FrameSaver® SLV 9124

TECHNICAL REFERENCE

Document No. 9124-A2-GH30-00

May 1999

PRELIMINARY DRAFT

PARADYNE™

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Avenue North, P.O. Box 2826, Largo, Florida 33779-2826.

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 there. Select *Service & Support* → *Warranty Registration.*)
- **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

All products and services mentioned herein are the trademarks, service marks, registered trademarks or registered service marks of their respective owners.

Patent Notification

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

Contents

About This Guide

1 About the FrameSaver SLV

2 Management Control

3 Typical Applications

4 User Interface and Basic Operation

5 Using the OpenLane NMS

6 Using NetScout Manager Plus

7 Concord’s Network Health

8 Configuration

9 Security and Logins

10 Operation and Maintenance

11 Troubleshooting

A Menu Hierarchy

B IP Addressing

C SNMP MIBs and Traps, and RMON Alarm Defaults

D Cables, Connectors, and Pin Assignments

E Technical Specifications

F 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 9124, a T1 Frame Relay Service Level Verifier (SLV) unit. It is intended for system designers, engineers, administrators, and operators.

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

Document Organization

Section	Description
Chapter 1	*About the FrameSaver SLV.* Describes the 9124 service level verifier unit and its features.
Chapter 2	*Management Control.* Describes how you establish a management link and configure end-to-end management control.
Chapter 3	*Typical Applications.* Shows typical applications of the FrameSaver SLV unit in a frame relay network.
Chapter 4	*User Interface and Basic Operation.* Shows how to navigate the user interface.
Chapter 5	*Using the OpenLane NMS.* Identifies the key features of OpenLane NMS applications and describes setup and applicable windows. Also includes service-level management reports information.
Chapter 6	*Using NetScout Manager Plus.* Identifies the key features of the NetScout Manager Plus application and the minimum hardware and software required to run the applications. Also, describes setup and related windows.

Section	Description
Chapter 7	*Concord's Network Health. D*escribes setup and related windows, and identifies those reports that apply to the FrameSaver unit.
Chapter 8	*Configuration.* Provides instructions for setting up the unit, including how to enter identity information and set up the date and time on the screens. Also provides instructions for configuring the unit, along with full descriptions of each option and possible settings.
Chapter 9	*Security and Logins.* Provides procedures for controlling access to the FrameSaver SLV and setting up logins.
Chapter 10	*Operation and Maintenance.* Provides procedures to display unit identification information, and to display and interpret status and statistical information.
Chapter 11	*Troubleshooting.* Provides troubleshooting and test procedures.
Appendix A	*Menu Hierarchy*. Contains a graphical representation of how the user interface screens are organized.
Appendix B	*IP Addressing.* Provides guidelines for selecting an IP addressing scheme and shows examples of typical schemes with subnet masks assigned.
Appendix C	*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 D	*Cables, Connectors, and Pin Assignments*. Identifies cables used with the access unit and provides pin assignments for them, along with those of the connectors/interfaces.
Appendix E	*Technical Specifications*.
Appendix F	*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.*

Conventions Used

Convention Used	When Used
Italic	To indicate variable information (e.g., DLCI *nnnn*) or model-specific information (e.g., *9124 only*).
Menu sequence:	To provide an abbreviated method for indicating the selections to be made from a menu or selections from within a menu before performing a procedural step. For example, *Main Menu→ Status→ System and Test Status* indicates that you should select Status from the Main Menu, then select System and Test Status.
(Path:)	To provide a check point that coincides with the menu path shown at the top of the screen. Always shown within parentheses so you can verify that you are referencing the correct table (e.g., Path: main/config/alarm).
Brackets [ ]	To indicate multiple selection choices when more than one selection is available (e.g., *Performance Statistics→ Status→ [Network/Port-1]*).
Text highlighted in red	To indicate a hyperlink to additional information. Click on the highlighted text (e.g., clicking on *Performance Statistics* in Chapter 10 takes you directly to the *Performance Statistics* section in Chapter 10, *Operation and Maintenance*.

Product-Related Documents

Document Number	Document Title
Paradyne FrameSaver Documentation:	
9124-A2-GN10	*FrameSaver SLV 9124 Installation Instructions*
9124-A2-GL10	*FrameSaver SLV 9124 Quick Reference*
Paradyne OpenLane NMS Documentation:	
7700-A2-GB23	*OpenLane DCE Manager for HP OpenView for Windows User's Guide*
7800-A2-GB26	*OpenLane DCE Manager User's Guide*
7800-A2-GB28	*OpenLane Performance Wizard User's Guide*
NetScout Documentation:	
2930-170	*NetScout Probe User Guide*
2930-610	*NetScout Manager/Plus User Guide*
2930-620	*NetScout Manager/Plus & NetScout Server Administrator Guide*
2930-788	*NetScout Manager Plus Set Up & Installation Guide*
Concord Communications Documentation:	
09-10010-005	*Network Health User Guide*
09-10020-005	*Network Health Installation Guide*
09-10050-002	*Network Health – Traffic Accountant Reports Guide*
09-10070-001	*Network Health Reports Guide*

Contact your sales or service representative to order product documentation.

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

To request 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

Overview

The FrameSaver® SLV (Service Level Verifier) system consists of:

- FrameSaver SLV 9124 units
- OpenLane™ NMS applications for Unix or Windows
  - — DCE Manager and/or
  - — Performance Wizard, with Diagnostic Wizard and Service Level Management Reports
- NetScout Manager Plus application
- Standalone NetScout Probes, if needed

This system provides increased manageability, monitoring, and diagnostics so customers can identify problems more efficiently, troubleshoot those problems faster, and maximize their network to control costs.

It provides everything needed to effectively and economically monitor network service levels:

- Ability to track protocols being used in the network and display their bandwidth consumption rates, with the ability to adjust the frame relay network so traffic will run smoothly.
- Ability to track network usage down to the node level so users generating excessive traffic can be identified.
- Ability to determine when traffic will be the heaviest, so bandwidth can be adjusted for greater network efficiency during high-traffic periods.
- Ability to monitor traffic at multiple levels so capacity requirements and major network changes can be planned.
- Service-level reporting for network performance as well as specific failures, real-time as well as network-wide reporting.
- Intelligent service-level verification that accurately analyzes instantaneous burst and dropped packets, not averages, and verifies SLAs (service-level agreements).

Plus:

- RMON-based (remote monitoring-based) performance monitoring for network optimization and planning.
- Advanced frame relay diagnostic and management tools for maximum network availability.

The FrameSaver SLV unit's unique PVC multiplexing capability, referred to as embedded DLCIs (EDLCIs), reduces the number of frame relay ports required and permits multiple data streams to share a single PVC. Used in conjunction with the OpenLane and NetScout Manager Plus NMS applications, the system provides a unique solution for measuring network performance that is proactive and integrated and is applicable to both end user and service provider frame relay management needs.

For service providers, implementing this solution differentiates services provided while reducing deployment and maintenance costs. In addition, fewer provisioning and security problems will occur since extra DLCIs do not have to be configured for management data and the data does not have to go through a customer's router.

FrameSaver SLV Features

The FrameSaver SLV product is a single, flexible, and standards-based frame relay monitoring solution that provides the following features:

- **Interoperability with other FrameSaver Units.** Operates with FrameSaver 9120/9620s; FrameSaver SLV 9124/9624s, 9126/9128s, and the international 9820-C/9820s.
- **IP Connectivity.** Supports connectivity within an IP (Internet Protocol) network for up to 300 IP routes to provide IP routing for SNMP, Telnet, and FTP messages.
- **Standards-Based Protocol Support.** Supports two link-layer protocols for connection to an external SNMP manager or network device via the COM or modem port, and the three standard LMI protocols for communication over the frame relay interface.
- **Frame Relay Aware.** 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 NextEDGE system'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.
- **Maximum PVCs, EDLCIs, and Management PVCs.** The number of remote sites and PVCs that can be created for each FrameSaver SLV 9124 is summarized in the following table.

Feature	Central Site FrameSaver SLV 9124	Remote Site FrameSaver SLV 9124
Remote Connections (PVCs)	120	64
Remote Management Connections (EDLCIs)	122	66
Dedicated Management PVCs	2	2

- **Intelligent Service Level Verification.** Provides Quality of Service (or QoS) features for determining whether service level agreements (SLAs) are being met and whether the network or the customer's data is the cause of missed SLAs. Actual service level agreement parameters and thresholds for service level verification can be configured.

- **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. These ratios are available through OpenLane Performance Wizard's service level management reports.
- **Auto-Configuration**. Provides the following automatic configuration features:
  - — Frame Relay Discovery – For automatic discovery of network DLCIs and configuration of a data port DLCI, the PVC connection, and a management PVC, which is multiplexed with user data DLCIs.
  - — Time Slot Discovery – For automatic discovery of network time slots and configuration of corresponding time slots in the system.
  - — LMI Protocol Discovery – For automatic configuration of the protocol being used by the network.
- **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 a complete view of the network's and a data port's performance through the statistical data collected: SLV, DLCI, frame relay, and DBM call statistics.

  All the data collected for a specified interval is stored in a bucket. Two default intervals are used: 15 minutes and one day. Using these intervals, the system can collect, display, and store 24 hours of 15-minute buckets (96 buckets) and five 24-hour data buckets simultaneously, providing up to five days of daily statistical totals. These intervals can be changed using the NetScout Manager Plus application.
- **User-Selectable Ranges for Frame and Burst Sizes**. Provides user configurability for statistical data collection using OpenLane DCE Manager to set upper and lower limits for data collection. The accumulated data is used for graphs and reports, and to trigger alarms.
- **Extensive Testing Capability.** Provides a variety of tests to identify and diagnose device, network, and PVC problems with continuous and nondisruptive background latency testing, unique nondisruptive frame relay diagnostics for troubleshooting and testing DLCIs, and local/remote line speed reporting to identify rate mismatches. The following are provided:
  - — DLCI tests: PVC loopback, send/monior pattern, and connectivity. All are nondisruptive to data when between NextEDGE and FrameSaver devices.
  - — Physical interface tests: various local and remote loopbacks, and send/monitor pattern tests. For voice APMs, test tones and force/monitor signaling are also provided.
  - — IP PING and Self-test

  These tests can be commanded from the system's menu-driven user interface, OpenLane Performance Wizard's Diagnostic Wizard, and OpenLane DCE Manager (using SNMP MIB test commands). The IP PING and self-test cannot be run using DCE Manager.

- **Dedicated Troubleshooting PVC.** Provides a troubleshooting management link that helps service providers isolate problems within their network. This feature can be configured.
- **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.
- **Security.** Provides multiple levels of security to prevent unauthorized access to the system, which include requiring logins, disabling a remote access method, specifying community names and access types, and authorizing NMS IP addresses and access type.
- **Router-Independence.** Unique diagnostics, performance monitoring, PVC-based in-band network management, and SNMP connectivity is not dependent upon external routers, cables, or LAN adapters.
- **Inverse ARP and Standard RIP Support.** Provides Inverse ARP (Address Resolution Protocol) support so the frame relay router at one end of a management PVC can acquire the IP address of a FrameSaver unit at the other end of the PVC. Standard RIP (Routing Information Protocol) allows the router to automatically learn the routes to all FrameSaver units connected to that FrameSaver unit.
- **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 unit is up and running. Two software loads can be stored, to be implemented at the user’s discretion.
- **DSX-1 Drop/Insert Port.** Allows DTEs/PBXs that support the DS1 signal format to share the T1 network with other high-speed equipment so that voice traffic can share the same local access circuit as the frame relay data.
- **Two Customer-Specified Configuration Storage Areas.** Allows 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.
- **Back-to-Back Operation.** Allows two NextEDGE/FrameSaver units to be connected via a network crossover cable so a point-to-point configuration simulating a leased line environment can be simulated.
- **Network Management Support.** Operates and is compatible with OpenLane, NetScout, and Concord Communications products.

The OpenLane Management Solution

FrameSaver SLV units are managed by Paradyne's preeminent OpenLane network management solution for Unix or Windows-based systems. The OpenLane solution consists of the following applications:

- DCE Manager
- Performance Wizard with Diagnostic Wizard

OpenLane DCE Manager

This application is a powerful management system that runs from an HP OpenView console, and provides a real-time view of network and device statuses.

Some of its features include:

- Plug-and-play device discovery, full awareness of PVCs, and database-level integration into HP OpenView.
- Device identification and access to detailed health and status, alarms, tests, etc., information.
- Level 1 and 2 physical and logical frame relay monitoring and diagnostics (loopbacks).
- Enhanced SNMP trap processing to ensure that network trap icons reflect the alarm on the device.
- Real-time graphical representations of the device and all its interfaces.
- Device configuration.
- Telnet access to devices.

OpenLane Performance Wizard

OpenLane Performance Wizard is an advanced performance monitoring application that provides real-time and historical data collection for determining network performance and service level verification. This application gathers network performance data from a FrameSaver SLV unit's user-history collection buckets to provide an accurate view of network traffic at any time.

Some of its features include:

- Java-based, for operating system flexibility (it runs on UNIX or Windows).
- Real-time graphical displays of service level verification parameters – latency, availability, and frame delivery ratios (which includes the ability to report accurate measurements of dropped frames transmitted above or within CIR (Committed Information Rate).

  Real-time displays include PVC throughput, data delivery analysis, transmit burst analysis, frame size distribution, physical link performance, network utilization, diagnostics, and congestion data.
- Web-based daily, weekly, and monthly reports designed to verify frame relay service level agreements.
- Automatic end-to-end PVC discovery and configuration to eliminate or minimize manual configuration and operator intervention.
- Enhanced navigation, with the intuitive standard folder concept (automatically creates folders that group devices) for network partitioning and circuit name identification, and search utilities for finding devices by their name.
- Enhanced diagnostic capabilities, with loopback and PVC testing.

NetScout Manager Plus

This application supports FrameSaver SLV units and NetScout Probes with complete LAN and WAN traffic analysis and monitoring functions. NetScout Manager Plus provides the following features for FrameSaver SLV units:

- Configurable thresholds for RMON 1 alarms and events.
- Performance monitoring using collected RMON 2 data.
  - Protocol Directory and Distribution functionality allows FrameSaver SLV units to measure up to eleven network-layer protocols and report the amount of traffic generated by each.
  - IP Top Talkers and Listeners reporting identifies the devices using network bandwidth. The network's top six users are identified.
  - User history buckets to collect performance statistics from FrameSaver SLV units. 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.

NetScout Probes

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

Management Control

2

This chapter contains customer end user and service provider management overviews, followed by the steps needed to provide local and remote management connectivity to the FrameSaver unit.

You need to select and configure:

- A method of local management connectivity for FrameSaver units.
- A method for end-to-end management connectivity across the network.
- An IP addressing scheme that fits the local and end-to-end management connectivity methods.

