets lost is $numLost.'
enterpriseModuleMis-Config(8)	■ devCfgCardSlot	An APM is installed in a slot currently configured for another type of APM. *String:* 'Misconfiguration occurred on module in slot *s*.' (Slot *s* is the slot number.)
enterpriseModuleMis-ConfigClear(108)		The APM was returned to its configured slot; the misconfiguration error has cleared. *String:* 'Misconfiguration cleared on module in slot *x*.' (Slot *x* is the slot number.)

Table B-7. enterprise-Specific Traps and Variable-Bindings (3 of 4)

Trap	Variable-Bindings	Possible Cause
enterprisePower-Supply(7)	■ devLastTrapString (devHealthAndStatus.-mib.)	Power to the unit has been lost. *String:* 'Power supply failed.'
enterprisePower-SupplyClear(107)		Power to the unit has been restored. *String:* 'Power supply restored.'
enterprisePrimary-ClockFail(1)	■ devLastTrapString (devHealthAndStatus.-mib)	Operating software has detected that the primary clock source has failed. *String:* 'Primary clock failed.'
enterprisePrimary-ClockFailClear(101)		Operating software has detected that the primary clock source is operational again. *String:* '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. *String:* 'RMON database reset to defaults.'
enterpriseSecondary-ClockFail(4)	■ devLastTrapString (devHealthAndStatus.-mib)	Operating software has detected that the secondary clock source has failed. *String:* 'Secondary clock failed.'
enterpriseSecondary-ClockFailClear(104)		Operating software has detected that the secondary clock source is operational again. *String:* 'Secondary clock restored.'
enterpriseSelfTest-Fail(2)	■ devLastTrapString (devHealthAndStatus.-mib)	Unit has completed (re)initialization and a hardware failure was detected. *String:* 'Self test failed: $*s*.' ($*s* is the contents of devSelfTestResult.)

Table B-7. enterprise-Specific Traps and Variable-Bindings (4 of 4)

<table>
<tr><th>Trap</th><th>Variable-Bindings</th><th>Possible Cause</th></tr>
<tr><td>enterpriseTest-Start(5)</td><td rowspan="2">For physical interfaces and frame relay links:
■ ifIndex (RFC 1573)
■ .0.0 (placeholder)
■ devLastTrapString (devHealthAndStatus.-mib
For virtual circuits (DLCIs):
■ devFrExtDlciIfIndex (devFrExt.mib)
■ devFrExtDlciDlci (devFrExt.mib)
■ devLastTrapString (devHealthAndStatus.-mib
For OCU APM:
■ ifIndex (RFC 1573)
■ ifAdminStatus (RFC 1573)
■ ifOperStatus (RFC 1573)
■ ifType (RFC 1573)
■ devOcuTestType (devOcu.mib)
For E&M, FXS, FXO APM:
■ ifIndex (RFC 1573)
■ ifAdminStatus (RFC 1573)
■ ifOperStatus (RFC 1573)
■ ifType (RFC 1573)
■ devVoiceTestType (devVoice.mib)
For a Voice Port:
■ ifIndex (RFC 1573)
■ ifAdminStatus (RFC 1573)
■ ifOperStatus (RFC 1573)
■ ifType (RFC 1573)
■ ifTestType (RFC 1573)</td><td>At least one test has been started on an interface or virtual circuit.
String:
‘$testString test started on $ifString.’ (e.g., ‘DTE Loopback test started on Sync Data Port S01P1.’)</td></tr>
<tr><td>enterpriseTest-Stop(105)</td><td>All tests have been halted on an interface or virtual circuit.
String:
‘$testString test stopped on $ifString.’ (e.g., ‘Disruptive PVC Loopback test stopped on DLCI 100 of Sync Data Port S01P1 frame relay.’)</td></tr>
</table>

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. risingAlarm and fallingAlarm 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. *String:* '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. *String:* 'Change in $variableName $typeString threshold of $alarmFallingThreshold by $(alarmValue – AlarmFallingThreshold.' (E.g., Octets received on Network T1 frame relay fell to threshold of 1.')

RMON Alarm and Event Defaults

The FrameSaver unit supports automatic generation of RMON alarm and event information. Each alarm sets an SNMP variable to monitor. When the threshold set for the monitored variable is exceeded, an SNMP trap or a log event is sent.

Event Defaults

Since all events sent are under the control of the FrameSaver unit, there is no need to define multiple events for each alarm type, so only the following two events need to be generated:

eventIndex	eventDescription	eventType	eventCommunity
1	Default SLV Rising Event	snmp-trap(3)	0
2	Default SLV Falling Event	snmp-trap(3)	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 Default*
- *Static Frame Relay Interface Alarm Defaults*
- *Dynamic Frame Relay Interface Alarm Defaults*
- *DLCI Alarm Defaults – Paradyne Area*
- *Static DLCI Alarm Defaults – NetScout Area*
- *Dynamic 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

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

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
Errored Seconds	D	*MIB:* DS1/E1 MIB (RFC 1406) *Tag:* dsx1TotalESs *OID:* .1.3.6.1.2.1.10.18.9.1.2.**I**	900 secs (15 mins)	Rising	1	1
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.

Static Frame Relay Interface Alarm Defaults

These alarms apply to the FrameSaver unit's frame relay interfaces. They are created during RMON initialization.

Table B-10. Static Frame Relay Interface Alarm Defaults (1 of 2)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Invalid Frames	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxIlFrames *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.18.**I**	900 secs (15 mins)	Rising	1	1
Short Frames	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxShort *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.6.**I**	900 secs (15 mins)	Rising	1	1
Long Frames	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxLong *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.7.**I**	900 secs (15 mins)	Rising	1	1
Rx Discards	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxDiscards *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.15.**I**	900 secs (15 mins)	Rising	1	1
Tx Discards	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTxDiscards *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.14.**I**	900 secs (15 mins)	Rising	1	1
Rx Total Errors	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotRxErrs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.20.**I**	900 secs (15 mins)	Rising	1	1

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

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

Table B-10. Static Frame Relay Interface 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.

Dynamic Frame Relay Interface Alarm Defaults

These alarms apply to the FrameSaver unit's frame relay interfaces. They are created during RMON initialization, and will change if the interface's line speed changes.

Table B-11. Dynamic Frame Relay Interface Alarm Defaults

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Rx Utilization	D	*MIB:* MIB II (RFC 1573) *Tag:* ifInOctets *OID:* .1.3.6.1.2.1.2.2.1.10.**I**	60 secs (1 min)	Rising	70% of link capability	65% of link capability
Tx Utilization	D	*MIB:* MIB II (RFC 1573) *Tag:* ifOutOctets *OID:* .1.3.6.1.2.1.2.2.1.16.**I**	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.
[2] **I** in the OID = Interface ID of the frame relay link.

DLCI Alarm Defaults – Paradyne Area

These alarms apply to DLCIs on the network interface. They are created either during RMON initialization or when a DLCI is created, and put into the Paradyne-defined alarm area.

Table B-12. DLCI Alarm Defaults – Paradyne Area

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
DLCI Inactive Seconds	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsInactive-Secs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.2.**I.D**	900 secs (15 mins)	Rising	1	1
Missing Latency Responses	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciMissedSLVs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.23.**I.D**	900 secs (15 mins)	Rising	5	5
Rx FECNs	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs *OID:* .1.3.6.1.2.1.10.32.2.1.4.**I.D**	60 secs (1 min)	Rising	1	1
Rx BECNs	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs *OID:* .1.3.6.1.2.1.10.32.2.1.5.**I.D**	60 secs (1 min)	Rising	1	1
Congested Seconds	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciSts-CongestedSecs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.6.**I.D**	60 secs (1 min)	Rising	5	5
Frames Dropped by Network	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciNetDropFr *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.20.**I.D**	60 secs (1 min)	Rising	1	1

[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.

Static 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 10, *Setting Up NetScout Manager Plus for FrameSaver Devices*.

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

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Current Latency	A	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyLatest *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.7.**I.D**	60 secs (1 min)	None	Must be configured.	0
Average Latency	A	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyAvg *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.5.**I.D**	900 secs (15 mins)	None	Must be configured.	0
Frames Received	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames *OID:* .1.3.6.1.2.1.10.32.2.1.8.**I.D**	60 secs (1 min)	None	Must be configured.	0
Frames Sent	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames *OID:* .1.3.6.1.2.1.10.32.2.1.6.**I.D**	60 secs (1 min)	None	Must be configured.	0
Tx Frames Exceeding CIR	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciTxFrOutCIR *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.17.**I.D**	60 secs (1 min)	None	Must be configured.	0

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

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Tx CIR Utilization	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets *OID:* .1.3.6.1.2.1.10.32.2.1.7.**I**.**D**	60 secs (1 min)	None	Must be configured.	0

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

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

Dynamic DLCI Alarm Defaults – NetScout Area

These alarms apply to DLCIs on the network interface. They are created either during RMON initialization or when a DLCI is created, and put into the NetScout-defined alarm area. They will be reconfigured if the interface's line speed changes.