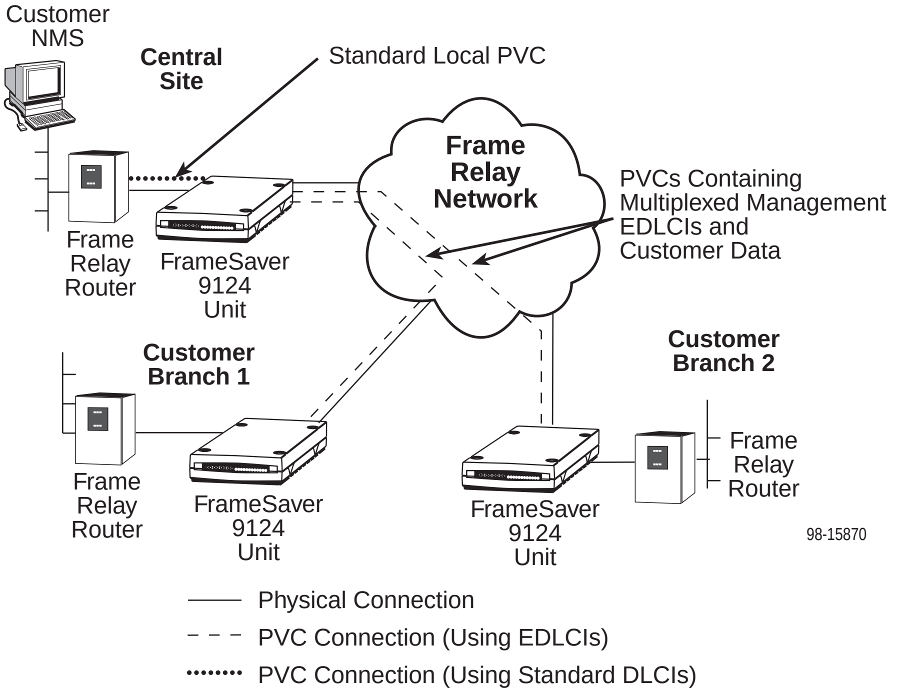
Examples illustrating various network configurations are included in each section.

- *Customer End User Management Overview* on page 2-2.
- *Service Provider Management Overview* on page 2-3.
- *Managing the FrameSaver Unit* on page 2-4.
- *Configuring Local Management Control* on page 2-4.
- *Configuring End-to-End Management Control* on page 2-7.

Customer End User Management Overview

The optimal method for managing an end-user network is shown in the example below. Using this method saves PVC charges because management data is multiplexed with customer data using a single PVC.

By accessing the remote units in-band, the remote units are not router-dependent, so trouble isolation is easier when there are LAN outages.

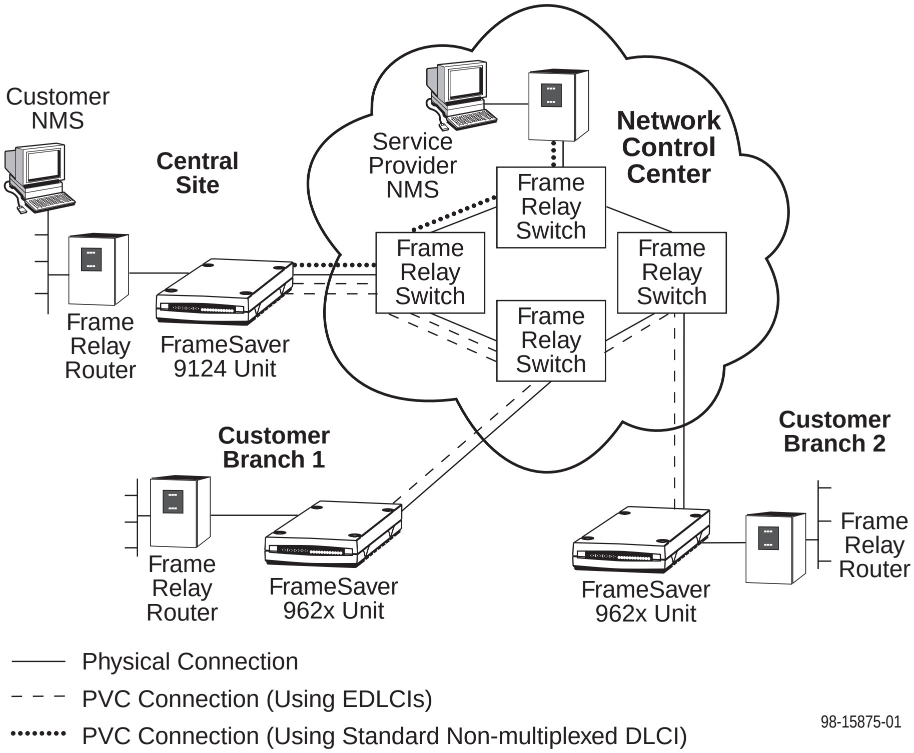


For details configuring in-band management links to the central and remote site FrameSaver units, see *Configuring Management PVCs* in Chapter 8, *Configuration Options*.

Service Provider Management Overview

In the service provider example below, the service provider’s management data is multiplexed with the customer data using EDLCIs traveling between the customer’s central site and the customer branches.

A dedicated DLCI is configured from the customer’s central site to the service provider’s network control center, so the customer’s entire network can be managed from the service provider’s network operation/control center using a single DLCI. This dedicated DLCI carries only management data; no customer data is carried.



The service provider’s diagnostic capabilities are greatly enhanced using this topology. Service provider troubleshooting and management of the customer’s network is completely independent of the customer’s routers. PVC Loopbacks and Pattern tests can be performed without disrupting customer data.

Managing the FrameSaver Unit

Local management is accomplished through the following methods:

- DTE port configured with a frame relay management PVC, with the router providing RFC 1490 or Cisco encapsulation of the IP traffic.
- COM port configured as a terminal for access to the menu-driven async user interface using a VT-100 async terminal or compatible terminal or PC.
- COM port connected to the manager or router for an IP management link using either PPP or SLIP as the link layer.
- COM port connected to an external LAN adapter for Ethernet connectivity for an IP management link.

Remote management is accomplished via the following methods:

- Merging or multiplexing management data with user data, and transferring the information over a specified network PVC.
- Dedicated frame relay PVC between FrameSaver units at each end of the circuit for in-band management. This is required when communicating with non-FrameSaver equipment.
- Management PVCs configured between DTE ports and RFC 1490-compliant or Cisco encapsulation routers at one or both ends of the circuit to route management and user data through the same port to the routers.

Configuring Local Management Control

Local management methods are typically used at the central site or at large regional sites, where the FrameSaver unit is colocated with the NMS. This is illustrated in the *Customer End User Management Overview*, page 2-2.

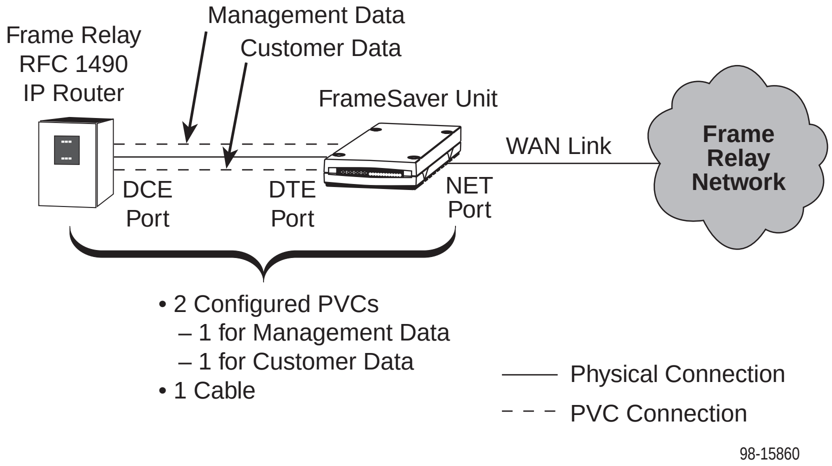
When managing the FrameSaver unit locally, you can establish a management link by:

- *Creating a Management DLCI Between the Router and Unit Via the DTE Port* on page 2-5.
- *Creating a Separate Management Link Via the COM Port* on page 2-6.

Creating a Management DLCI Between the Router and Unit Via the DTE Port

The following configuration shows the management connection using an RFC 1490-compliant or Cisco frame relay IP router connected to the FrameSaver unit's user data port.

As shown below, in-band management is accomplished through the dedicated PVC between the frame relay router or FRAD and the FrameSaver unit.



In this configuration, the FrameSaver unit depends on the router for management connectivity. User data PVCs share the same port as the management PVC. No additional cables need to be purchased.

NOTE:

The router to be used for management must configure a local PVC between the router and the FrameSaver unit to support RFC 1490 or Cisco encapsulation. Typically, this is done using a map or subinterface statement on the router. If the FrameSaver unit is located with the NMS at the central site and in-band management through the frame relay network is desired to manage remote site units, map statements must also be added to the router for the remote units.

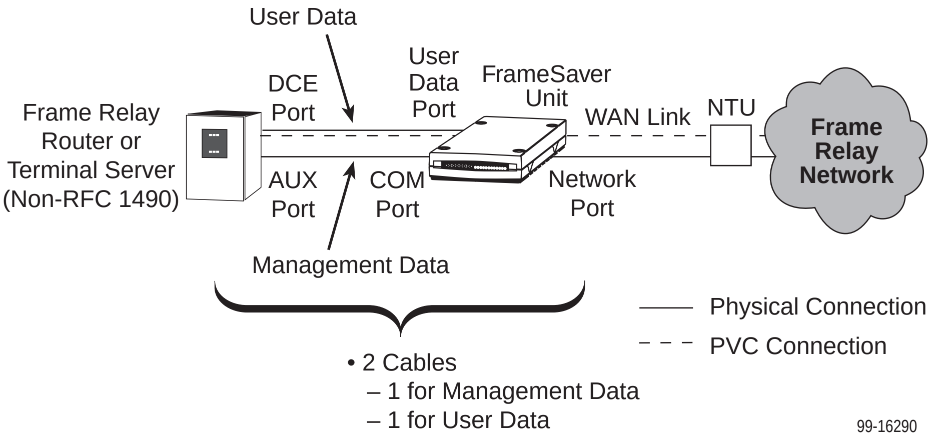
Depending upon the router, a single subinterface statement using a subnet may be used instead of multiple map statements. The subinterface method assumes that all the FrameSaver units are on a different subnet than the endpoint routers.

See the Primary Link RIP options in Table 8-12, Management PVC Options, in Chapter 8, *Configuration Options*, for additional Inverse ARP and Standard RIP information.

Creating a Separate Management Link Via the COM Port

A dedicated PVC can be configured to carry customer data over the DTE port, while management data is carried over the COM port. The illustration below shows a management link connected to the COM port for local access to a non-RFC 1490 router. The router must have an asynchronous interface running PPP or SLIP link-layer protocol.

When the COM port is configured as the IP management link, the async user interface is accessible via Telnet. Once the interface is configured, it operates like an IP interface so it can be PINGed, used for SNMP, Traps, FTP, and Telnet. Although not shown in the illustration below, an external LAN adapter can be connected to the COM port to provide Ethernet connectivity.



The Communication Port options should be configured for a separate (out-of-band) management link:

> *Main Menu→Configuration→Management and Communication→Communication Port*

See Table 8-17, Communication Port Options, in Chapter 8, *Configuration Options*, for information about the Communication Port options.

NOTE:

When Port Use is set to Net Link on the COM Port, the RIP option must be disabled (set to None) to prevent user data from traveling across the management link.

When the communication (COM) port is configured as the IP management link, the async user interface is accessible through Telnet. See Table 8-14, Telnet and FTP Session Options, in Chapter 8, *Configuration Options*, for information about the Telnet options.

Configuring End-to-End Management Control

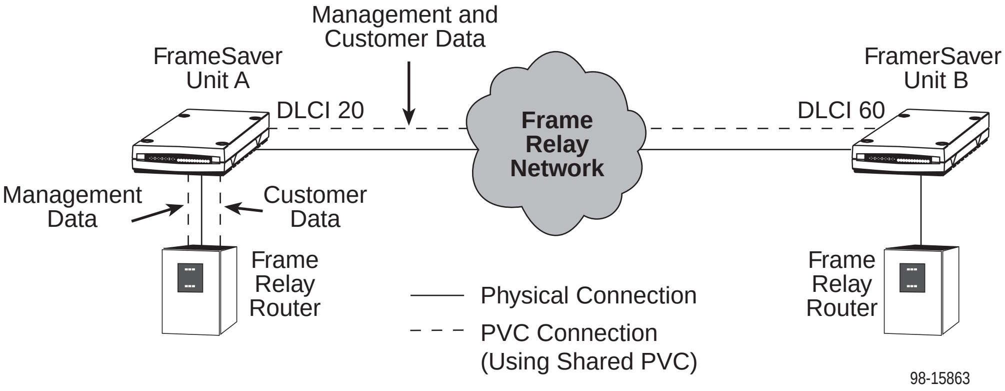
End-to-end management control methods are typically used for accessing remote site units that are not colocated with the NMS. When managing the FrameSaver unit remotely, you can establish a management link across the network in one of three ways. You can:

- Use a shared PVC (embedded DLCI).
- Use a dedicated DLCI or PVC.
- Use RFC 1490 routers for transparent management control.

Management Control Using PVC Multiplexing (EDLCI)

This is the preferred method for accessing remote site units that are not co-located with the NMS.

In the configuration below, the FrameSaver unit's management data is multiplexed with customer data onto a single PVC, sharing the same PVC – source DLCI 20 to destination DLCI 60. There is one configured PVC through the network – a shared PVC for management and customer data.



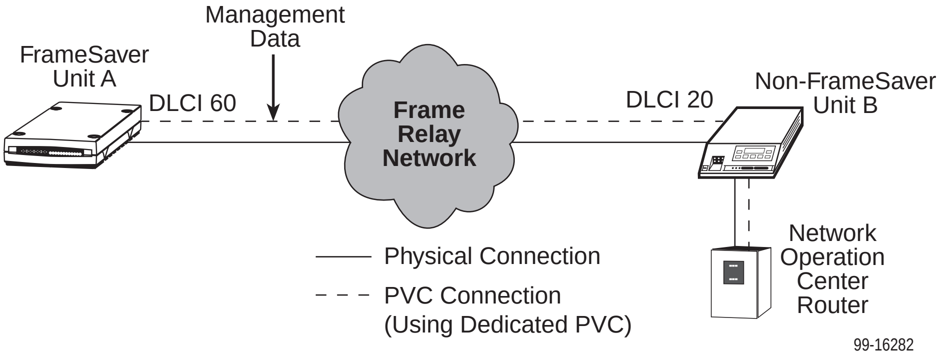
If using this method to access remote sites, map or subinterface statements must be added to the router at the central site to ensure that management traffic destined for the remote site units is routed to the FrameSaver unit at the central site by the router. Once traffic gets to the central site FrameSaver unit, it is rerouted to the appropriate remote site FrameSaver units.

If desired, higher priority may be given to DLCIs carrying customer data. When configuring an embedded DLCI (EDLCI) for management data, the DE (discard eligible) bit may be set. When there is traffic congestion, the network first discards the management data since they are already marked discard eligible.

Management Control Using a Dedicated DLCI

Management control through a dedicated DLCI is typically used by service providers to provide a single point of access (i.e., a standard, nonmultiplexed DLCI), usually to the customer's central site unit, to manage the customer's network. See *Service Provider Management Overview* on page 2-3 for a typical service provider configuration.