Table B-14. 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	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets *OID:* .1.3.6.1.2.1.10.32.2.1.9.**I**.**D**	60 secs. (1 min)	Rising	70% of link capability	65% of link capability
Tx DLCI Link Utilization	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets *OID:* .1.3.6.1.2.1.10.32.2.1.7.**I**.**D**	60 secs. (1 min)	Rising	70% of link capability	65% of link capability

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

A = Absolute. Indicates that the exact value for the item is contained in the MIB.

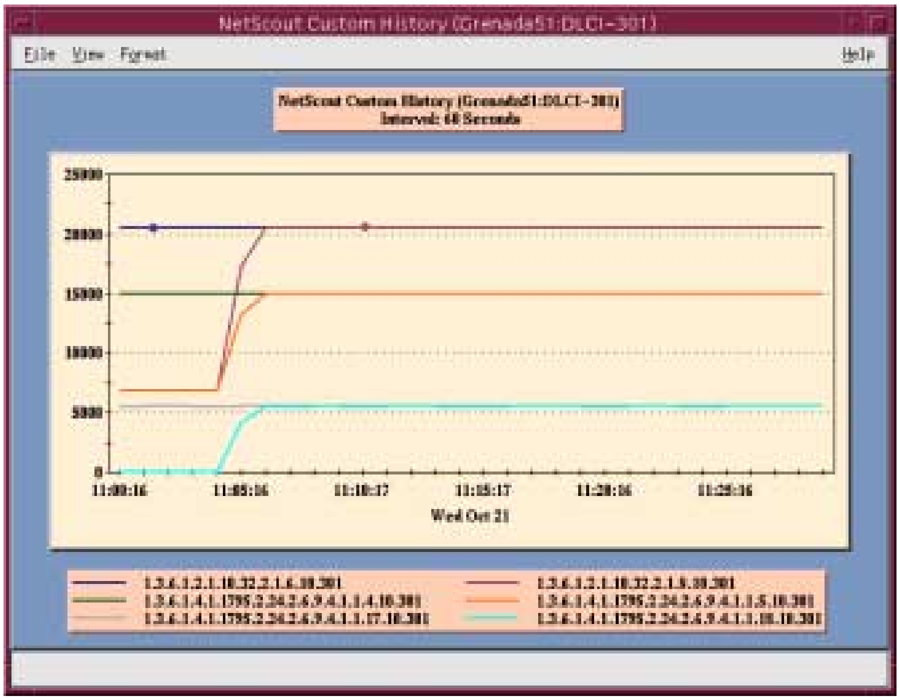
[2] **I** in the OID = Interface ID of the frame relay link.

D = DLCI number.

Object ID Cross-Reference (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-15 for an RMON history OID cross-reference and Table B-16 for an RMON alarm OID cross-reference.

Table B-15. History OID Cross-Reference (1 of 3)

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.**10.I**	All DLCI + LMI Rx Octets	*MIB:* MIB II (RFC 1573) *Tag:* ifInOctets
.1.3.6.1.2.1.2.2.1.**16.I**	All DLCI + LMI Tx Octets	*MIB:* MIB II (RFC 1573) *Tag:* ifOutOctets
.1.3.6.1.2.1.2.10.32.2.1. . .		
.1.3.6.1.2.1.10.32.2.1.4.**I.D**	Rx FECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.**5.I.D**	Rx BECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.**6.I.D**	Tx Frames	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx Octets	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**8.I.D**	Rx Frames	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.**9.I.D**	Rx Octets	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets
.1.3.6.1.2.1.16.12.2.1. . .		
.1.3.6.1.2.1.16.12.2.1.**2.P**	Protocol Octets (for 11 protocols)	*MIB:* RMON II (RFC 2021) *Tag:* protocolDistStatsOctets
.1.3.6.1.4.1.1795.2.24.2. . .		
.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.**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] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-15. History OID Cross-Reference (2 of 3)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.3.I.D**	DLCI CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciFrCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.17.I.D**	Tx Frames Above CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciTxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.18.I.D**	Rx Frames Above CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciRxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.20.I.D**	Network Frames Lost	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciNetDropFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.22.I.D**	Rx DEs	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciRxDE
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.37.I.D**	Network Frames Offered	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciRmtOffFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.39.I.D**	Network Frames Offered In CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciRmtOffFrInCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.41.I.D**	Network Frames Dropped In CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciDropOffFrInCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.43.I.D**	Network Frames Offered Above CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciRmtOffFrOutCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.45.I.D**	Network Frames Lost Above CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciRmtDropFrOutCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.2.I.D**	Inactive Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsInactiveSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.5.I.D**	Average Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.6.I.D**	Maximum Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyMax

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

Table B-15. History OID Cross-Reference (3 of 3)

Object ID (OID) [1]	**Item**	**MIB/Tag**
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1**.2.I.D.N**	Burst Upper Limit (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtBurstUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1**.3.I.D.N**	Burst Octets (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtBurstOctets
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1**.4.I.D.N**	Burst Frames (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtBurstFrames
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1**.2.I**	LMI Unavailable Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkNoLMISecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1**.17.I**	Total Rx CRC Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxCrcErr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1**.19.I**	Total Tx Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1**.20.I**	Total Rx Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1**.32.I**	Total LMI Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotLMIErrs

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

See Table B-16 for an RMON alarm OID cross-reference.

Table B-16. Alarm OID Cross-Reference (1 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.2.1.2.2.1. . .		
.1.3.6.1.2.1.2.2.1.**10.I**	Rx Utilization	*MIB:* MIB II (RFC 1573) *Tag:* ifInOctets
.1.3.6.1.2.1.2.2.1.**16.I**	Tx Utilization	*MIB:* MIB II (RFC 1573) *Tag:* ifOutOctets
.1.3.6.1.2.1.10.18.9.1. . .		
.1.3.6.1.2.1.10.18.9.1.**2.I**	Errored Seconds	*MIB:* DS1/E1 MIB (RFC 1406) *Tag:* dsx1TotalUASs
.1.3.6.1.2.1.10.18.9.1.**5.I**	Unavailable Seconds	*MIB:* DS1/E1 MIB (RFC 1406) *Tag:* 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	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.**5.I.D**	Rx BECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.**6.I.D**	Frames Sent	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx CIR Utilization	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx DLCI Link Utilization	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**8.I.D**	Frames Received	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.**9.I.D**	Rx DLCI Link Utilization	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets

[1] **I** = Interface ID of the frame relay link
D = DLCI number

Table B-16. 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.**1.1.17.I.D**	Tx Frames Exceeding CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciTxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.20.I.D**	Frames Dropped by Network	*MIB:* pdn_FrExt.mib (E) *Tag:* frFrExtDlciNetDropFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.23.I.D**	Missing Latency Responses	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciMissedSLVs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.6.I.D**	Congested Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsCongestedSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.2.I.D**	DLCI Inactive Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsInactiveSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.5.I.D**	Average Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.7.I.D**	Current Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyLatest
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.6.I**	Rx Short Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxShort
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.7.I**	Rx Long Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxLong
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.14.I**	Tx Discards	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.15.I**	Rx Discards	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.16.I**	Rx Nonoctet Aligns	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxNonOctet
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.17.I**	Rx CRC Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxCrcErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.18.I**	Rx Illegal Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxIlFrames

[1] **I** = Interface ID of the frame relay link
D = DLCI number

Table B-16. 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.**7.1.19.I**	Tx Total Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.20.I**	Rx Total Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.28.I**	Rx Overruns	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxOverruns
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.29.I**	Tx Underruns	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTxUnderruns
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.32.I**	Total LMI Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotalLMIErrs

[1] **I** = Interface ID of the frame relay link
D = DLCI number

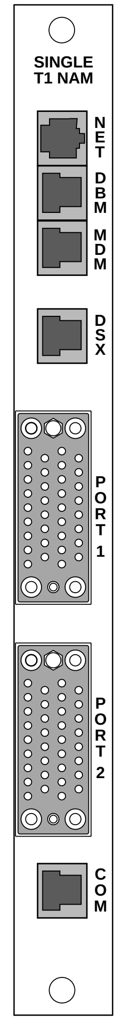
Connectors, Cables, and Pin Assignments

C

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

Rear Panel

The rear panel for the FrameSaver SLV NAM is shown. The NAM is installed in a 2-slot or 5-slot housing.