Nonmultiplexed DLCIs must be used when in-band management communication is desired between any non-FrameSaver unit and a FrameSaver unit.



As shown in the example, in-band management is accomplished through the dedicated PVC between the two units. Management data for non-FrameSaver Unit B goes to FrameSaver Unit A first, which then routes it into the dedicated PVC between the two units. Only management data is carried over the PVC – source DLCI 60 to destination DLCI 20.

If using this method to access remote sites, map or subinterface statements must be added to the router at the central site to ensure that management traffic destined for the remote site units is routed to the FrameSaver unit at the central site by the router. Once traffic gets to the central site FrameSaver unit, it is rerouted to the appropriate remote site FrameSaver units.

NOTE:

The router to be used for management must configure a local PVC between the router and the FrameSaver unit to support RFC 1490 or Cisco encapsulation. Typically, this is done using a map or subinterface statement on the router. If the FrameSaver unit is located with the NMS at the central site and in-band management through the frame relay network is desired to manage remote site units, map statements must also be added to the router for the remote units.

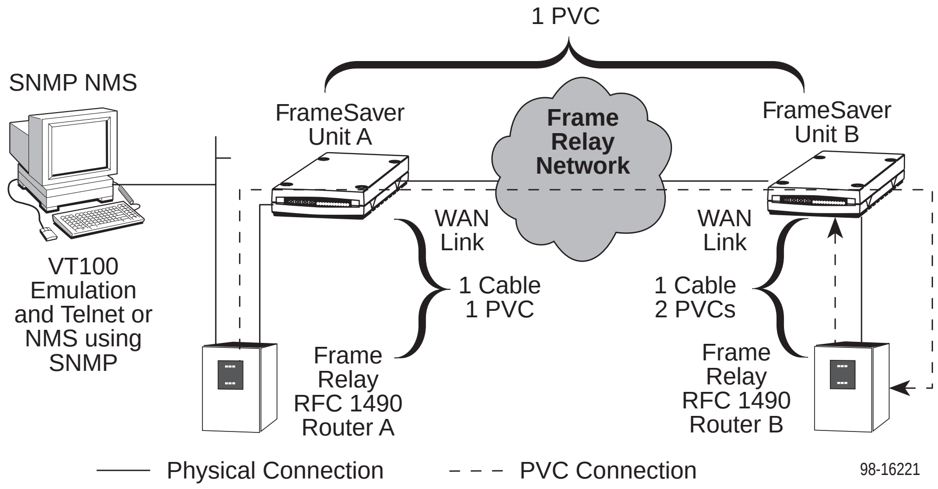
Depending upon the router, a single subinterface statement using a subnet may be used instead of multiple map statements. The subinterface method assumes that all the FrameSaver units are on a different subnet than the endpoint routers.

See the Primary Link RIP options in Table 8-12, Management PVC Options, in Chapter 8, *Configuration Options*, for additional Inverse ARP and Standard RIP information.

Transparent Remote Management Control Using RFC 1490 Routers

FrameSaver unit A can be managed locally via in-band management channels using a frame relay PVC that is configured on its DTE port. When managing the FrameSaver unit B remotely, FrameSaver unit A does not route IP traffic to FrameSaver unit B. Instead, IP traffic is transparently passed through FrameSaver unit A as part of customer data. The router then routes the management data back to FrameSaver unit B on the dedicated management DLCI configured between the router and the DTE port of the FrameSaver unit.

The configuration below shows both local and remote management across the network. Management data is being routed from frame relay Router A to IP Router B, then being redirected by the router to FrameSaver Unit B. Both management and customer data are carried over the same PVC; a separate, dedicated management PVC is not required.



NOTE:

This is not an optimum method due to router-dependency at the remote site, which can make fault isolation more difficult when there is a LAN or router failure.

Typical Applications

3

This chapter includes the following information:

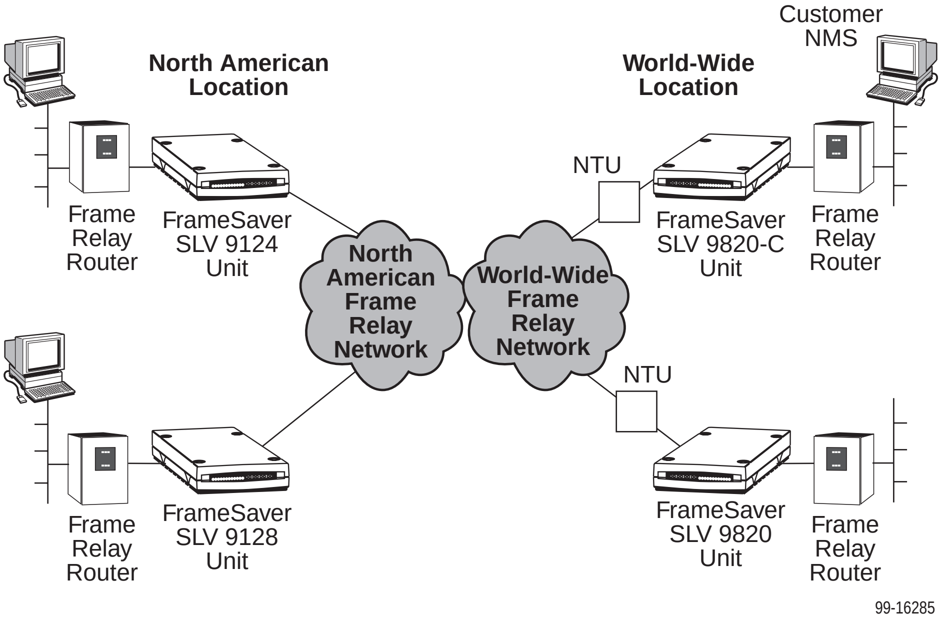
Multinational Frame Relay Solution

For multinational applications, North American FrameSaver SLV units can be teamed with FrameSaver 9820-C and 9820 units to provide a complete, end-to-end, global frame relay management solution for international companies.

This solution benefits:

- North American-based companies with international locations that are used to intelligent diagnostic and service-level verification features in their frame relay networks
- International companies can expand globally
- Multinational North American-based companies with international locations
- International companies with branches in North America

The illustration below shows this application.

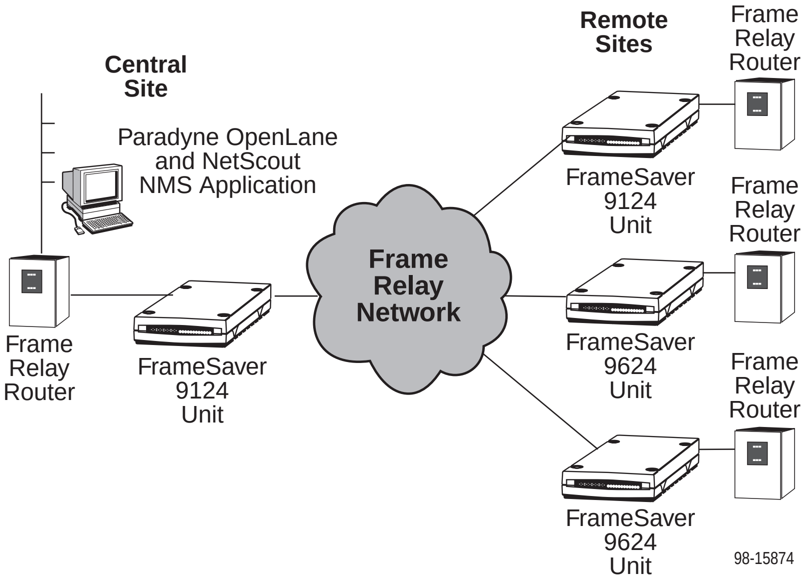


SLV Frame Relay Access

Typical remote monitoring (RMON) applications include a:

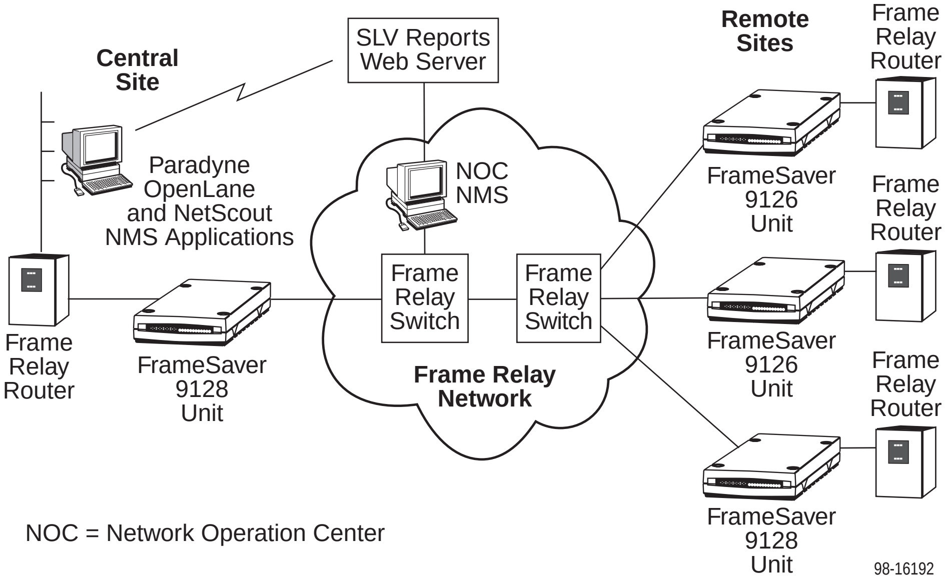
- FrameSaver SLV units with RMON capability at the central and remote sites using FrameSaver SLV 9124 and/or 9624 units, or
- Full NetScout RMON probes at the central sites and using FrameSaver 9124 units at regional and remote sites.

The SLV (Service Level Verifier) application shown below provides RMON capability at the central site and remote sites. This capability provides Physical, Frame Relay, and Network layer protocol statistical buckets for remote troubleshooting and frame relay SLV monitoring.



When the FrameSaver unit detects a failure, the unit proactively notifies the management station so the management station can actively monitor network conditions.

OpenLane Performance Wizard provides service providers or commercial end users and their customers with SLV reports through the World Wide Web. The NOC's (network operation center's) OpenLane management system must have access to the frame relay network so the system needs to be is inside the network service provider's protective firewall. The SLV Reports Web server, which is outside the firewall, enables communication with the customer Web browser and authenticates customer logins for access to SLV data. This is shown in the example below.



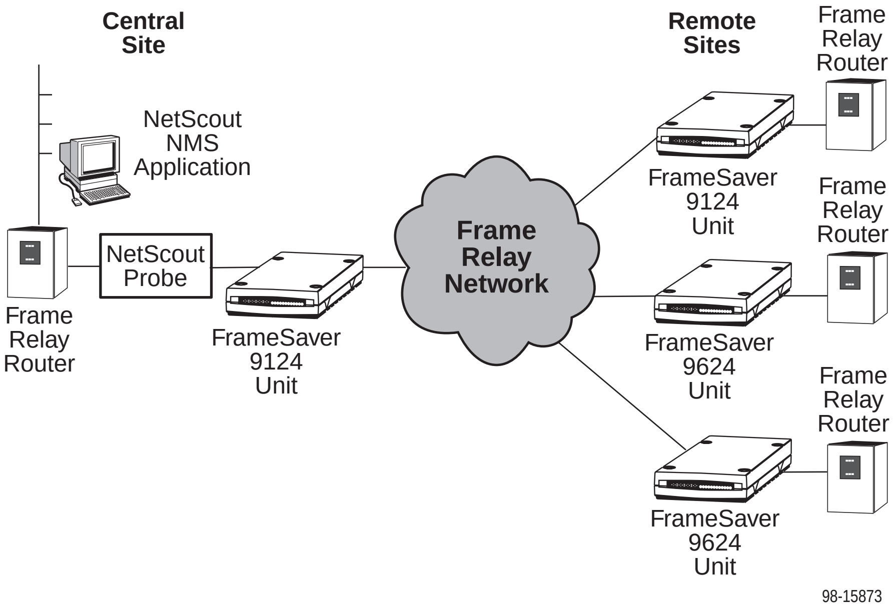
NOC = Network Operation Center

Customer access to SLV data is through a standard Netscape or Microsoft Web browser. The customer's profile, which contains the login information and specifies the device IP addresses that the customer is authorized to view, prevents unauthorized access to the SLV data. The customer enters the URL for the customer's subdirectory, enters the appropriate login, and selects a report.

See *Creating OpenLane Service Level Management (SLM) Reports* in Chapter 5, *Using the OpenLane NMS*, for information about these reports.

If LAN probing, application layer probing, or packet capture capability is desired, a NetScout probe can be used in conjunction with a FrameSaver 9124 at the central site.

In the example below, the FrameSaver 9124 is connected to NetScout's probe, which is using NetScout's NMS application to provide full probe capability at the central or regional site.

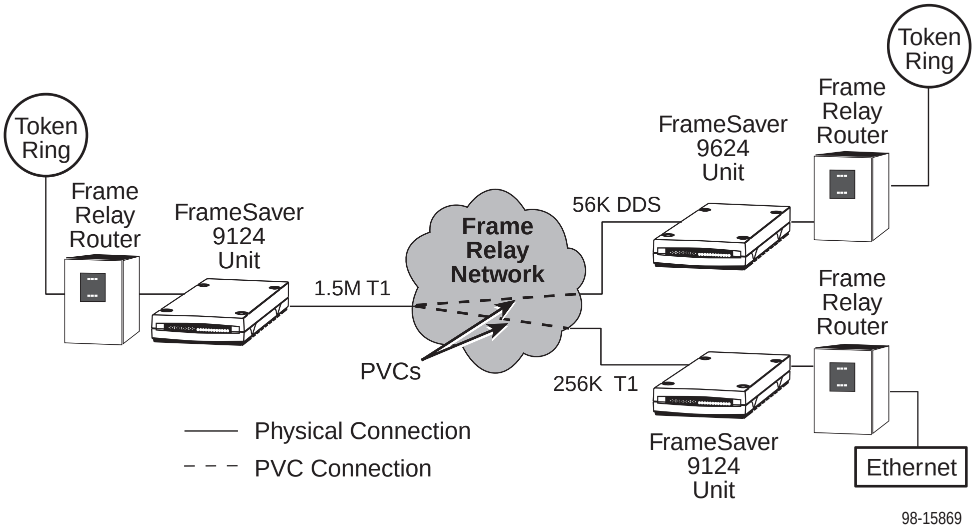


Diagnostic and statistical information is continuously collected every 15 minutes for 24 hours by the FrameSaver SLV units, with daily totals for up to 5 days. This information continues to be collected, even when frequent communication with the management station is not possible or desired due to bandwidth restrictions or network outages. As a result, the NMS application does not have to use networking bandwidth and CPU time to repeatedly query the remote FrameSaver unit for information, reducing network load and maximizing use of the information collected.

FrameSaver units can also respond to multiple managers, and each manager can pick and choose from the information collected, selecting and collecting only the information that is important to them through internal thresholds in the NetScout NMS.

Access to Frame Relay Network

The following configuration shows typical access to the frame relay service using FrameSaver SLV units or fractional T1, with each FrameSaver unit connected to a frame relay router.