COM Port Connector

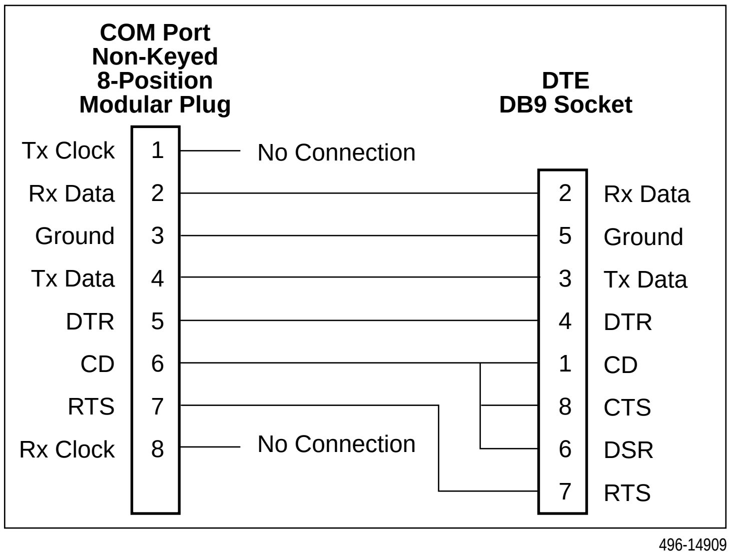
The following table shows the signals and pin assignments for the FrameSaver unit's 8-position communication port.

Table C-1. COM Port 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

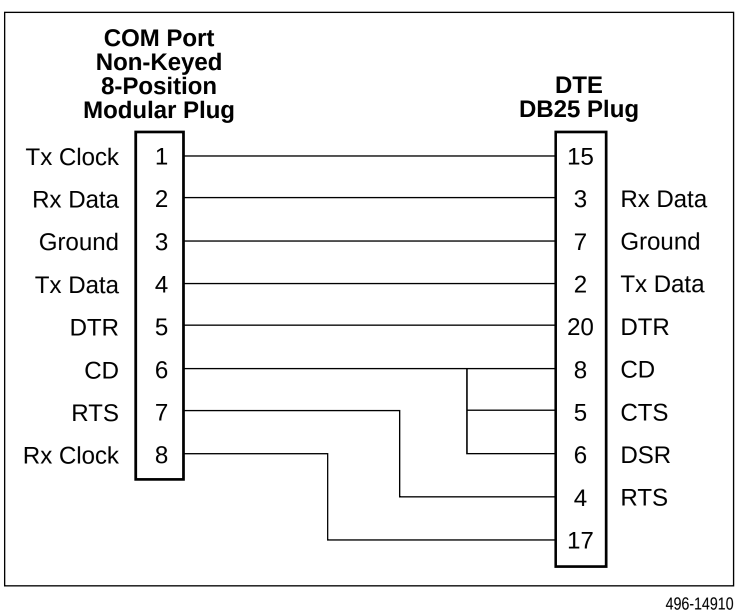
COM Port-to-PC Cable (Feature No. 3100-F2-550)

This cable comes with the FrameSaver unit. The following shows the pin assignments from the COM port to the PC interface.



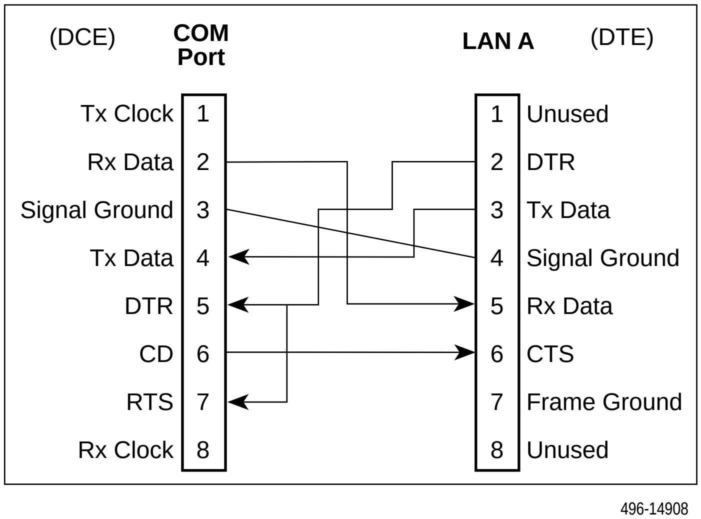
COM Port-to-Terminal Cable (Feature No. 3100-F2-540)

Order this cable when connecting the COM port to a terminal, rather than to a PC; it does not come with the FrameSaver unit. The following shows the pin assignments from the COM port to the terminal interface.



COM Port-to-LAN Adapter Cable (Feature No. 3100-F2-910)

A LAN adapter may be required when connecting to a LAN. The following shows the pin assignments for the custom 8-conductor cable (with modular plugs on both ends) between the COM port and the LAN.



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 cable's plug-type interface to a socket-type interface for the AUX port.

T1 Network Connector

The T1 network interface/connector is an RJ48C 8-position keyed modular jack.

T1 Network Cable (Feature No. 3100-F1-500)

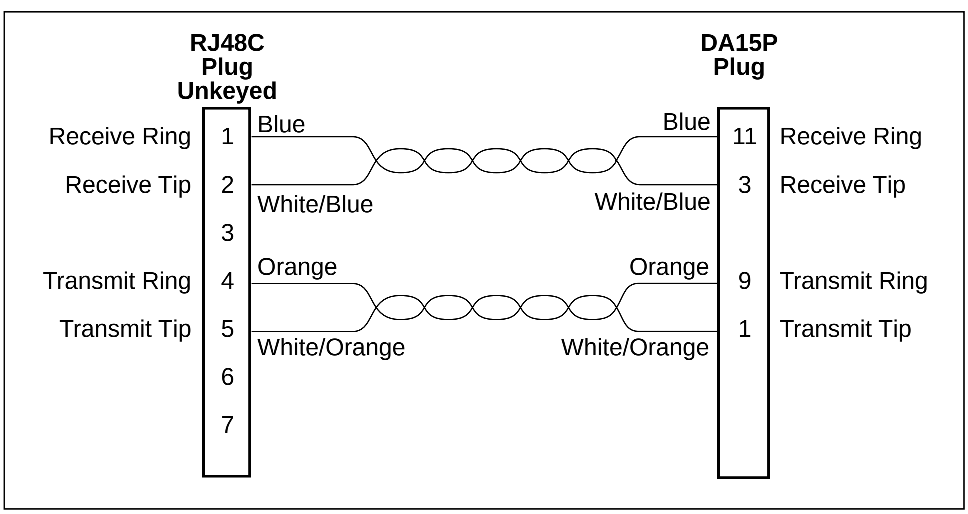
Network access to the FrameSaver unit is via a 20-foot cable with an RJ48C unkeyed plug-type connector on each end. The following table shows pin assignments and the purpose of each.

Table C-2. T1 Network Cable

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

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 NAM's network connector and the T1 network interface. The following diagram shows pin assignments and the purpose of each.



98-16215

DSX-1 Connector

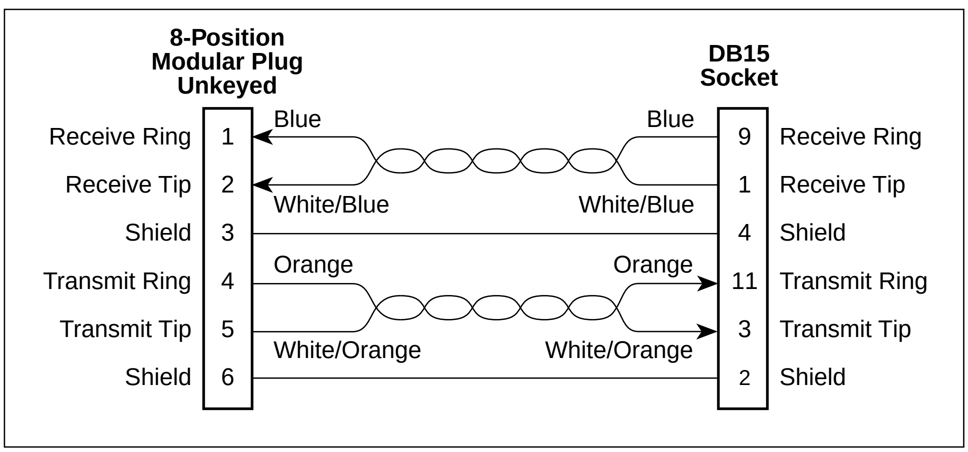
The following table shows the signals and pin assignments for the 8-position modular DSX-1 interface on the FrameSaver unit. The DSX-1 Adapter is required for this interface.

Table C-3. DSX-1 Connector

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

DTE Port Connectors

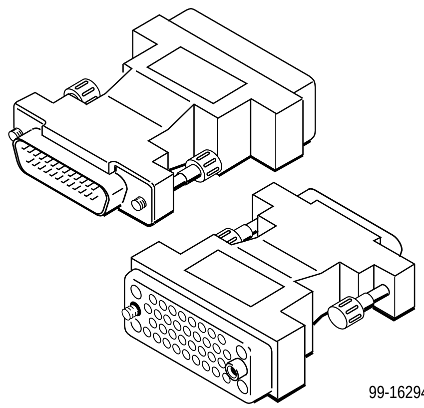
The following table provides the pin assignments for the FrameSaver unit's 34-position V.35 connector to the DTE.

Table C-4. V.35 DTE Port Connectors

Signal	ITU CT#	Direction	34-Pin Socket
Shield	101	—	A
Signal Ground/Common	102	—	B
Request to Send (RTS)	105	To DSU (In)	C
Clear to Send (CTS)	106	From DSU (Out)	D
Data Set Ready (DSR)	107	From DSU (Out)	E
Receive Line Signal Detector (RLSD or LSD)	109	From DSU (Out)	F
Data Terminal Ready (DTR)	108/1, /2	To DSU (In)	H
Local Loopback (LL)	141	To DSU (In)	L
Transmit Data (TXD)	103	To DSU (In)	P (A) S (B)
Receive Data (RXD)	104	From DSU (Out)	R (A) T (B)
Transmit Signal Element Timing – DTE Source (XTXC or TT)	113	To DSU (In)	U (A) W (B)
Receive Signal Element Timing – DCE Source (RXC)	115	From DSU (Out)	V (A) X (B)
Transmit Signal Element Timing – DCE Source (TXC)	114	From DSU (Out)	Y (A) AA (B)
Test Mode Indicator (TM)	142	From DSU (Out)	NN

EIA-530A-to-V.35 DTE Adapter

This adapter is used as an interface between a 25-position EIA-530A synchronous data port and a DTE's V.35 connector.



99-16294

The following table provides the pin assignments for the EIA-530A-to-V.35 DTE adapter.

Table C-5. EIA-530A-to-V.35 DTE Adapter

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

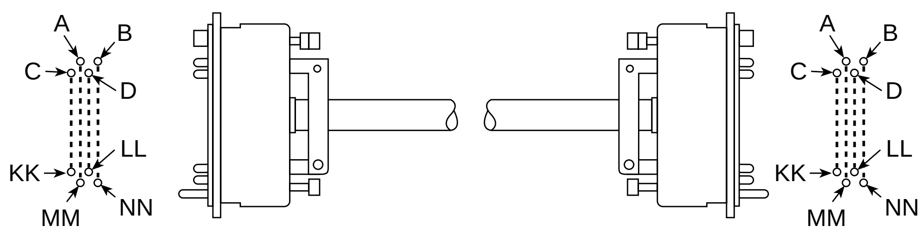
Standard V.35 Straight-through Cable

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.



	P1 Pin	P2 Pin
TXD A	P	T
TXD B	S	R
RXD A	R	S
RXD B	T	P
TXC A	Y	Z
TXC B	AA	AA
	Z	Y
RXC A	V	W
RXC B	X	U
ETXC A	U	X
ETXC B	W	V
FRM GND	A	A
SIG GND	B	B
RTS	C	F
CD	F	C
DTR	H	E
DSR	E	H
LL	L	L

98-16165a

Modem Connector

The dial modem interface/connector that is integrated into the FrameSaver NAM is an RJ11 6-position, 4-contact unkeyed modular jack. The following table shows pin assignments and the purpose of each.

Table C-6. Modem Connector

Function	Circuit	Direction	Pin Number
Ring	R	To Local Loop	2
Tip	T	To Local Loop	3

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 ISDN PRI and BRI DBMs, and the purpose of each.

Table C-7. ISDN PRI DBM 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

Table C-8. ISDN BRI/U DBM 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

Synchronous Data APM Connectors

The following table shows the EIA-530A circuit and pin assignments for the synchronous data APM.

Table C-9. EIA-530A Synchronous Data Port Connectors

Signal	Circuit Mnemonic	ITU/ CCITT #	Direction	25-Pin Pin #
Shield	—	—	—	1
Transmitted Data (TXD)	BA	103	To DCE	2 (A) 14 (B)
Received Data (RXD)	BB	104	From DCE	3 (A) 16 (B)
Request to Send (RTS)	CA	105	To DCE	4 (A) 19 (B)
Clear to Send (CTS)	CB	106	From DCE	5 (A) 13 (B)
Data Set (or DCE) Ready (DSR)	CC	107	From DCE	6
Signal Ground/Common (SG)	AB	102A	—	7
Received Line Signal Detector (RLSD or LSD)	CF	109	From DCE	8 (A) 10 (B)
Transmit Signal Element Timing (TXC – DTE Source)	DA	113	To DCE	11 (B) 24 (A)
Transmitter Signal Element Timing (TXC – DCE Source)	DB	114	From DCE	12 (B) 15 (A)
Receiver Signal Element Timing (RXC – DCE Source)	DD	115	From DCE	17 (A) 9 (B)
Local Loopback (LL)	LL	141	To DCE	18
Data Terminal (or DTE) Ready (DTR)	CD	108/1, /2	To DCE	20
Remote Loopback (RL)	RL	140	To DCE	21
Signal Common	AC	102B	—	22, 23
Test Mode Indicator (TM)	TM	142	From DCE	25

Voice APM Connectors

This section provides the pin assignments for the FXO, FXS and E&M voice APM 50-pin Amphenol connectors (RJ27X socket), followed by the pin assignments for the extension cables that can be used with these APMs.

FXO/FXS Voice APM Connector

The FXO/FXS Analog Voice APM uses a single 50-pin connector to provide eight 2-wire interfaces for connecting to analog voice equipment.

Table C-10. FXO/FXS 50-Pin Amphenol Connector

Port	Pin	Signal
1	26	T
	1	R
2	29	T
	4	R
3	32	T
	7	R
4	35	T
	10	R
5	38	T
	13	R
6	41	T
	16	R
7	44	T
	19	R
8	47	T
	22	R
All other pins are unconnected.		

E&M Voice APM Connector

The E&M Analog Voice APM uses a single 50-pin connector (RJ27X socket) to provide eight 2-wire interfaces for connecting to analog voice equipment.

Table C-11. E&M 50-Pin Amphenol Connector (1 of 2)

Port	Pin	Function	Signal
1	26	Transmit tip	T
	1	Transmit ring	R
	27	Receive tip	T1
	2	Receive ring	R1
	28	E Lead	E
	3	M Lead	M
2	29	Transmit tip	T
	4	Transmit ring	R
	30	Receive tip	T1
	5	Receive ring	R1
	31	E Lead	E
	6	M Lead	M
3	32	Transmit tip	T
	7	Transmit ring	R
	33	Receive tip	T1
	8	Receive ring	R1
	34	E Lead	E
	9	M Lead	M
4	35	Transmit tip	T
	10	Transmit ring	R
	36	Receive tip	T1
	11	Receive ring	R1
	37	E Lead	E
	12	M Lead	M

Table C-11. E&M 50-Pin Amphenol Connector (2 of 2)

Port	Pin	Function	Signal
5	38	Transmit tip	T
	13	Transmit ring	R
	39	Receive tip	T1
	14	Receive ring	R1
	40	E Lead	E
	15	M Lead	M
6	41	Transmit tip	T
	16	Transmit ring	R
	42	Receive tip	T1
	17	Receive ring	R1
	43	E Lead	E
	18	M Lead	M
7	44	Transmit tip	T
	19	Transmit ring	R
	45	Receive tip	T1
	20	Receive ring	R1
	46	E Lead	E
	21	M Lead	M
8	47	Transmit tip	T
	22	Transmit ring	R
	48	Receive tip	T1
	23	Receive ring	R1
	49	E Lead	E
	24	M Lead	M
All	25	Signal Ground	SG
	50	Signal Battery	SB

APM Extension Cables

Extension cables can be ordered for use with the 50-pin FXO, FXS and E&M Voice APM connectors. They are all straight-through cables (i.e., Pin 1 on the voice APM side is Pin 1 on the M66 block side of the cable), and they coincide with the pins on the 50-pin APM connector.