In this example, the FrameSaver units use their physical connection to the T1 or DDS network to gain access to the frame relay network via logical PVC connections.

FrameSaver 9624 units operate at 56 kbps full-duplex (as shown), or 64 kbps clear-channel operation when available in an area. Access to the DDS network is through the unit's RJ48S interface.

Using FrameSaver 9124 units fractional T1, T1 access to the frame relay service is through a frame relay router connected to each FrameSaver unit. Using their physical connection to the T1 network, the FrameSaver units gain access to the frame relay network via logical PVC connections. Access to the T1 network is through the unit's RJ48C interface.

The application configurations in the following sections show this access.

Mixing FrameSaver Units in Applications

Deciding which frame relay FrameSaver unit is needed at a central or remote site is a matter of evaluating the site's traffic volume to determine the amount of network access required – FT1/T1 or 56/64 kbps.

A large central site's requirement for high-speed and high-volume indicates the need for a FrameSaver 9124 unit at this site. Connecting a RMON probe to the FrameSaver unit and using NMS application software that supports RMON MIBs will provide full remote monitoring capability at the site.

However, the amount of traffic at a remote or central site may not require the speed of T1, and FrameSaver 9624 units can be used.

In addition, not all remote sites need to have the same frame relay FrameSaver unit. They can have:

- All FrameSaver 9624 units at the remote sites.
- FrameSaver 9124 units providing voice service (e.g., SDN, Megacom, etc.) at some remote sites and FrameSaver 9624s at others.
- FrameSaver 9124 or 9624 units at remote sites where RMON is desired or needed, and FrameSaver 9120s at other remote sites. However, using non-SLV units like 9120s instead of SLV units eliminates any benefits that are gained by using a FrameSaver 9124 or 9624.

NOTE:

The additional capabilities provided by FrameSaver SLV units include:

— Intelligent latency and delivery verification.

— TruePut data delivery.

— RMON data collection and SLV reporting.

— Configurable alarm thresholds and custom history buckets.

— Interoperability with NetScout applications.

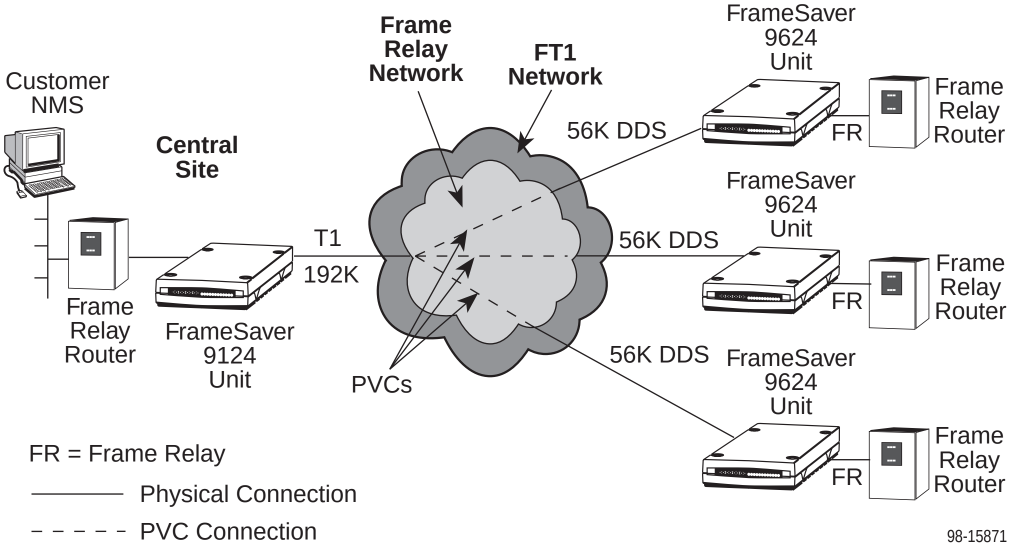
As a result, mixing SLV and non-SLV units is not recommended even though FrameSaver SLV units support non-SLV FrameSaver units.

Using All 9624 FrameSaver Units at Remote Sites

One of the most common and practical applications for frame relay FrameSaver units is to use a FrameSaver 9124 unit at the central site and FrameSaver 9624 units at most remote sites.

The example below shows this application.

- At the central site, the FrameSaver 9124 with increased memory supports up to 120 remote sites; the standard FrameSaver 9124 supports up to 64 remote sites. In typical applications, a circuit-multiplexed PVC is expected from each remote unit containing a PVC from the data port, plus a PVC for management.
- At remote sites, two DLCIs from each FrameSaver unit are aggregated onto one PVC going through the frame relay network to the central site. Each unit's multiplexed PVC contains one DLCI from its data port and one DLCI for management.

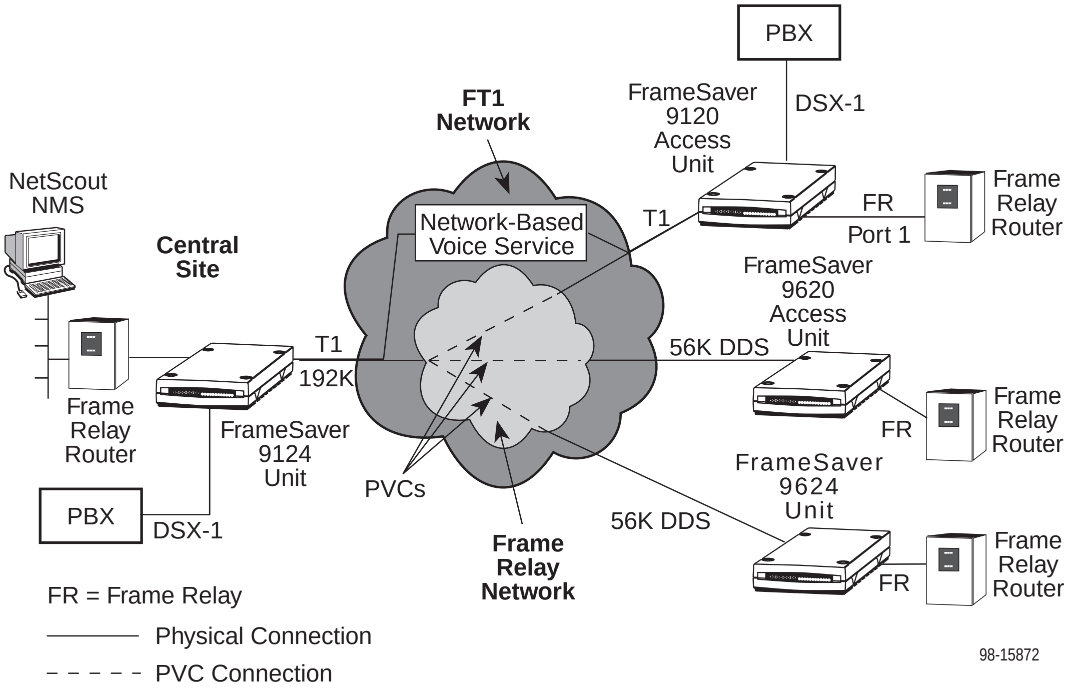


This PVC multiplexing is a patented method that provides the ability to multiplex frame relay frames coming from multiple DLCIs onto a single DLCI, sharing a single PVC connection.

Mixing 912x and 962x FrameSaver Units at Remote Sites

Not all remote sites need to be equipped the same. For example, there can be all FrameSaver 9624 units at the remote sites, or there can be a mix of FrameSaver products.

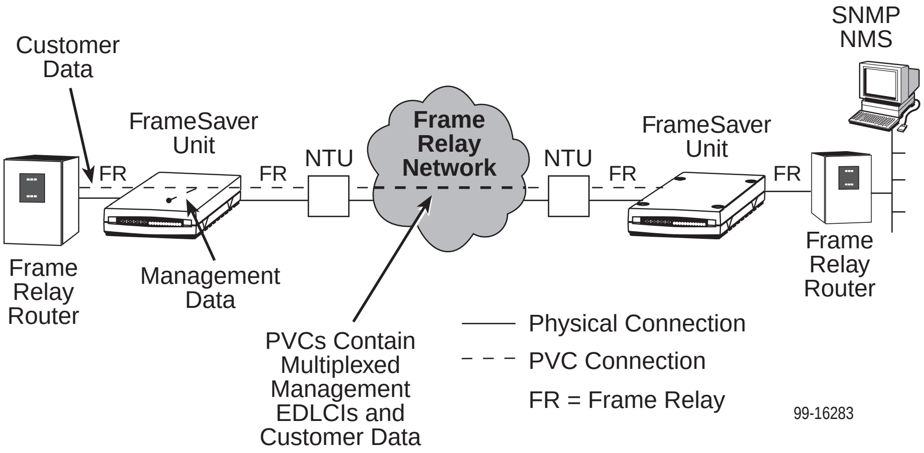
The example that follows illustrates this. It shows two remote sites supporting data-only service, one using a FrameSaver 9624 or 9620 unit and one site providing voice service, as well as remote monitoring using a FrameSaver 9120 or 9124.



In this illustration, the remote site shown as a 9120 unit can be a 9124, as shown in the *SLV Frame Relay Access* on page 3-3.

PVC Multiplexing Application

When FrameSaver units are at each end of the circuit, the FrameSaver unit provides the ability to multiplex data of multiple DLCIs onto a single network DLCI. This feature is referred to as *PVC multiplexing*. PVC multiplexing allows PVC diagnostic tests to be run without disrupting data, and uses the following network configuration.



The example shows frame relay data coming in over Port-1, with the frames being multiplexed onto a single network connection. PVCs are aggregated in the same manner.

This sharing of PVCs (i.e., multiplexing user DLCIs with management data/frames with user data/frames) is a proprietary method that is patented. When using this method:

- The first EDLCI, EDLCI 0, is used for the Port-1 data, and no overhead is associated with the multiplexing for EDLCI 0. Subsequent DLCIs have two bytes of overhead associated with them.
- A diagnostic EDLCI, which is transparent to the user, is also created on each multiplexed DLCI on the network interface. This allows nondisruptive PVC diagnostic tests to be run, as well as end-to-end communication of network latency, topology, and data delivery information.
- A management EDLCI, EDLCI 2, is created to route management data through the network interface. This allows for nondisruptive multiplexing of management data with user data and provides router-independent management of remote units.

To use this feature, the network DLCI Type must be Multiplexed.

Using Auto-Configuration

When the Frame Relay Discovery feature is used, DLCI configuration and PVC connection occur automatically. Based upon the network LMI status response message, the FrameSaver unit "discovers" network DLCIs and captures the network's CIR (committed information rate), provided the network switch supports this feature (e.g., Stratacom switch DLCI plus CIR). Network and Port interface DLCIs with the same number are created and connected automatically.

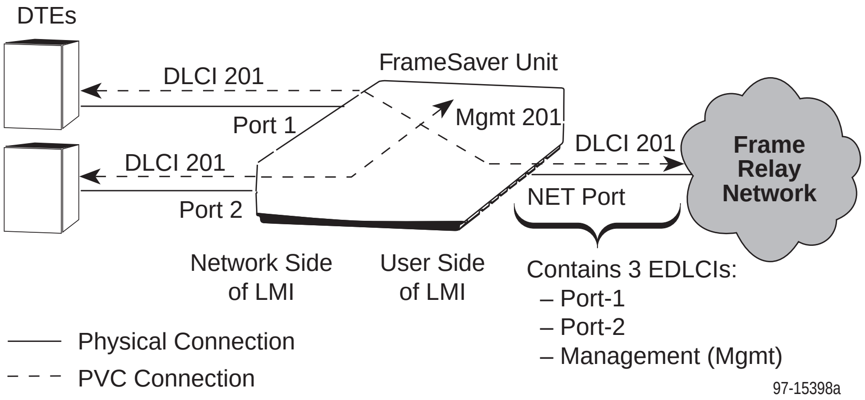
All automatically-configured DLCIs are multiplexed, with a management diagnostic EDLCI (embedded DLCI) being created. When management PVCs are multiplexed with user data PVCs, two DLCIs are created from the network DLCI, one matching DLCI for user data on Port-1, and another for management (Mgmt) information.

If the unit at the other end is *not* a FrameSaver unit, PVC diagnostic tests and SLV communication between FrameSaver units are disruptive to user data. PVCs configured for non-Paradyne units should not be multiplexed. This is because only FrameSaver models currently support PVC multiplexing and PVC diagnostics.

The following illustrations show the DLCI records and PVC connections created when a particular Frame Relay Discovery Mode is selected. The tables show the automatic configuration that takes place within the FrameSaver unit.

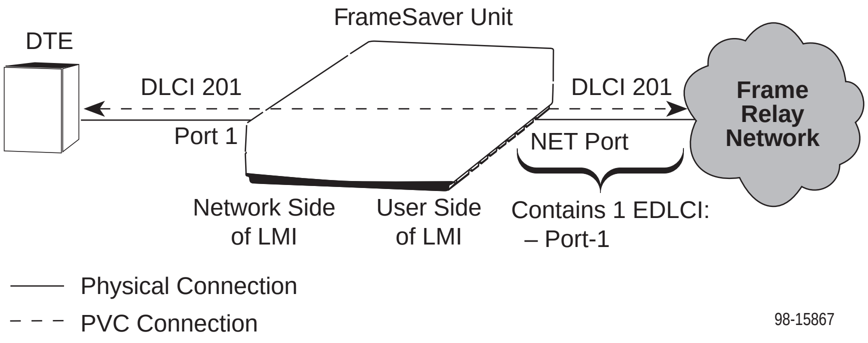
Refer to *Setting Up Auto-Configuration* in Chapter 8, *Configuration*, for additional information.

This example shows the 1-port management application (1MPort).



FR Discovery Mode Selection	Source Interface	Source DLCI	Destination Interface/Link	Destination DLCI	Destination EDLCI
One port with Management (1MPort)	Port-1	DLCI 201	Network	DLCI 201	EDLCI 0
	Internal	Mgmt201			EDLCI 2

The following example shows the 1-port, nonmanagement configuration (1Port).

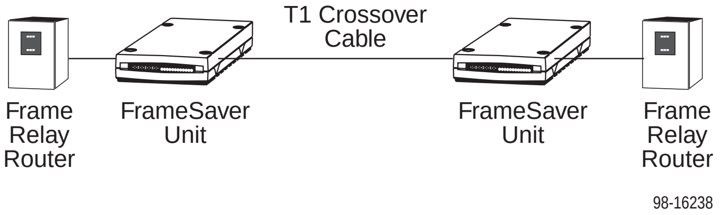


FR Discovery Mode Selection	Source Interface	Source DLCI	Destination Interface/Link	Destination DLCI	Destination EDLCI
One port with No Management (1Port)	Port-1	DLCI 201	Network	DLCI 201	EDLCI 0

Back-to-Back Operation

Back-to-back operation can be achieved by connecting two FrameSaver units using a network crossover cable, as in a test bench setup or a point-to-point configuration using a leased line. This configuration is useful for private frame relay networks, or for demonstrations when a frame relay circuit is not available. This feature is for dry copper applications only, when there are no frame relay switches at either end.

This configuration is shown in the illustration below.