The following table identifies these cables, indicates the voice APM it is used with, and describes when you might use each:

Table C-12. Extension Cables

Extension Cable	Length	Voice APM	When Used
1 Amphenol plug-to-1 Amphenol plug cable *(Twisted pair/25-pair: 1-26, 2-27, 3-28 . . . 25-50)* (Feature No. 9008-F1-531)	3′	E&M FXO FXS	To connect the voice APM's 50-pin Amphenol connector to the M66 block. When the M66 block is further than five feet from the APM connector, used as an extension to the 5-foot cable normally used. See *FXO/FXS Voice APM Connector* on Page C-13 or *E&M Voice APM Connector* on Page C-14 for pin assignments.
1 Amphenol socket-to-1 Amphenol plug cable *(Twisted pair/25-pair: 1-26, 2-27, 2-28 . . . 25-50)* (Feature No. 9008-F1-532)	25′	E&M FXO FXS	When the M66 block is further than five feet from the APM's connector, used as an extension to the 5-foot 1 Amphenol plug-to-1 Amphenol plug cable. See *FXO/FXS Voice APM Connector* on Page C-13 or *E&M Voice APM Connector* on Page C-14 for pin assignments.
3 Amphenol plugs-to-1 Amphenol plug connector assembly *(Twisted pair: T1-R1 . . .T24-R24, S1-S2)* (Feature No. 9008-F1-534)	6′	FXO FXS	To condense three voice APMs onto the single M66 block connector. Extend the cable using the 25-foot 1 Amphenol socket-to-1 Amphenol plug 25-pair cable. See Table C-13. *3 Amphenol Plugs-to-1 Amphenol Plug Cable* for pin assignments.
3 Amphenol plugs-to-4 Amphenol plugs connector assembly *(Twisted pair: T1-R1 . . .T24-R24, TR1-RR1 . . . TR24-RR24, M1-E1 . . . M24-E24, SG1-SG1 . . . SG3-SG3)* (Feature No. 9008-F1-533)	6′	E&M	To consolidate signals from three voice APMs and segregate four applications onto four M66 blocks (e.g., all transmit signals on one block, all receive signals on a second block, all E&M signals on a third, and all battery and signal ground signals on the fourth). Extend the cable using the 25-foot 1 Amphenol socket-to-1 Amphenol plug 25-pair cable. See Table C-14, Table C-15, and Table C-16 for pin assignments.

3 Amphenol Plugs-to-1 Amphenol Plug Cable

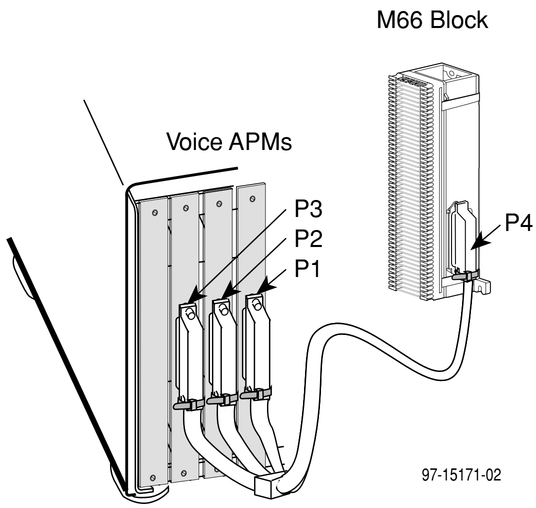


Table C-13. 3 Amphenol Plugs-to-1 Amphenol Plug Cable

M66 Plug	Pin	Connects to APM Plug	Pin	Signal	M66 Plug	Pin	Connects to APM Plug	Pin	Signal
P4	1	P1	1	R Port 1	P4	26	P1	26	T Port 1
	2		4	R Port 2		27		29	T Port 2
	3		7	R Port 3		28		32	T Port 3
	4		10	R Port 4		29		35	T Port 4
	5		13	R Port 5		30		38	T Port 5
	6		16	R Port 6		31		41	T Port 6
	7		19	R Port 7		32		44	T Port 7
	8		22	R Port 8		33		47	T Port 8
	9	P2	1	R Port 1		34	P2	26	T Port 1
	10		4	R Port 2		35		29	T Port 2
	11		7	R Port 3		36		32	T Port 3
	12		10	R Port 4		37		35	T Port 4
	13		13	R Port 5		38		38	T Port 5
	14		16	R Port 6		39		41	T Port 6
	15		19	R Port 7		40		44	T Port 7
	16		22	R Port 8		41		47	T Port 8
	17	P3	1	R Port 1		42	P3	26	T Port 1
	18		4	R Port 2		43		29	T Port 2
	19		7	R Port 3		44		32	T Port 3
	20		10	R Port 4		45		35	T Port 4
	21		13	R Port 5		46		38	T Port 5
	22		16	R Port 6		47		41	T Port 6
	23		19	R Port 7		48		44	T Port 7
	24		22	R Port 8		49		47	T Port 8
	25	–	–	–		50	–	–	–

3 Amphenol Plugs-to-4 Amphenol Plugs Cable

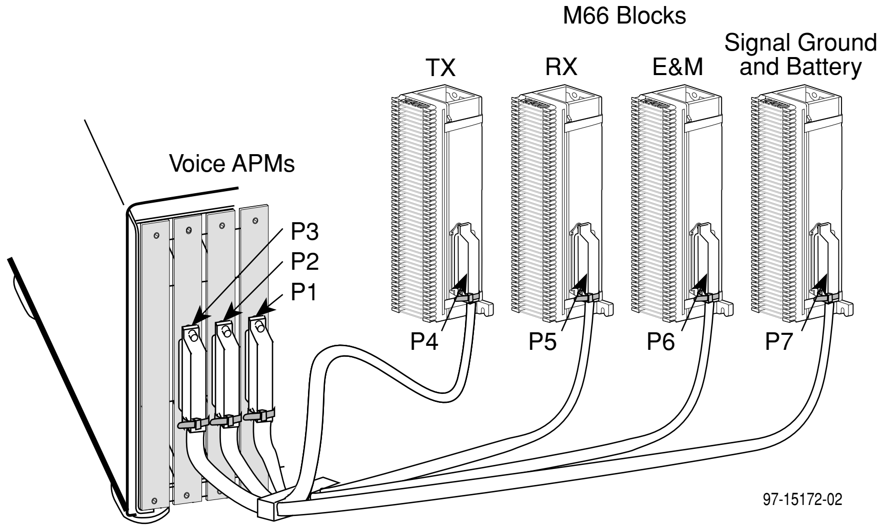


Table C-14. 3 Amphenol Plugs-to-4 Amphenol Plugs Cable for P1 (1 of 2)

P1 Pin #	Designation	Connects To	Pin #	Designation	Function
1	R (Port 1)	P4	1	R (Port 1)	Transmit Ring
2	R1 (Port 1)	P5	1	R1 (Port1)	Receive Ring
3	M (Port 1)	P6	1	M (Port 1)	M Lead
4	R (Port 2)	P4	2	R (Port 2)	Transmit Ring
5	R1 (Port 2)	P5	2	R1 (Port 2)	Receive Ring
6	M1 (Port 2)	P6	2	M (Port 2)	M Lead
7	R (Port 3)	P4	3	R (Port 3)	Transmit Ring
8	R1 (Port 3)	P5	3	R1 (Port 3)	Receive Ring
9	M (Port 3)	P6	3	M (Port 3)	M Lead
10	R (Port 4)	P4	4	R (Port 4)	Transmit Ring
11	R1 (Port 4)	P5	4	R1 (Port 4)	Receive Ring
12	M (Port 4)	P6	4	M (Port 4)	M Lead
13	R (Port 5)	P4	5	R (Port 5)	Transmit Ring
14	R1 (Port 5)	P5	5	R1 (Port 5)	Receive Ring
15	M (Port 5)	P6	5	M (Port 5)	M Lead
16	R (Port 6)	P4	6	R (Port 6)	Transmit Ring
17	R1 (Port 6)	P5	6	R1 (Port 6)	Receive Ring
18	M (Port 6)	P6	6	M (Port 6)	M Lead
19	R (Port 7)	P4	7	R (Port 7)	Transmit Ring
20	R1 (Port 7)	P5	7	R1 (Port 7)	Receive Ring
21	M (Port 7)	P6	7	M (Port 7)	M Lead
22	R (Port 8)	P4	8	R (Port 8)	Transmit Ring
23	R1 (Port 8)	P5	8	R1 (Port 8)	Receive Ring
24	M (Port 8)	P6	8	M (Port 8)	M Lead
25	SG (Ports 1–8)	P7	1–8	SG (Ports 1–8)	Signal Ground

Table C-14. 3 Amphenol Plugs-to-4 Amphenol Plugs Cable for P1 (2 of 2)