Using this feature, one FrameSaver unit must be configured for Back-to-Back operation so it presents the network side of the UNI and provides network timing from its internal clock. The other FrameSaver unit must be configured for Standard operation, which is the setting for normal operation.

See *Setting Up Units for Back-to-Back Operation* in Chapter 10, *Operation and Maintenance*, for additional information.

User Interface and Basic Operation

4

Access to the easy to use, menu-driven user interface is provided through an async (asynchronous or other VT100-compatible) terminal, PC terminal emulation, or a Telnet session.

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

- *Logging On* (see below)*.*
- *Main Menu* on page 4-4.
- *Screen Elements* on page 4-5.
- *Navigating the Screens* on page 4-6.

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 over the COM port or modem port 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 menu-driven user interface screen is blank. Press Return to activate the interface. One of the following occurs:

- If no security was set up or security was disabled, the Main Menu screen appears (see page 4-4). 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 Return to reactivate the interface.

▶ Procedure

To log in when security is being enforced:

1. Enter your assigned Login ID and press Return.
2. Enter your Password and press Return.
   - 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 (see page 4-4). Begin your session.
Invalid	Message, **`Invalid Password`**, is displayed on line 24, and the Login screen is redisplayed. After three unsuccessful attempts: – A Telnet session is closed. – The User Interface Idle screen appears for a directly-connected terminal. – An external modem is disconnected. – An SNMP trap is generated. Access is denied. See your system administrator to verify your login (Login ID/Password combination).

If two sessions are already active. Wait and try again.

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

  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 Return.

   — For a COM port-connected terminal, the session is ended.

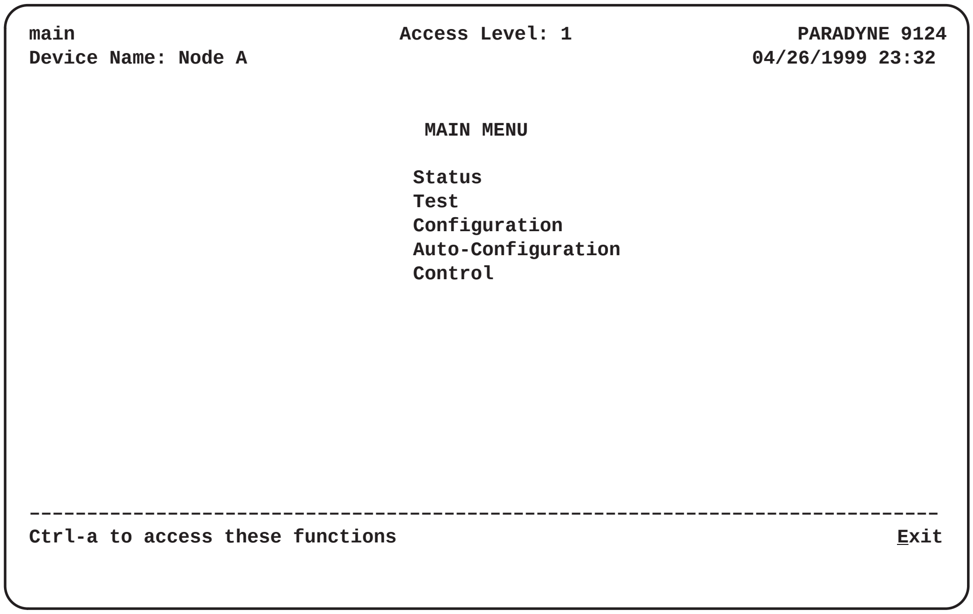
   — For a modem port-connected terminal, the session is ended and the modem is disconnected.

   — For a Telnet connection, the session is closed and, if no other Telnet or FTP session is occurring over the connection, the modem is disconnected.

If ending a session from the Configuration branch, see *Saving Configuration Options* in Chapter 8, *Configuration*.

Main Menu

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



```
main                                 Access Level: 1                 PARADYNE 9124
Device Name: Node A                                                04/26/1999 23:32


                                       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. Also, to 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. Automatically populate network and data port DLCI configuration options with numeric settings.
Control	Control the async user interface for call directories, device naming, login administration, and selecting software releases. Also, to initiate a power-on reset of the FrameSaver unit.

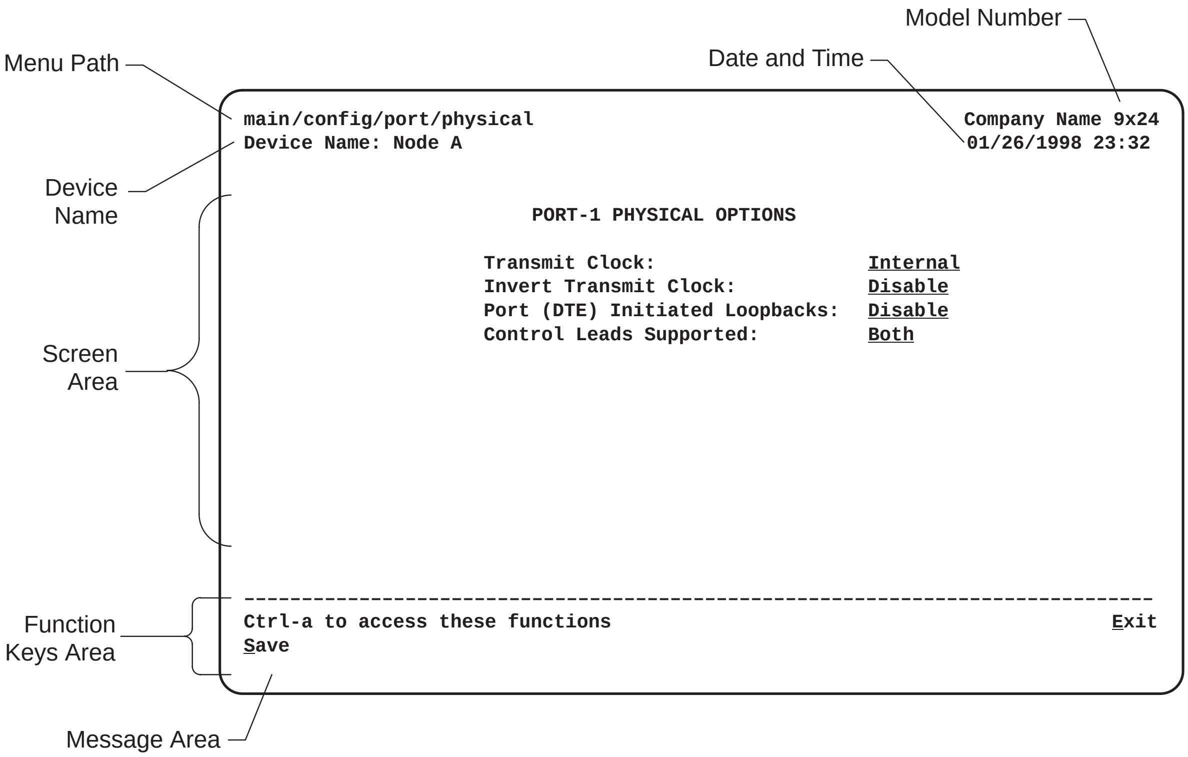
See Appendix A, *Menu Hierarchy*, for a pictorial view of the menu hierarchy, which represents the organization of the FrameSaver unit's menus and screens.

Screen Elements

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.



```
main/config/port/physical                                    Company Name 9x24
Device Name: Node A                                           01/26/1998 23:32

                          PORT-1 PHYSICAL OPTIONS

                    Transmit Clock:                 Internal
                    Invert Transmit Clock:          Disable
                    Port (DTE) Initiated Loopbacks: Disable
                    Control Leads Supported:        Both

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

Screen Format	Description
Menu Path	Menu selections made to reach the current screen.
Device Name	Customer-assigned identification of the FrameSaver unit.
9124	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 Return.
Message Area	System-related information and valid settings for input fields in the lower left corner. System and Test Status messages in the lower right corner.

Navigating the Screens

You can navigate the screens by:

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

Keyboard Keys

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

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

Function Keys

All function keys (located in the lower part of the screen; see the example on page 4-5) 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 async 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.
P or p	PrevDLCI	Display the previous DLCI.
N or n	NextDLCI	Display the next DLCI.
F or f	ClrFarStats	Reset far-end ESF line statistics and refresh the screen.
P or p	ClrNearStats	Reset near-end ESF line statistics and refresh the screen.

The following sections provide examples that show you how to:

- Select from a menu page 4-8).
- Switching between screen areas page 4-8).
- Select a field page 4-9).
- Enter information (see page 4-9).

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 Return. The selected menu or screen appears.

▶ Procedure

To return to a previous screen, use either of the following methods:

- Press the Escape (Esc) key until you reach the desired screen.
- Switch to the function keys area of the screen, and select MainMenu.

Switching Between Screen Work Areas

Use Ctrl-a to switch between screen areas (see page 4-5).

▶ 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 Return. 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.

Using the OpenLane NMS

5

This chapter includes:

- OpenLane Management features.
- Installation and Setup of the OpenLane DCE Manager and Performance Wizard on page 5-2.
- *Viewing OpenLane Performance Wizard Graphs* specific to FrameSaver SLV data collection and display on page 5-10.
- *Creating OpenLane Service Level Management (SLM) Reports* on page 5-26.

OpenLane Performance Wizard includes Diagnostic Wizard, a feature that allows you to setup, run, and monitor test results applicable to the system from a single screen. Diagnostic Wizard information is incorporated into Chapter 11, *Troubleshooting*.

The OpenLane Advantage

OpenLane Management features:

- Nondisruptive tests from OpenLane NMSs
- Layers 1, 2 and 3 monitoring
- Real-time and historical focus
- Diagnostic focus
  - Alarm and operational status monitoring
  - WAN errors and congestion monitoring
  - Nondisruptive network integrity checks and latency tests
  - Capacity analysis
  - Throughput utilization
  - Data delivery and congestion analysis
  - Patent pending PVC Data Delivery Analysis
- Service level accounting and quality of service verification

Using an OpenLane NMS Application

For additional information about accessing and managing the FrameSaver SLV unit through OpenLane DCE Manager and OpenLane Performance Wizard, and for hardware and software requirements necessary to support these applications refer to the:

- *OpenLane DCE Manager User's Guide* to help you set up and configure devices and their interfaces; and monitor, operate, and perform diagnostic testing using the Unix-based management application.
- *OpenLane DCE Manager for HP OpenView for Windows User's Guide* to help you set up and configure devices and their interfaces; and monitor, operate, and perform diagnostic testing using the Windows-based management application.
- *OpenLane Performance Wizard User's Guide* to query devices for both real time and historical data, and to display graphs.

Installation and Setup of DCE Manager

OpenLane DCE Manager is used in conjunction with HP OpenView or NetView, and if performance graphs are wanted, used with OpenLane Performance Wizard, as well.

When adding FrameSaver SLV units to your network, follow the procedures provided in the appropriate DCE Manager User's Guide:

- Install the OpenLane DCE Manager for Unix or Windows software and open the application as specified in the applicable User's Guide.
- Use the Autodiscovery feature to discover the new FrameSaver SLV units.

Refer to the appropriate User's Guide for installation and setup, and information about accessing and managing the FrameSaver SLV unit through OpenLane DCE Manager:

- *OpenLane DCE Manager User's Guide*
- *OpenLane DCE Manager for HP OpenView for Windows User's Guide*

Installation and Setup of Performance Wizard

Performance Wizard can be used alone, or it can be invoked from an HP OpenView or NetView window. To use this application:

- Install the OpenLane Performance Wizard software and open the application.
- Add frame relay agents to the Device Explorer, unless using DCE Manager.
- Set up historical data collection.

Installing and Starting OpenLane Performance Wizard

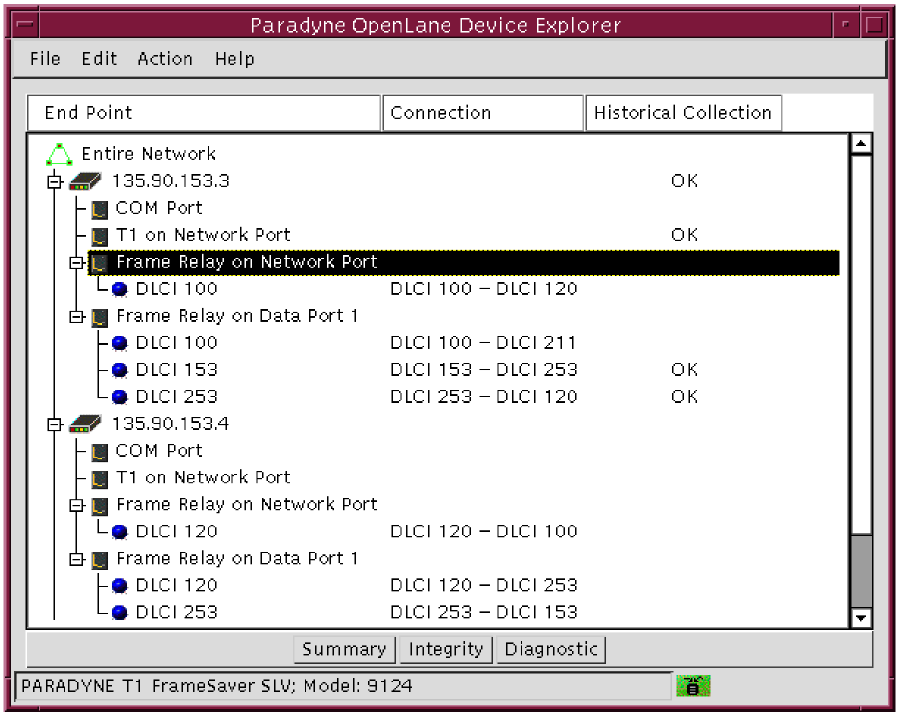
Installation instructions are located in the *OpenLane Performance Wizard User's Guide*. Open the application by following the instructions contained in *Getting Started with the Performance Wizard*. Depending upon your platform, see one of the following procedures:

- *Installing on Solaris, HP-UX, and AIX*
- *Installing on Windows NT or Windows 95*

The OpenLane Performance Wizard Device Explorer window opens. This window has three columns of information:

- **End Point** – Shows the devices in the network and their interfaces.
- **Connection** – Shows the PVC connections.
- **Historical Collection** – Shows whether historical data is being collected for the interface or PVC.

Based upon the item that is highlighted, appropriate graph selection buttons appear near the bottom of the window. Once a graph window is open, other graphs can be launched from the graph selections under the menu bar.



End Point	Connection	Historical Collection
Entire Network		
135.90.153.3		OK
COM Port		
T1 on Network Port		OK
Frame Relay on Network Port		
DLCI 100	DLCI 100 – DLCI 120	
Frame Relay on Data Port 1		
DLCI 100	DLCI 100 – DLCI 211	
DLCI 153	DLCI 153 – DLCI 253	OK
DLCI 253	DLCI 253 – DLCI 120	OK
135.90.153.4		
COM Port		
T1 on Network Port		
Frame Relay on Network Port		
DLCI 120	DLCI 120 – DLCI 100	
Frame Relay on Data Port 1		
DLCI 120	DLCI 120 – DLCI 253	
DLCI 253	DLCI 253 – DLCI 153	

PARADYNE T1 FrameSaver SLV; Model: 9124

Notice the green icon at the bottom of the window. Move the cursor over the icon and the status message says **`Historical Daemon Running`**. If the Historical Daemon is not running, a red circle with a slash through it overlays the icon.

Adding FrameSaver SLV Units to Your Network

Use either one of these procedures to add FrameSaver SLV units to your network.

▶ Procedure

To add an SLV unit from HP OpenView or NetView:

1. Use the HP OpenView or NetView autodiscovery feature to create submaps and discover an SLV unit.
2. Click on the submap containing the SLV unit, then click on the icon for the unit.
3. Use the following HP OpenView menu selection sequence to access Performance Wizard Device Explorer:

   Windows: *Control* → *Performance Wizard* → *Device Explorer*

   Unix: *Performance* → *Performance Wizard* → *Device Explorer*

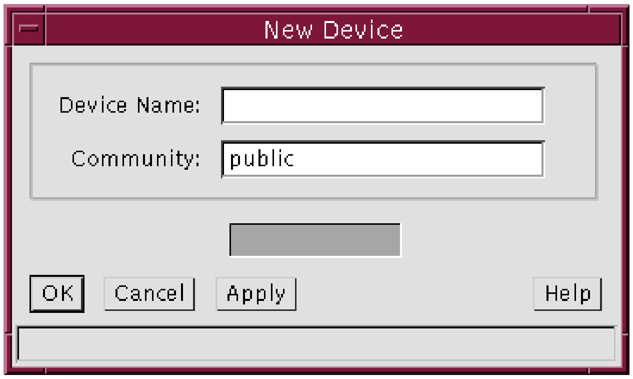
   The OpenLane Performance Wizard Device Explorer window opens so you can change or verify the Community Name and view the graphs.

Refer to your DCE Manager User's Guide for additional information.

▶ Procedure

To add an SLV unit from Performance Wizard Device Explorer:

1. Select New Device... from the File menu. The New Device dialog box opens.



New Device

Device Name:

Community: public

2. Enter the unit's IP address or IP hostname in the Device Name field.
3. Change the Community Name, if necessary.
4. Select the OK button. The New Device dialog box closes and the unit's IP address or IP hostname appears in the Device Explorer device display area.

   Refer to *Populating the Device Display Area* in Chapter 2, *Using the Device Explorer*, of the *OpenLane Performance Wizard User's Guide* for additional information.

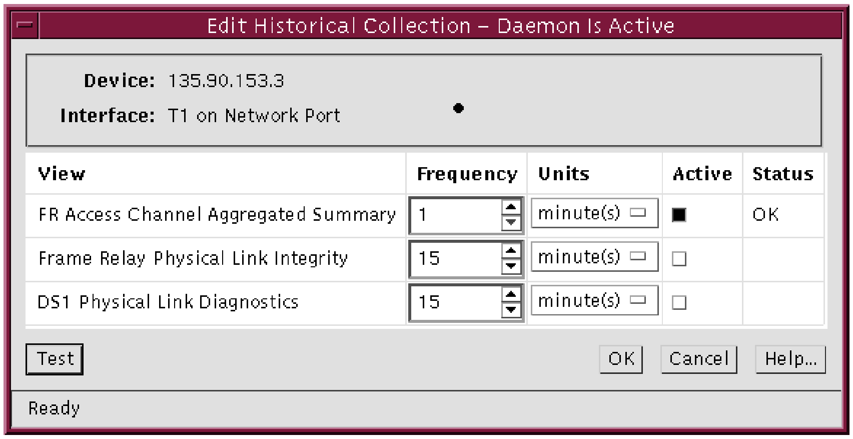
Setting Up for Collection of Historical Data

See the sample Device Explorer window on page 5-3. OK appears under the Historical Collection column. In this example, historical data is being collected for performance statistics on the T1 or Network Port interface of the 135.90.153.3 device.

▶ Procedure

To specify collection of historical data:

1. Select an interface or PVC so it is highlighted.
2. Click the right mouse button and select Historical Collection... from the menu. The following dialog box opens.



Edit Historical Collection – Daemon Is Active

Device: 135.90.153.3

Interface: T1 on Network Port

View	Frequency	Units	Active	Status
FR Access Channel Aggregated Summary	1	minute(s)	■	OK
Frame Relay Physical Link Integrity	15	minute(s)	□	
DS1 Physical Link Diagnostics	15	minute(s)	□	

Ready

3. Change the frequency of samples to be taken and the unit of time to be used for each of the graphical views.
4. Click on the Active box for the graphical views wanted so a checkmark appears in the box.
5. Select the Test button to verify that the data collection parameters are correct. OK should appear in the message area.
6. Select the OK button. The Edit Historical Collection dialog box closes, and an OK appears under the Historical Collection column for the interface or PVC selected, and for the device.
7. Click on Action at the menu bar, and select Start Historical Daemon if it is not currently running. Check the lower right corner of the Device Explorer window to see whether Historical Daemon is running (see the example on page 5-3).

Accessing NetScout Manager Plus

A direct link to the NetScout Manager Plus application is provided by OpenLane Performance Wizard. Use this feature to launch NetScout reports.

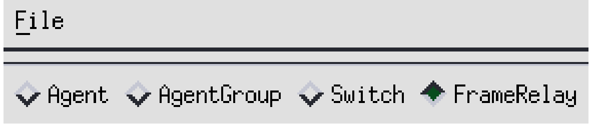
▶ Procedure

To access the NetScout Manager Plus main window:

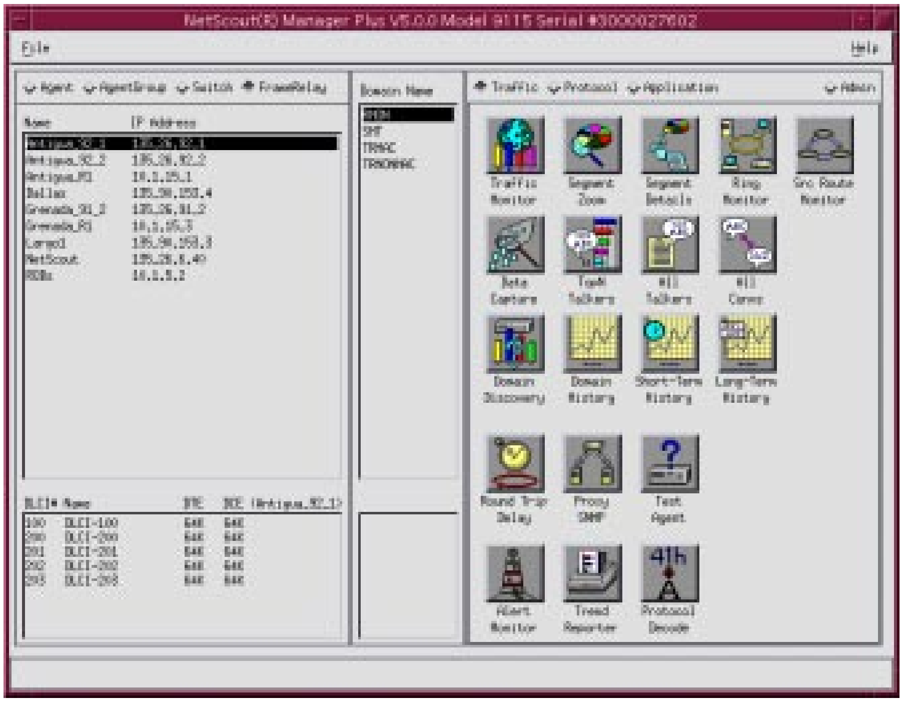
1. Select Start NetScout Manager from the Action menu.

   The NetScout Manager Plus main window appears.

2. Select the FrameRelay radio button from the agent type selection bar (on the left side of the window).



   Applicable icons appear on the right side of the main window.



Name	IP Address
Antigua_92_1	135.26.92.1
Antigua_92_2	135.26.92.2
Antigua_FR	10.1.15.1
Dallas	135.38.153.4
Grenada_91_2	135.26.91.2
Grenada_FR	10.1.15.3
Largo1	135.90.153.3
NetScout	135.26.8.40
RDBs	10.1.5.2

DLCI#	Name	DTE	DCE (Antigua_92_1)
100	DLCI-100	64K	64K
200	DLCI-200	64K	64K
201	DLCI-201	64K	64K
202	DLCI-202	64K	64K
203	DLCI-203	64K	64K

Refer to *Launching NSM* in Chapter 3 of the *NetScout Manager/Plus & NetScout Server Administrator Guide* for information about how to start reports.

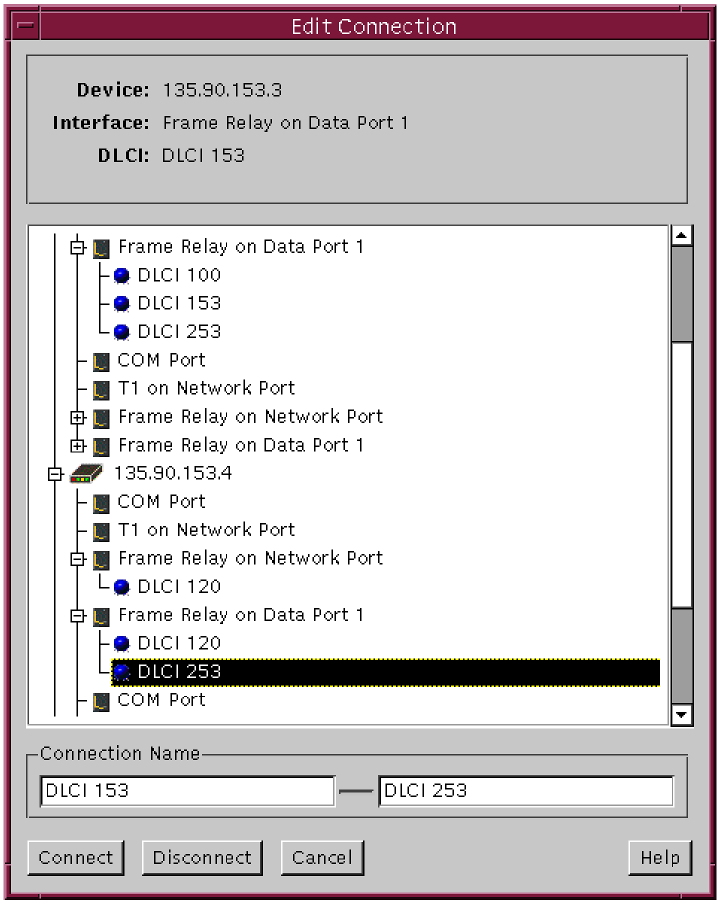
Creating PVC Connections

Port-1 PVC definitions need to be created between two endpoints in the network. Network PVCs were automatically created when the unit is discovered.

▶ Procedure

To create PVC definitions:

1. From Device Explorer, select a device's DLCI so it is highlighted.
2. Click the right mouse button and select Connection... from the menu. The Edit Connection dialog box opens, with the network collapsed.
3. Expand the remote network device in the device display area so that its DLCIs are shown.



Device: 135.90.153.3
Interface: Frame Relay on Data Port 1
DLCI: DLCI 153

Connection Name: DLCI 153 — DLCI 253

4. Select the appropriate DLCI so it is highlighted.

   The selected DLCI numbers appear in the Connection Name field for both ends of the connection, which can be edited for a more meaningful name.
5. Select the Connect button. The Edit Connection dialog box closes and the PVC appears under the Connection column for the devices at both ends of the connection.

Repeat the procedure until all Port-1 DLCI connections have been defined.

Setting Frame and Burst Ranges

You can configure frame size and burst upper limits to:

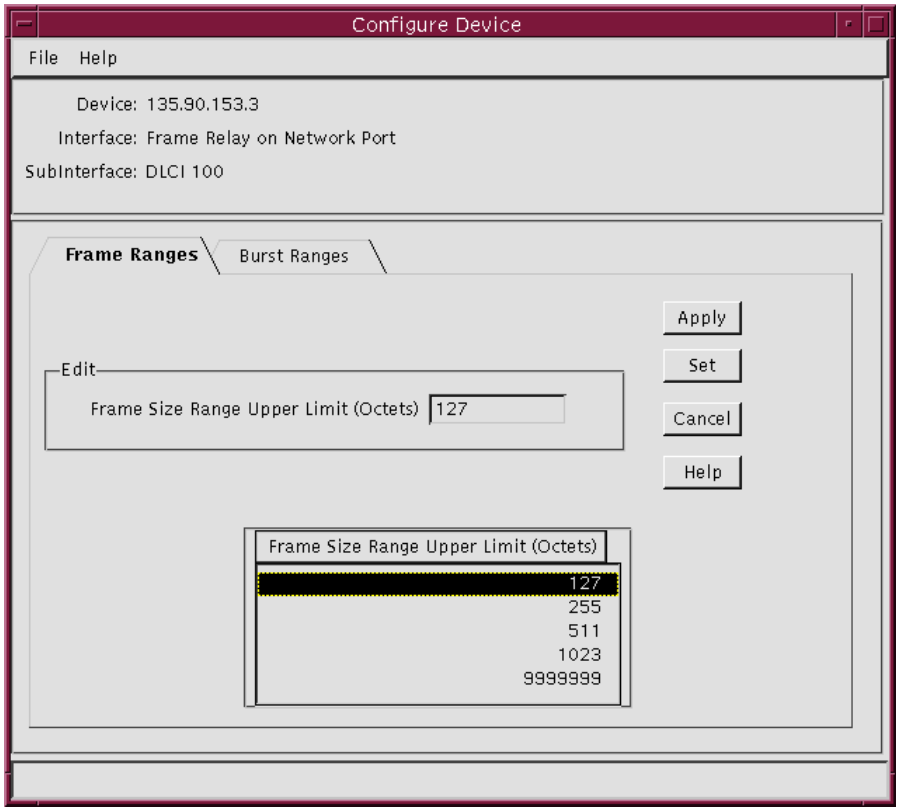
- Match service level agreement parameters.
- Identify problem areas.
- Display the Frame Burst Breakdown graph.
- Assist in troubleshooting.
- Match the site's traffic patterns.

▶ Procedure

To set frame and burst range parameters:

1. From Device Explorer, select a device's DLCI so it is highlighted.
2. Select Configure Device... from the Edit menu.

   The Configure Device dialog box opens to the Frame Ranges tab, with the Burst Ranges tab in the background.



Device: 135.90.153.3

Interface: Frame Relay on Network Port

SubInterface: DLCI 100

Frame Size Range Upper Limit (Octets) 127

Frame Size Range Upper Limit (Octets)
127
255
511
1023
9999999

3. Select the Burst Ranges tab to bring it to the forefront if you want to set Burst Range Upper Limits.

   The procedure for setting the frame size and burst upper limits is the same.

4. Select a row in the box below the Frame Size Range Upper Limit (Octets) or Burst Range Upper Limit (Octets) heading so it is highlighted, and the selected value appears in the Edit box.

   NOTE:

   If you change frame size ranges, the frame size distribution cannot be displayed by the NetScout Manager. Performance Wizard is recommended for display.