P1 Pin #	Designation	Connects To	Pin #	Designation	Function
26	T (Port 1)	P4	26	T (Port 1)	Transmit Tip
27	T1 (Port 1)	P5	26	T1 (Port 1)	Receive Tip
28	E (Port 1)	P6	26	E (Port 1)	E Lead
29	T (Port 2)	P4	27	T (Port 2)	Transmit Tip
30	T1 (Port 2)	P5	27	T1 (Port 2)	Receive Tip
31	E (Port 2)	P6	27	E (Port 2)	E Lead
32	T (Port 3)	P4	28	T (Port 3)	Transmit Tip
33	T1 (Port 3)	P5	28	T1 (Port 3)	Receive Tip
34	E (Port 3)	P6	28	E (Port 3)	E Lead
35	T (Port 4)	P4	29	T (Port 4)	Transmit Tip
36	T1 (Port 4)	P5	29	T1 (Port 4)	Receive Tip
37	E (Port 4)	P6	29	E (Port 4)	E Lead
38	T (Port 5)	P4	30	T (Port 5)	Transmit Tip
39	T1 (Port 5)	P5	30	T1 (Port 5)	Receive Tip
40	E (Port 5)	P6	30	E (Port 5)	E Lead
41	T (Port 6)	P4	31	T (Port 6)	Transmit Tip
42	T1 (Port 6)	P5	31	T1 (Port 6)	Receive Tip
43	E (Port 6)	P6	31	E (Port 6)	E Lead
44	T (Port 7)	P4	32	T (Port 7)	Transmit Tip
45	T1 (Port 7)	P5	32	T1 (Port 7)	Receive Tip
46	E (Port 7)	P6	32	E (Port 7)	E Lead
47	T (Port 8)	P4	33	T (Port 8)	Transmit Tip
48	T1 (Port 8)	P5	33	T1 (Port 8)	Receive Tip
49	E (Port 8)	P6	33	E (Port 8)	E Lead
50	SB (Ports 1–8)	P7	26–33	SB (Ports 1–8)	Signal Battery

Table C-15. 3 Amphenol Plugs-to-4 Amphenol Plugs Cable for P2 (1 of 2)

P2 Pin #	Designation	Connects To	Pin #	Designation	Function
1	R (Port 1)	P4	9	R (Port 9)	Transmit Ring
2	R1 (Port 1)	P5	9	R1 (Port 9)	Receive Ring
3	M (Port 1)	P6	9	M (Port 9)	M Lead
4	R (Port 2)	P4	10	R (Port 10)	Transmit Ring
5	R1 (Port 2)	P5	10	R1 (Port 10)	Receive Ring
6	M (Port 2)	P6	10	M (Port 10)	M Lead
7	R (Port 3)	P4	11	R (Port 11)	Transmit Ring
8	R1 (Port 3)	P5	11	R1 (Port 11)	Receive Ring
9	M (Port 3)	P6	11	M (Port 11)	M Lead
10	R (Port 4)	P4	12	R (Port 12)	Transmit Ring
11	R1 (Port 4)	P5	12	R1 (Port 12)	Receive Ring
12	M (Port 4)	P6	12	M (Port 12)	M Lead
13	R (Port 5)	P4	13	R (Port 13)	Transmit Ring
14	R1 (Port 5)	P5	13	R1 (Port 13)	Receive Ring
15	M (Port 5)	P6	13	M (Port 13)	M Lead
16	R (Port 6)	P4	14	R (Port 14)	Transmit Ring
17	R1 (Port 6)	P5	14	R1 (Port 14)	Receive Ring
18	M (Port 6)	P6	14	M (Port 14)	M Lead
19	R (Port 7)	P4	15	R (Port 15)	Transmit Ring
20	R1 (Port 7)	P5	15	R1 (Port 15)	Receive Ring
21	M (Port 7)	P6	15	M (Port 15)	M Lead
22	R (Port 8)	P4	16	R (Port 16)	Transmit Ring
23	R1 (Port 8)	P5	16	R1 (Port 16)	Receive Ring
24	M (Port 8)	P6	16	M (Port 16)	M Lead
25	SG (Ports 1–8)	P7	9–16	SG (Ports 9–16)	Signal Ground

Table C-15. 3 Amphenol Plugs-to-4 Amphenol Plugs Cable for P2 (2 of 2)

P2 Pin #	Designation	Connects To	Pin #	Designation	Function
26	T (Port 1)	P4	34	T (Port 9)	Transmit Tip
27	T1 (Port 1)	P5	34	T1 (Port 9)	Receive Tip
28	E (Port 1)	P6	34	E (Port 9)	E Lead
29	T (Port 1)	P4	35	T (Port 10)	Transmit Tip
30	T1 (Port 1)	P5	35	T1 (Port 10)	Receive Tip
31	E (Port 1)	P6	35	E (Port 10)	E Lead
32	T (Port 1)	P4	36	T (Port 11)	Transmit Tip
33	T1 (Port 1)	P5	36	T1 (Port 11)	Receive Tip
34	E (Port 1)	P6	36	E (Port 11)	E Lead
35	T (Port 1)	P4	37	T (Port 12)	Transmit Tip
36	T1 (Port 1)	P5	37	T1 (Port 12)	Receive Tip
37	E (Port 1)	P6	37	E (Port 12)	E Lead
38	T (Port 1)	P4	38	T (Port 13)	Transmit Tip
39	T1 (Port 1)	P5	38	T1 (Port 13)	Receive Tip
40	E (Port 1)	P6	38	E (Port 13)	E Lead
41	T (Port 1)	P4	39	T (Port 14)	Transmit Tip
42	T1 (Port 1)	P5	39	T1 (Port 14)	Receive Tip
43	E (Port 1)	P6	39	E (Port 14)	E Lead
44	T (Port 1)	P4	40	T (Port 15)	Transmit Tip
45	T1 (Port 1)	P5	40	T1 (Port 15)	Receive Tip
46	E (Port 1)	P6	40	E (Port 15)	E Lead
47	T (Port 1)	P4	41	T (Port 16)	Transmit Tip
48	T1 (Port 1)	P5	41	T1 (Port 16)	Receive Tip
49	E (Port 1)	P6	41	E (Port 16)	E Lead
50	SB (Ports 1–8)	P7	34–41	SB (Ports 9–16)	Signal Battery

Table C-16. 3 Amphenol Plugs-to-4 Amphenol Plugs Cable for P3 (1 of 2)

P3 Pin #	Designation	Connects To	Pin #	Designation	Function
1	R (Port 1)	P4	17	R (Port 17)	Transmit Ring
2	R1 (Port 1)	P5	17	R1 (Port 17)	Receive Ring
3	M (Port 1)	P6	17	M (Port 17)	M Lead
4	R (Port 2)	P4	18	R (Port 18)	Transmit Ring
5	R1 (Port 2)	P5	18	R1 (Port 18)	Receive Ring
6	M (Port 2)	P6	18	M (Port 18)	M Lead
7	R (Port 3)	P4	19	R (Port 19)	Transmit Ring
8	R1 (Port 3)	P5	19	R1 (Port 19)	Receive Ring
9	M (Port 3)	P6	19	M (Port 19)	M Lead
10	R (Port 4)	P4	20	R (Port 20)	Transmit Ring
11	R1 (Port 4)	P5	20	R1 (Port 20)	Receive Ring
12	M (Port 4)	P6	20	M (Port 20)	M Lead
13	R (Port 5)	P4	21	R (Port 21)	Transmit Ring
14	R1 (Port 5)	P5	21	R1 (Port 21)	Receive Ring
15	M (Port 5)	P6	21	M (Port 21)	M Lead
16	R (Port 6)	P4	22	T (Port 22)	Transmit Ring
17	R1 (Port 6)	P5	22	R1 (Port 22)	Receive Ring
18	M (Port 6)	P6	22	M (Port 22)	M Lead
19	R (Port 7)	P4	23	R (Port 23)	Transmit Ring
20	R1 (Port 7)	P5	23	R1 (Port 23)	Receive Ring
21	M (Port 7)	P6	23	M (Port 23)	M Lead
22	R (Port 8)	P4	24	R (Port 24)	Transmit Ring
23	R1 (Port 8)	P5	24	R1 (Port 24)	Receive Ring
24	M (Port 8)	P6	25	M (Port 24)	M Lead
25	SG (Ports 1–8)	P7	17–24	SG (Port 17–24)	Signal Ground

Table C-16. 3 Amphenol Plugs-to-4 Amphenol Plugs Cable for P3 (2 of 2)

P3 Pin #	Designation	Connects To	Pin #	Designation	Function
26	T (Port 1)	P4	42	T (Port 17)	Transmit Tip
27	T1 (Port 1)	P5	42	T1 (Port 17)	Receive Tip
28	E (Port 1)	P6	42	E (Port 17)	E Lead
29	T (Port 2)	P4	43	T (Port 18)	Transmit Tip
30	T1 (Port 2)	P5	43	T1 (Port 18)	Receive Tip
31	E (Port 2)	P6	43	E (Port 18)	E Lead
32	T (Port 3)	P4	44	T (Port 19)	Transmit Tip
33	T1 (Port 3)	P5	44	T1 (Port 19)	Receive Tip
34	E (Port 3)	P6	44	E (Port 19)	E Lead
35	T (Port 4)	P4	45	T (Port 20)	Transmit Tip
36	T1 (Port 4)	P5	45	T1 (Port 20)	Receive Tip
37	E (Port 4)	P6	45	E (Port 20)	E Lead
38	T (Port 5)	P4	46	T (Port 21)	Transmit Tip
39	T1 (Port 5)	P5	46	T1 (Port 21)	Receive Tip
40	E (Port 5)	P6	46	E (Port 21)	E Lead
41	T (Port 6)	P4	47	T (Port 22)	Transmit Tip
42	T1 (Port 6)	P5	47	T1 (Port 22)	Receive Tip
43	E (Port 6)	P6	47	E (Port 22)	E Lead
44	T (Port 7)	P4	48	T (Port 23)	Transmit Tip
45	T1 (Port 7)	P5	48	T1 (Port 23)	Receive Tip
46	E (Port 7)	P6	48	E (Port 23)	E Lead
47	T (Port 8)	P4	49	T (Port 24)	Transmit Tip
48	T1 (Port 8)	P5	49	T1 (Port 24)	Receive Tip
49	E (Port 8)	P6	49	E (Port 24)	E Lead
50	SB (Ports 1–8)	P7	42–49	SB (Ports 17–24)	Signal Battery

OCU Ports

The OCU-DP APM can have either two or six ports, each port having an RJ48S connector. Connect the OCU port to the DDS network using one of the following cables:

- 14-foot DDS cable (Feature No. 3600-F3-501)
- 25-foot DDS cable (Feature No. 3600-F3-502)

OCU Port Connectors

The OCU-DP port is a USOC RJ48S connector. The following table shows pin assignments and the purpose of each.