5. Change the Upper Limit value, and select the Apply button.

   If you change the upper limit, the numbers under the Frame Size Range Upper Limit (Octets) heading are re-sorted going from lowest to the highest.

   When editing Upper Limits, you cannot:

   — Enter letters or characters; only numbers are permitted.

   — Have duplicate numbers; each range limit must be unique.

   — Enter a number lower than the lowest limit shown, or higher than the highest limit, which is all 9s (e.g., 9999999).

6. Continue Steps 3 through 5 until all desired edit changes have been made, then select the Set button. The changed settings become the new Upper Limits.

Getting Error Messages

Error messages may appear in the messages area at the bottom of the window to indicate when there is a problem (e.g., **`Unable to set table. SNMP Error: No such name`**). When this type of error occurs, you need to resynchronize with the FrameSaver unit.

▶ Procedure

To resynchronize:

1. Leave the current view and return to the Device Explorer main window.

2. Select Device Sync... from the File menu.

3. Return to the view where the error message appeared. The error message should be gone.

   If the error message is not cleared, see the *OpenLane Performance Wizard User's Guide*, or the Help feature, for additional information.

Viewing OpenLane Performance Wizard Graphs

The following OpenLane Performance Wizard graphs support FrameSaver SLV units, integrating the new service level verifier capability provided by FrameSaver SLV units into Device Explorer:

- **Frame Relay Access Channel Aggregated Summary** – Capacity, Throughput, and Heaviest Users – Output
- **Frame Relay Physical Link Integrity** – Throughput, Errored Frames, LMI Signaling Errors, and Unknown Protocol Frames
- **DS1 Physical Link Integrity (T1 Devices Only)** – Error Free Seconds, Errored Seconds, and Transmission Errors
- **DS1 Physical Link Diagnostics (T1 Devices Only)** – Error Free Seconds, Errored Seconds, and Transmission Errors
- **PVC Throughput** – Transmit and Receive
- **Frame Relay DLCI Congestion** – Capacity, Throughput, and Congestion
- **PVC Data Delivery Analysis** – Transmit Bit Burst Analysis As % CIR, Round Trip Network Latency, End-to-End Data Delivery Success, and Transmit Frame Size Distribution

Status and error messages appear in the messages area at the bottom of Performance Wizard windows. If an error message appears, try and resynchronize with the FrameSaver unit.

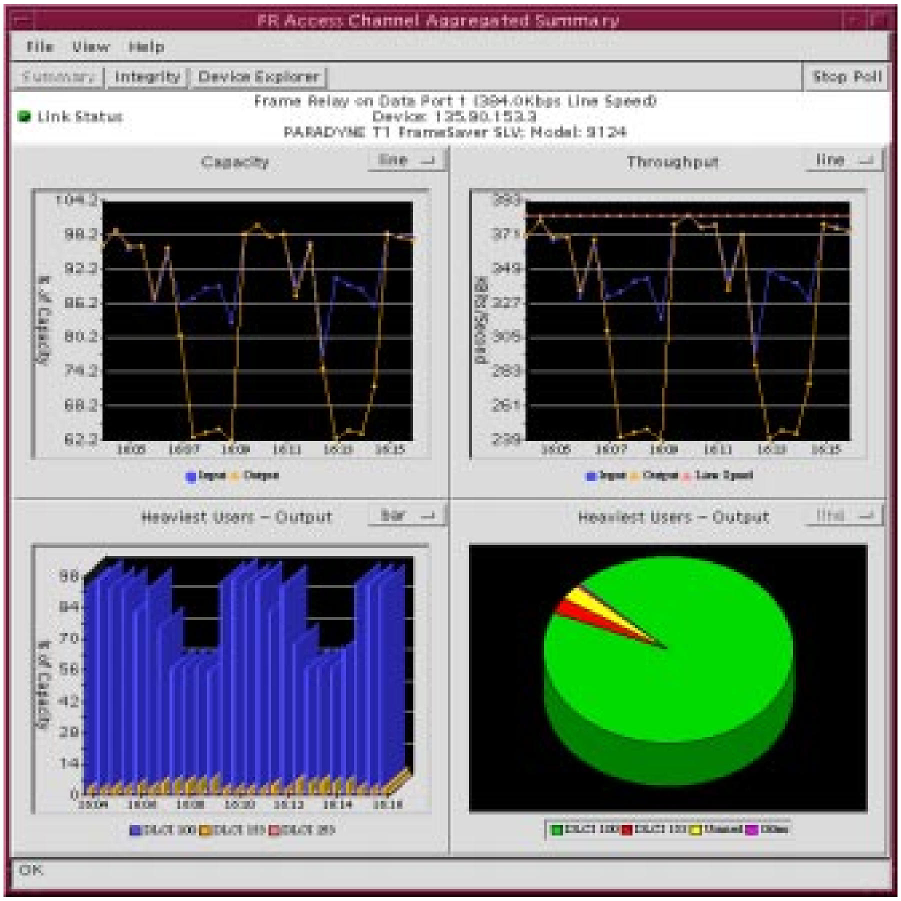
The following sections show and discuss the frame relay windows that can be accessed when monitoring a FrameSaver SLV unit.

Refer to the *OpenLane Performance Wizard User’s Guide*, or the Help feature, for additional information.

Frame Relay Access Channel Aggregated Summary

For a complete view of an interface's traffic, this graph summary brings together the information needed to determine how well an interface's, or link's, capability is being utilized.

This set of graphs is provided for the network and data ports. For the FrameSaver 9124, it is also available for the T1 interface.



Frame Relay on Data Port 1 (384.0Kbps Line Speed)
Device: 135.90.153.3
PARADYNE T1 FrameSaver SLV; Model: 9124

Correlate the time at which a problem occurred to the following graphs.

- **Capacity** – Shows what percent of the physical link is being used. A measurement is provided for both incoming and outgoing data. The percentage is based upon line speed.
- **Throughput** – Shows the actual volume of data in kilobits per second for both incoming and outgoing data over a physical link. The line speed is also shown so you can easily see when the link's physical capacity is about to be exceeded.

- **Heaviest Users – Output** – Shows which DLCIs are generating the most traffic over the frame relay link. Up to three high-volume DLCIs can be shown.

  This information can be viewed in two forms:

  — **Graph** – The data shown for each DLCI is a percent of the line speed over time. Up to three high-volume DLCIs can be shown.

  — **Pie Chart** – The data shown for each DLCI is a percent of the total output per the most recent snapshot.

  NOTE:

  Position the cursor over a particular DLCI within the graph and press the right mouse button to display a menu which includes the DLCI's exact % of Capacity. In the pie chart, the % of Capacity for the unused portion is also shown.

If errors occurred when transmitted data bursts exceeded line capacity, looking at the Heaviest Users should indicate the DLCI(s) most responsible for the problem. Once identified, PVCs generating the greatest amount of traffic can be examined further.

▶ Procedure

To immediately launch PVC graphs:

1. From within a Heaviest Users graph or pie chart, position the cursor over a DLCI segment.

2. Press the right mouse button to display the menu.

3. Select either the PVC Throughput or PVC Congestion graph, or PVC Analysis if viewing the aggregated summary for the network interface. See one of the following:

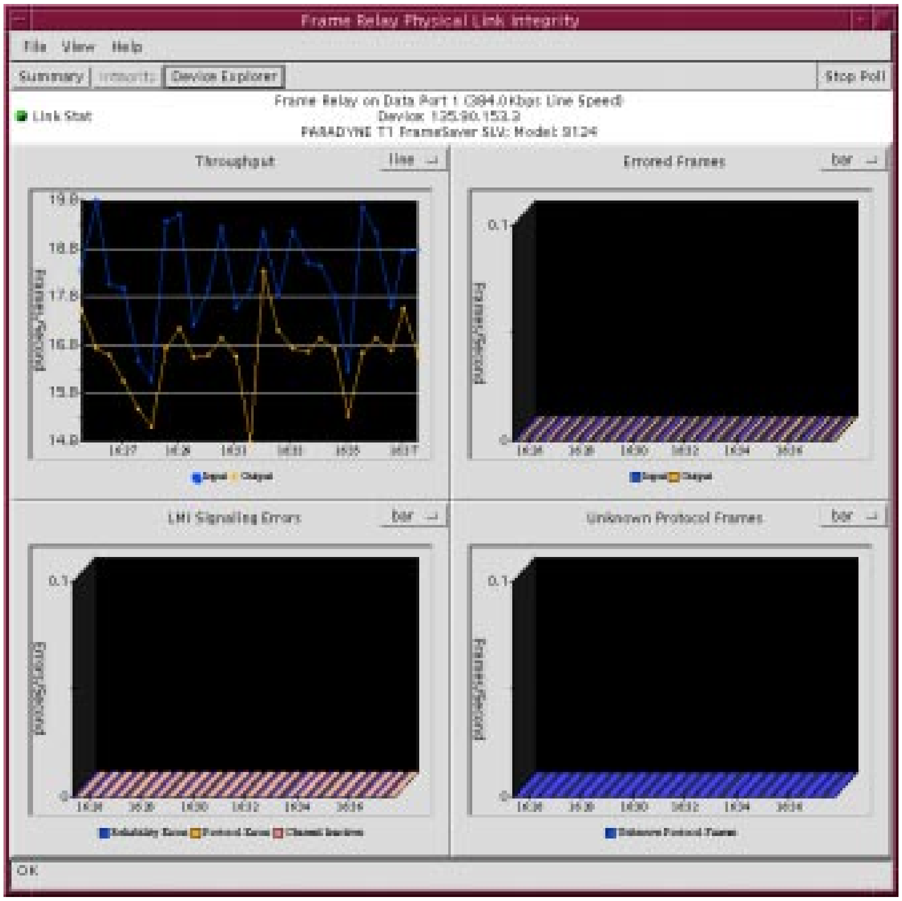
   — PVC Throughput for end-to-end connectivity between units at both ends of the PVC, and to see the types of errors that are being recorded by each unit.

   — PVC Congestion for if the PVC is exceeding its contracted CIR and whether it is causing network congestion.

   — PVC Analysis for a more complete view of network traffic. Only appears for a network interface.

Frame Relay Physical Link Integrity

Use this grouping of graphs to relate actual throughput on the frame relay link to the types of errors that are occurring. It can also be used to verify that the network is operational and traffic is flowing normally.



Frame Relay on Data Port 1 (384.0 Kbps Line Speed)
Device: 135.90.153.2
PARADYNE T1 FrameSaver SLV: Model 9124

OK

Correlate the time at which a problem occurred to the following graphs.

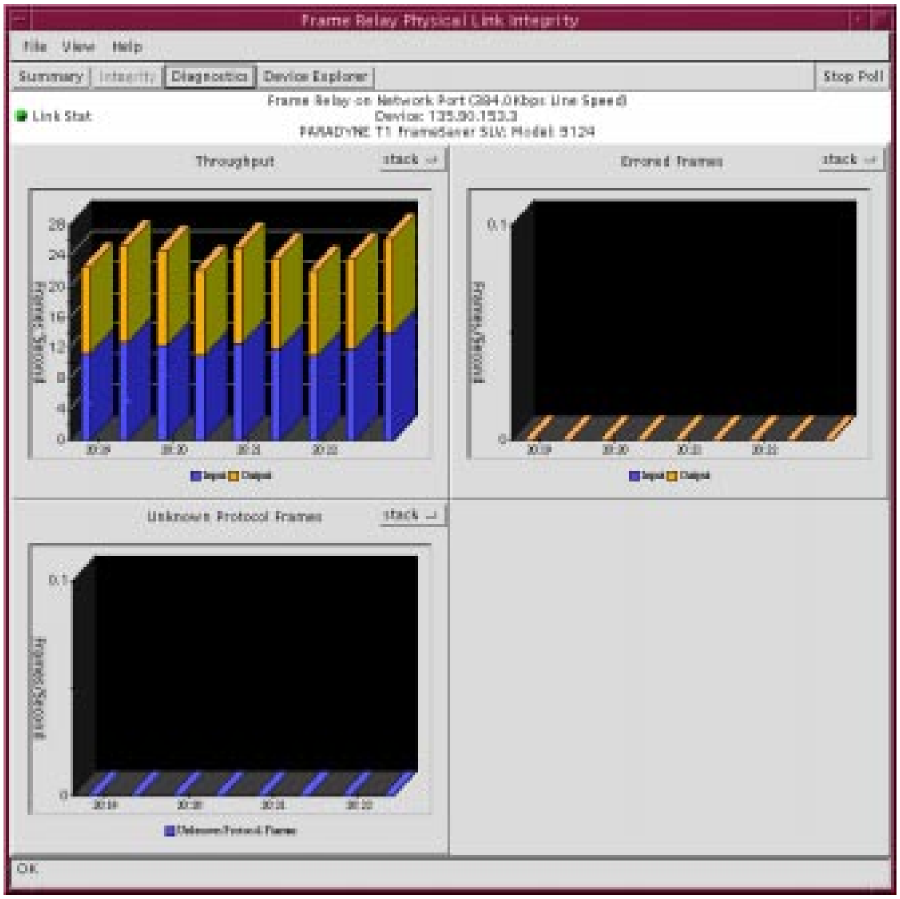
- **Throughput** – Shows the actual volume of data in frames per second for both incoming and outgoing data over a physical link. The line speed is also shown so you can easily see when the link's physical capacity is about to be exceeded.
- **Errored Frames** – Shows a count of errored or discarded frames over a physical link for both incoming and outgoing data.
- **LMI Signaling Errors**
  - Only displayed if the Frame Relay on Data Port 1 interface was selected. This is an errors-per-second count for each type of error detected: Reliability Errors, Protocol Errors, and Channel Inactives.
  - Unknown Protocol Frames shows the number of unknown protocol errors received on the link.

If Frame Relay for Data Port 1 was selected, compare LMI Signaling Protocol Errors against the Unknown Protocol Frames graph to see how many of the LMI errors were due to wrong protocol being used.

See *Frame Relay Performance Statistics* in Chapter 11, *Displaying System Information*, for additional information.

DS1 Physical Link Integrity (T1 Only)

Use this grouping of graphs to compare actual throughput with T1 errors. With this window, you can determine the amount of time the link has been operating error free, and what types of errors are causing the greatest number of problems.



Frame Relay on Network Port (384.0Kbps Line Speed)
Device: 135.90.153.3
PARADYNE T1 FrameSaver SLV: Model 9124

Correlate the time at which a problem occurred to the following graphs.