Table C-17. OCU Port Connector

Function	Circuit	Pin #
Transmit ring	R	1
Transmit tip	T	2
Receive tip	T1	7
Receive ring	R1	8

Technical Specifications

D

The following technical specifications are included:

- 2-Slot Housing Technical Specifications
- 5-Slot Housing Technical Specifications
- FrameSaver NAM and I/O Card Technical Specifications
- APM Technical Specifications
  - Synchronous Data APM
  - Voice APMs
  - OCU-DP APM
- ISDN DBM Technical Specifications
  - ISDN BRI DBM
  - ISDN PRI DBM

Table D-1. 2-Slot Housing Technical Specifications

Specification	Criteria
Physical Dimensions	
Height	11.0 inches (27.95 cm)
Width	4.3 inches (10.80 cm)
Depth	14.8 inches (37.48 cm)
Weight	
Empty housing (includes power supply)	11 lbs. 2 oz. (5.05 kg)
Heat Dissipation (Max.) at 115 VAC	
Fully loaded housing	145 Btu per hour
Power Requirements	
115 volts	90 to 132 VAC, 60 Hz $\pm$3, 0.5 amps

Table D-2. 5-Slot Housing Technical Specifications

Specification	Criteria
Physical Dimensions	
Height Desktop Rack-mount	 11.9 inches (30.23 cm) 10.5 inches (26.67 cm)
Width Desktop Rack-mount	 8.8 inches (22.35 cm) 8.2 inches (20.83 cm)
Depth Desktop Rack-mount	 15.6 inches (39.63 cm) 14.3 inches (36.32 cm)
Weight	
Empty housing (without power supply)	11 lbs. 6 oz. (5.15 kg)
Heat Dissipation (Max.) at 115 VAC	
Fully loaded housing	360 Btu per hour maximum
Power Requirements	
AC	90 to 132 VAC, 60 Hz±3, 1.5 amps maximum
DC	+24 VDC 4.85 amps 116 watts –48 VDC 2.35 amps 113 watts
Operating Voltage	*For negative input voltages:* Power supply disabled: Voltage < |38.5 ±1 VDC| Power supply enabled: Voltage > |43 ±0.5 VDC| *For positive input voltages:* Power supply disabled: Voltage <16.5 VDC nominal Power supply enabled: Voltage +20 VDC to +30 VDC Approximately 2 volts hysteresis between turn-on and turn-off voltage.

Table D-3. FrameSaver NAM and I/O Card Technical Specifications (1 of 2)

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 95% (noncondensing)
Shock and vibration	Withstands normal shipping and handling
Physical Dimensions	
NAM or APM Card	
Height	8 inches (20.32 cm)
Depth	11.58 inches (29.41 cm)
I/O Card	
Height	10.15 inches (25.78 cm)
Depth	2.9 inches (7.37 cm)
Weight	
NAM	1 lb. 2 oz. (.51 kg)
I/O Card	6 oz. (.17 kg)
Power Consumption and Dissipation	9.5 watts, 0.080 A at 120 VAC Result: 32 Btu per hour
T1 Network Interface	8-position modular unkeyed 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, ANSI T1-403

Table D-3. FrameSaver NAM and I/O Card Technical Specifications (2 of 2)

Specification	Criteria
DSX-1 Interface	
Physical interface	8-position modular unkeyed jack
Framing format	D4, ESF
Coding format	AMI, B8ZS
DTE line equalization	5 selectable ranges from 0 to 655 feet (0 to196.5 meters)
Send AIS	Selectable
COM Port – Communications/Management	8-position modular jack unkeyed
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
DTE Ports	34-position V.35 connector
Standard	V.35/ITU (ISO 2593)
Data rates	Variations for T1 rates; automatically set to the network rate.
ISDN BRI DBM Interface	One 8-position modular keyed USOC RJ49C jack
Physical interface	RJ49C
Service supported	BRI, NI-1
Data rates	56 kbps and 64 kbps
ISDN PRI DBM Interface	One 8-position modular unkeyed USOC RJ48C jack
Physical interface	RJ48C
Service supported	PRI, NI-1 or NI-2
Data rates	1.536 Kbps
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
Modem (MDM) Interface	6-position modular unkeyed USOC RJ11C jack
Data rates	Up to 14.4 Kbps
Link Protocol	PPP, SLIP

Table D-4. APM Technical Specifications (1 of 3)

Specification	Criteria
Synchronous Data APM	
Weight	
Sync Data APM	15 oz. (.425 kg)
Sync Data I/O card	6 oz. (.170 kg)
Size	
Sync Data APM	11.58 inches x 8.00 inches (29.41 cm x 20.32 cm)
Sync Data I/O card	2.90 inches x 10.15 inches (7.37 cm x 25.78 cm)
Power Consumption	5.8 watts, 0.48 amps input current at 12 volts Result: 19.79 Btu per hour
DTE Ports	
Standards	EIA-530A, V.35, RS-449, V.11, X.21
Rates	Nx64 – 64K to 1.536 Mb Nx56 – 56K to 1.344 Mb
Loopbacks	
Standard	V.54 Loop 2 (DCLB) and V.54 Loop 3 (DTPLB)
Additional	DTE Loopback
Voice APMs	
Weight	
E&M APM	14 oz. (.397 kg)
FXO APM	1 lb. (.454 kg)
FXS APM	1 lb. (.454 kg)
Voice I/O card	6 oz. (.170 kg)
Size	
E&M/FXO/FXS APM	11.58 inches x 8.00 inches (29.41 cm x 20.32 cm)
Voice I/O card	2.90 inches x 10.15 inches (7.37 cm x 25.78 cm)
Cable Length (Max.)	18,000 feet using 26 AWG
Power Consumption	
E&M APM	3.1 watts, 0.26 amps input current at 12 volts Result: 10.58 Btu per hour
FXO APM	3.5 watts, 0.29 amps input current at 12 volts Result: 11.94 Btu per hour
FXS APM (8 lines talking)	10.1 watts, 0.84 amps input current at 12 volts Result: 34.46 Btu per hour
FXS APM (8 lines ringing)	13.3 watts, 1.11 amps input current at 12 volts Result: 45.38 Btu per hour
Interface Connector	50-pin amphenol connector (RJ27X)

Table D-4. APM Technical Specifications (2 of 3)

Specification	Criteria
Voice APMs (cont'd)	
Operating Modes	
E&M	E&M Transmit Only
FXO	DPT FXO FXO DN FXO DN Wink
FXS	DPO FXS FXS DN FXS DN Wink PLAR
Signaling Types	
E&M	Type I Type II Type IV Type V
FXO	Loop Start Loop Start/Forward Disconnect Ground Start
FXS	Loop Start Loop Start/Forward Disconnect Ground Start Ground Start Immediate Ground Start Automatic PLAR D3 PLAR D4

Table D-4. APM Technical Specifications (3 of 3)

Specification	Criteria
OCU-DP APM	
Weight	
2-port OCU-DP APM	0.800 lbs. (.362 kg)
6-port OCU-DP APM	1.052 lbs. (.477 kg)
OCU-DP I/O card	0.286 lbs. (.130 kg)
Size	
OCU-DP APM	11.58 inches x 8.00 inches (29.41 cm x 20.32 cm)
OCU-DP I/O card	2.90 inches x 10.15 inches (7.37 cm x 25.78 cm)
Power Consumption (max)	
2-Port OCU	2.78 watts, 0.232 amps input current at 12 volts Result: 9.49 Btu per hour
6-Port OCU	5.04 watts, 0.420 amps input current at 12 volts Result: 17.20 Btu per hour
DDS Ports	
Standards	AT&T PUB 62310, Bellcore TA-TSY-00077, ANSI T1.410, AT&T PUB 61330, AT&T TR41458
Rates	56 kbps, 64 kbps Clear Channel, 4-wire Switched 56
Loopbacks	DS-0, OCU Line, OCU Data, OCU, Local and Remote Latching and Nonlatching DSU/CSU

Table D-5. ISDN DBM Technical Specification (1 of 2)

Specification	Criteria
ISDN BRI DBM	
DBM Interface	ISDN BRI U-interface: One 8-position modular keyed USOC RJ49C jack
Physical interface	RJ49C
Service supported	Capability Package B for 1B-channel service, or Capability Package I for 2B-channel support, NI-1 (supporting up to two B-channels)
Data rates	56 kbps and 64 kbps
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 RJ45 8-pole keyed modular plug and jack, specified in ISO/IEC 8877
Transmit Interface	
Signal Level	13.5 dBm nominal over frequency band, 0 Hz – 80 kHz
Impedance	135 Ω
Receive Interface	
Dynamic Range	Operates on 2-wire loops, defined in ANSI T1.601-1992
Impedance	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 DBM Technical Specification (2 of 2)

Specification	Criteria
ISDN PRI DBM	
DBM Interface	One 8-position modular unkeyed USOC RJ48C jack
Physical interface	RJ48C
Service supported	PRI, NI-2, ATT 4ESS, or ATT 5ESS custom (supporting up to 23 B-channels), with Circuit-Switched Data capabillity
Data rates	1.536 Kbps
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
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 (3.41 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 *Cables* on page E-4 for cables you can order.

Description	**Model/Feature Number**
FrameSaver SLV Multiservices Access (MSA) Units	
1xT1 Frame 9191 NAM with 2-slot housing and integral modem, 120 VAC power supply with power cord, and NAM I/O card. *Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9192-A1-201
1xT1 Frame 9191 NAM with 2-slot housing, an integral modem, an ISDN BRI DBM, 120 VAC power supply with power cord, and NAM I/O card. *Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9192-A1-202
1xT1 Frame 9191 NAM with 2-slot housing, an integral modem, an ISDN PRI DBM, 120 VAC power supply with power cord, and NAM I/O card. *Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9192-A1-222
1xT1 Frame 9191 NAM with 5-slot housing an integral modem, 120 VAC power supply with power cord, and NAM I/O card. *Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9195-A1-201
1xT1 Frame 9191 NAM with 5-slot housing, an integral modem, an ISDN BRI DBM, 120 VAC power supply with power cord, and NAM I/O card. *Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9195-A1-202
1xT1 Frame 9191 NAM with 5-slot housing, an integral modem, an ISDN PRI DBM, 120 VAC power supply with power cord, and NAM I/O card. *Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9195-A1-222

Description	Model/Feature Number
1xT1 Frame 9191 NAM with 5-slot housing (without bezel and chassis skin), rack-mount bracket, an integral modem, 120 VAC power supply with power cord, and NAM I/O card*. Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9195-A1-209
1xT1 Frame 9191 NAM with 5-slot housing, an integral modem, –48 and +24 VDC power supply with power cord, and NAM I/O card*. Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9195-A1-501
1xT1 Frame 9191 NAM with 5-slot housing, an integral modem, an ISDN BRI DBM, –48 and +24 VDC power supply with power cord, and NAM I/O card*. Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9195-A1-502
1xT1 Frame 9191 NAM with 5-slot housing, an integral modem, an ISDN PRI DBM, –48 and +24 VDC power supply with power cord, and NAM I/O card*. Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9195-A1-522
1xT1 Frame 9191 NAM with 5-slot housing (without bezel and chassis skin), rack-mount bracket, an integral modem, –48 and +24 VDC power supply with power cord, and NAM I/O card*. Includes network cable, COM Port-to-PC cable Installation Instructions*, *and Quick Reference*.	9195-A1-509
Network Access Module (NAM)	
1xT1 Frame 9191 NAM with integral modem and a NAM I/O card*. Includes network cable and FrameSaver SLV 9191 Multiservices NAM Installation Instructions.*	9191-B1-212
Optional Features	
ISDN BRI DBM	9098-F1-870
ISDN PRI DBM	9098-F1-875
High-Speed Synchronous Data APM	9109-F1-604
FXS Analog Voice APM – 2-Wire	9109-F1-648
FXO Analog Voice APM – 2-Wire	9109-F1-658
OCU-DP 2-Port APM	9109-F1-622
OCU-DP 6-Port APM	9109-F1-626
E&M Analog Voice APM – 4-Wire	9109-F2-668
Mounting Brackets for 5-Slot Housing	9001-F1-890
Universal 2/5-Slot Wall Mount Kit	9008-F1-893

Description	Model/Feature Number
Power Supplies	
120 VAC Power Supply (for 2-slot housing)	9002-F1-020
120 VAC Power Supply (for 5-slot housing)	9005-F1-020
DC Power Supply (for 5-slot housing)	9005-F1-050
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
2-Slot Housing	
2-Slot housing and 120 VAC power supply with power cord. *Includes COM Port-to-PC cable and 2-Slot Housing Installation Instructions.*	9002-B1-200
5-Slot Housing	
5-Slot housing and –48 and +24 VDC power supply with power cord and alarm relay connector, and filler panels. *Includes COM Port-to-PC cable and 5-Slot Housing with DC Power Supply Installation Instructions.*	9005-B1-500
5-Slot housing (without bezel and chassis skins) and –48 and +24 VDC power supply with power cord, rack-mount bracket, alarm relay connector, and filler panels. *Includes COM Port-to-PC cable and 5-Slot Housing with DC Power Supply Installation Instructions.*	9005-B1-509
5-Slot housing and 120 VAC power supply, alarm relay connector, and filler panels. *Includes COM Port-to-PC cable and* 5-*Slot Housing with AC Power Supply Installation Instructions.*	9005-B1-200
5-Slot housing (without bezel and chassis skins) and 120 VAC power supply with power cord, rack-mount bracket, alarm relay connector, and filler panels. *Includes COM Port-to-PC cable and* 5-*Slot Housing with AC Power Supply Installation Instructions*.	9005-B1-209
Printed Manual	
FrameSaver SLV Multiservices Access Unit, Models 9191, 9192, and 9195, User's Guide	9191-A2-GB20

Cables

This table lists cables you can order.

Description	Part Number	Feature Number
RJ48C T1 and DSX-1 Network Cables, RJ48C-to-RJ48C/RJ49C – 20 feet/6.1 meters	035-0209-2031	3100-F1-500
RJ49C Cable for an ISDN BRI DBM ISDN-U – 20 feet/6.1 meters	035-0209-2031	3100-F1-500
RJ48C Cable for an ISDN PRI DBM – 20 feet/6.1 meters	035-0209-2031	3100-F1-500
T1 Line Interface Cable, RJ48C-to-CA81A – 20 feet/6.1 meters *For use in Canada.*	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, Standard EIA-232 Straight-Through Cable (D-Sub9-to-DB25 for PC serial port) – 14 feet/4.3 meters	035-0313-1431	3100-F2-550
V.35 DTE Adapter (connects Port to the DTE's V.35 interface), EIA 530A-to-V.35 – 1 foot/.3 meter	002-0095-0031	3100-F1-570
COM Port-to-LAN Adapter Cable (custom unkeyed 8-pin plug-to-8-pin plug modular cable) – 14 feet/4.3 meters *Used as a LANA.*	035-0315-1431	3100-F2-910
RJ48S DDS Network Cable		
14 feet/4.3 meters	035-0267-1431	3600-F3-501
25 feet/7.6 meters	035-0267-2531	3600-F3-502
EIA-530 straight-through cable (10 feet – 3 meters)	035-0385-1031	9008-F1-523
Voice Cable – Plug-to-Plug (Amphenol plug-to-Amphenol plug, 25 pairs),		
Amphenol plug-to-Amphenol plug – 6 feet/1.9 meters	035-0320-0531	9008-F1-531
3 Amphenol plug-to-1 Amphenol plug – 25 feet/7.6 meters	035-0321-2531	9008-F1-532
Voice Cable – Socket-to-Plug (Amphenol socket-to-Amphenol plug, 25 pairs) – 25 feet/7.6 meters	035-0321-2531	9008-F1-532

Description	Part Number	Feature Number
Voice Adaptor – Plug-to-Plug		
3 Amphenol plug-to-4 Amphenol plug – 6 feet/1.9 meters	035-0318-0631	9008-F1-533
3 Amphenol plug-to-1 Amphenol plug – 6 feet/1.9 meters	035-0319-0631	9008-F1-534
M66 Block (with 2-socket 50-pin connectors)	—	9008-F1-535
DSX-1 Adapter Cable, RJ48C-to-DB15 – 1 foot/0.3048 meters	035-0386-0031	9008-F1-560

Index

Numbers

A

B

C

D

E

M

N

O

P

Q

R

T

U

V

W

Y