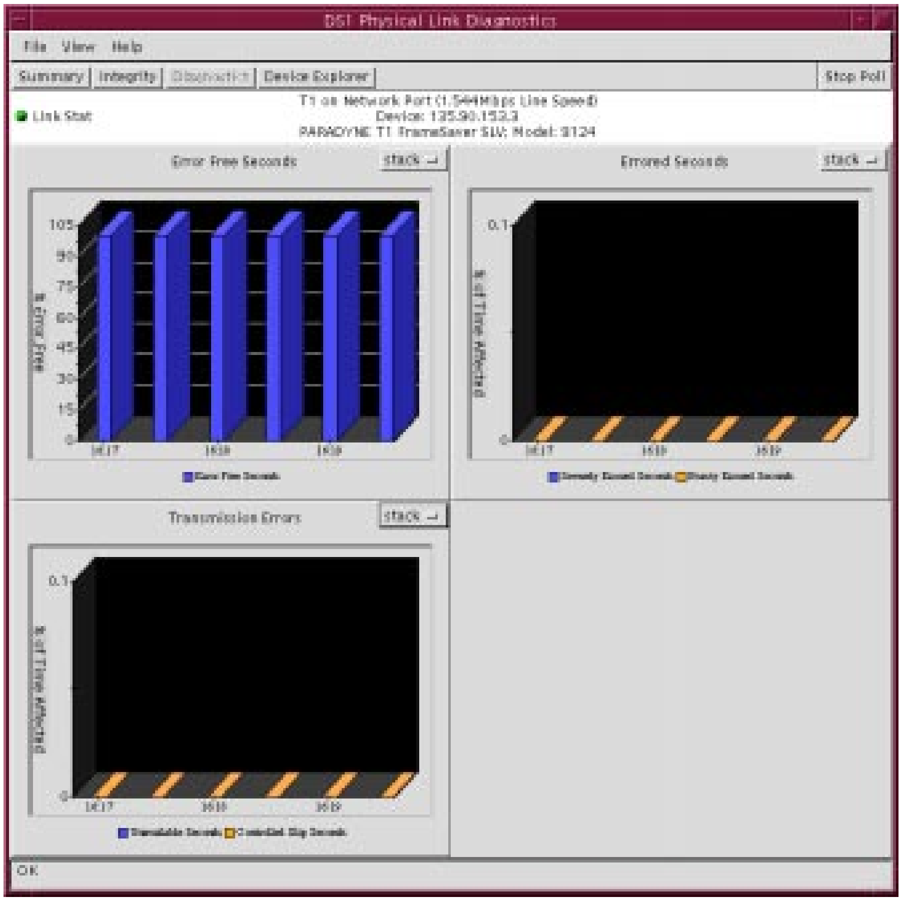
- **Throughput** – Shows the actual volume of data in frames per second for both incoming and outgoing data over the T1 link.
- **Errored Frames** – Shows the number of frames per second during which a Severely Errored Seconds or Bursty Errored Seconds condition existed for both incoming and outgoing data over the T1 link, calculated on the percent of the time interval shown.
- **Unknown Protocol Frames** – Shows the number of frames per second that were counted when the unit could not recognize the protocol used in the packet.

When errors occur on the T1 link, select the Diagnostic button under the menu bar for additional insight to the problem.

See Chapter 11, *Displaying System Information*, for additional information on these types of errors.

DS1 Physical Link Diagnostics (T1 Only)

Use this summary graph when errors are detected on the T1 link. This window is only available to a FrameSaver unit with a T1 interface, when either T1 or Frame Relay on Network Port was the selected interface. Using this graph combination, you can assess the amount of time the T1 link was free of problems, or not, and the types of errors the link was experiencing.



T1 on Network Port (1.544Mbps Line Speed)
Device: 135.90.153.3
PARADYNE T1 FrameSaver SLV; Model: 9124

Correlate the time at which a problem occurred to the following graphs.

- **Error Free Seconds** – Shows the amount of time during which no errored seconds occurred on the T1 link, counted as a percentage of the time interval shown.
- **Errored Seconds** – Shows the percentage of time during which a Severely Errored Seconds or Bursty Errored Seconds condition existed, calculated on the percent of the time interval shown.
- **Transmission Errors** – Shows the percentage of time during which an Unavailable Seconds or Controlled Slip Seconds condition existed, calculated on the percent of the time interval shown.

See Chapter 11, *Displaying System Information*, for information on these types of errors.

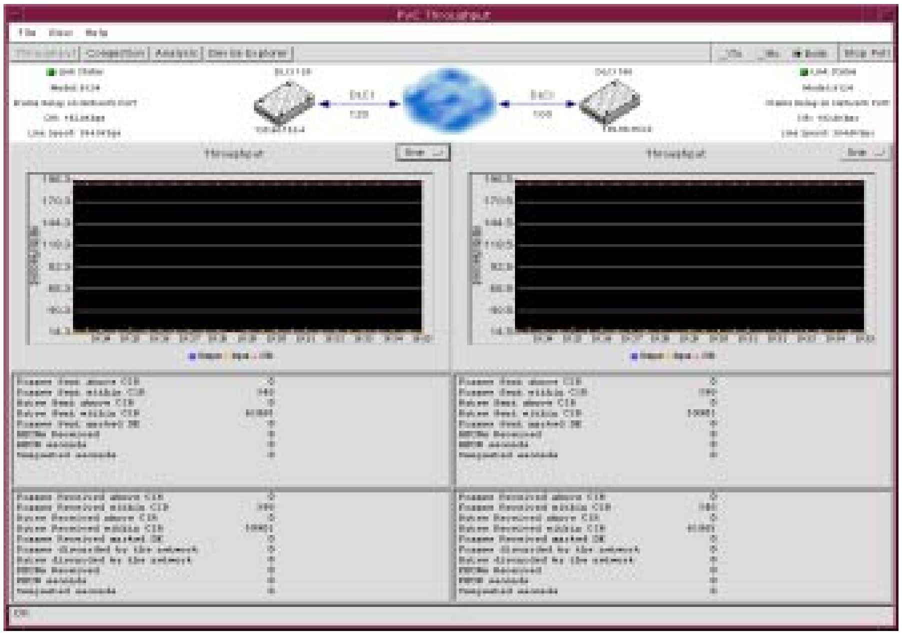
PVC Throughput

Congestion and CIR issues are clearly identified by this window.

Using this window, you can determine end-to-end performance for a PVC. The lines into the cloud change based upon the upper right radio button selected: Tx, Rx, or Both directions. The radio buttons refer to the input and output of the device.

Link Status next to each device indicate the link's current status. Each device is identified using a connection name, DLCI name, and DLCI number.

The Throughput graphs for each device shows the input and/or output for each device. Lines are shown for CIR, physical link speed, and input and output in bits per second.



```
Frames Sent above CIR                 0
Frames Sent within CIR                [illegible]
Bytes Sent above CIR                  0
Bytes Sent within CIR                 [illegible]
Frames Sent marked DE                 0
BECNs Received                        0
BECN seconds                          0
Congested seconds                     0

Frames Received above CIR             0
Frames Received within CIR            [illegible]
Bytes Received above CIR              0
Bytes Received within CIR             [illegible]
Frames Received marked DE             0
Frames discarded by the network       0
Bytes discarded by the network        0
FECNs Received                        0
FECN seconds                          0
Congested seconds                     0
```

```
Frames Sent above CIR                 0
Frames Sent within CIR                [illegible]
Bytes Sent above CIR                  0
Bytes Sent within CIR                 [illegible]
Frames Sent marked DE                 0
BECNs Received                        0
BECN seconds                          0
Congested seconds                     0

Frames Received above CIR             0
Frames Received within CIR            [illegible]
Bytes Received above CIR              0
Bytes Received within CIR             [illegible]
Frames Received marked DE             0
Frames discarded by the network       0
Bytes discarded by the network        0
FECNs Received                        0
FECN seconds                          0
Congested seconds                     0
```

OK

Variables that could appear in the panes below each graph include:

Variable Displayed	Indication
Frames Sent above CIR	Number of transmitted frames that exceeded the contracted CIR.
Frames Sent within CIR	Number of transmitted frames that complied with CIR.
Frames Sent marked DE	Transmit data on a management PVC is marked discard eligible, so the network can discard the lower-priority frame when there is congestion.
Frames discarded by the network	Number of transmitted frames that were dropped.
Bytes Sent above CIR	Number of transmitted bytes over the contracted CIR.
Bytes Sent within CIR	Number of transmitted bytes within or under the contracted CIR.
Bytes discarded by the network	Number of transmitted bytes actually lost.
BECNs Received	Backward explicit congestion notification (BECN) has been sent by the network, warning that outbound frames may encounter congestion and may be dropped.
BECNs seconds	Duration over which BECNs were received.
FECNs Received	Forward explicit congestion notification (FECN) has been sent by the network, warning that inbound frames may encounter congestion and may be dropped.
FECNs seconds	Duration over which FECNs were received.
Congested seconds	Duration over which BECNs and FECNs were received.

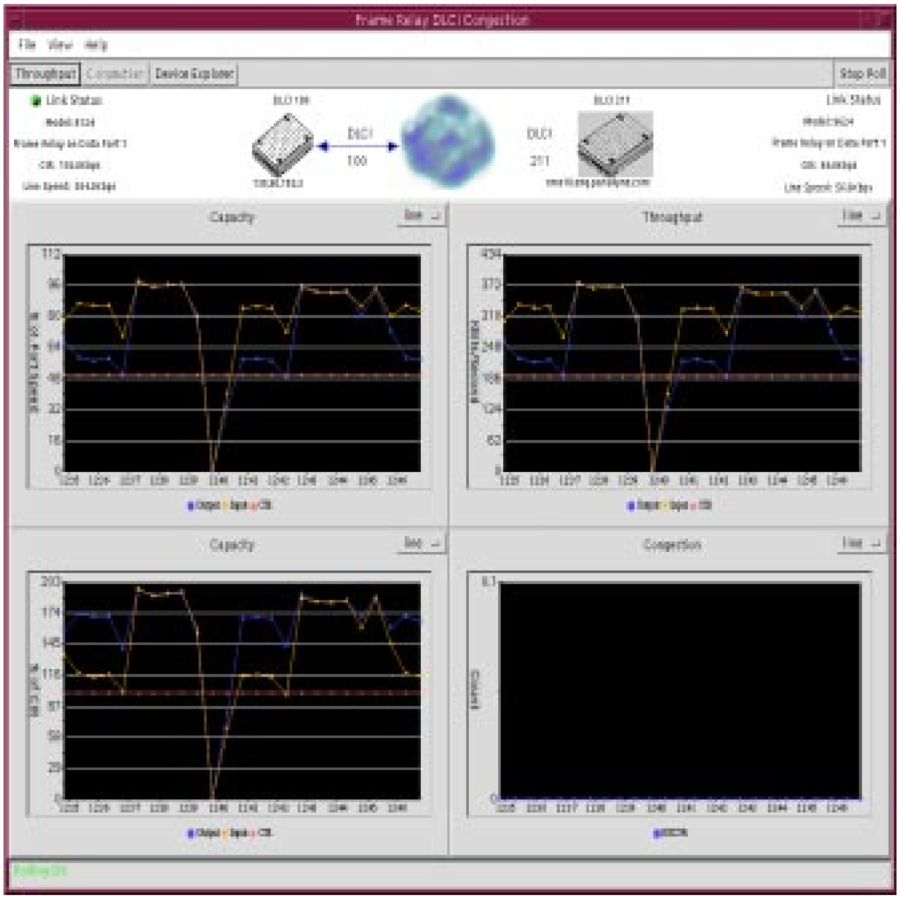
BECNs and FECNs indicate network congestion issues. Frames marked DE indicate that the DLCI is partly responsible for the network congestion; the DLCI has exceeded its contracted CIR.

When congestion is detected on the network, select the Congestion button under the menu bar to verify whether the DLCI is the cause for the problem.

See Chapter 11, *Displaying System Information*, for additional information on these types of errors.

Frame Relay DLCI Congestion

Although used primarily for capacity planning and CIR negotiations, this group of graphs can be used to assess whether a DLCI is contributing to network congestion.



Correlate the time at which a problem occurred to the following graphs.

- **Capacity** – Shows how a DLCI's capacity is being used for both incoming and outgoing data. When the DLCI's allocated bandwidth is underutilized, it is time to renegotiate CIR and excess burst size agreements.

  The DLCI's capacity is calculated based upon its data rate and CIR, which is provided in two graph views:

  — **% of Port Speed Capacity** – Shows capacity calculated based upon the FrameSaver unit's data rate.

  — **% of CIR Capacity** – Shows capacity calculated based upon the FrameSaver unit's CIR.

  Compare how CIR and Line Speed on the graphs compare to the CIR and Line Speed that had been configured, seen near the top of the window. The percentages calculated are based upon those values.

  When zero CIR has been configured, the speed of the link's capacity is used in the calculations instead of the speed of the DLCI's allocated capacity.

  These graphs are used primarily for capacity planning or in CIR negotiations.

- **Throughput** – Shows the actual volume of data in kilobits per second for both incoming and outgoing data over a frame relay PVC. Throughput only appears when the port is connected to the frame relay network. CIR is also shown so you can easily see when CIR is being exceeded.

  When the DLCI is exceeding CIR, trying to deliver more data than was contracted for, check the Round Trip Network Latency and End-to-End Data Delivery graphs on the PVC Data Delivery Analysis window to verify that the DLCI is the cause of apparent network problems.

- **Congestion** – Helps determine the degree of traffic congestion on the network, and the reason some frames may have been discarded by the network.

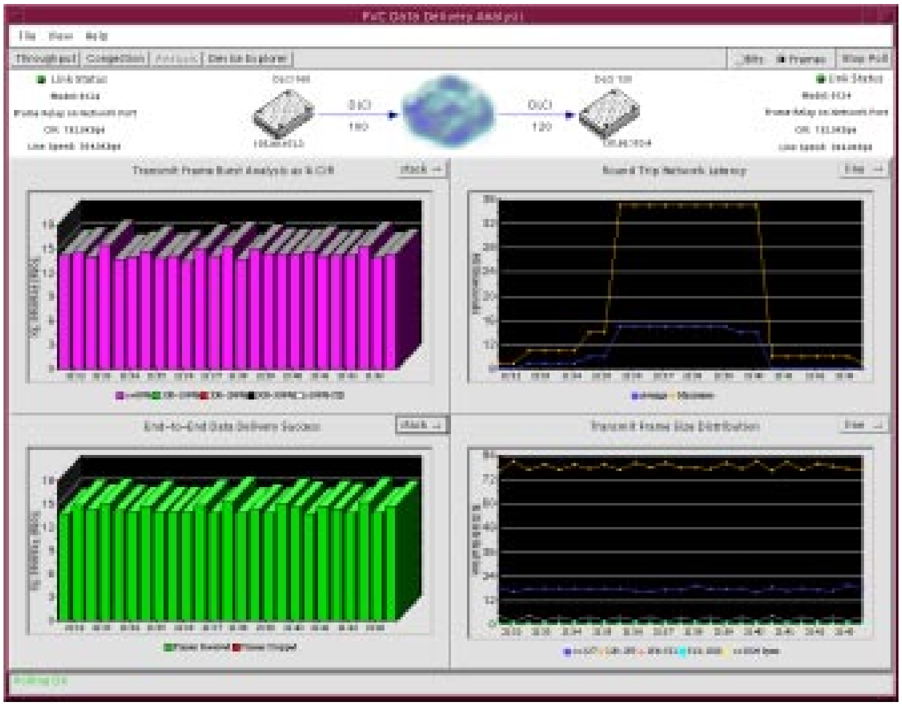
  The number of BECNs counted over time are shown. The network sends BECNs as a warning that outbound frames may encounter congestion and may be dropped.

When looking at these graphs, the % of Port Speed Capacity, % of CIR Capacity, and Throughput line graph patterns should be essentially the same. The only difference should be the scale values along the left side of each graph, based upon the measurement being shown.

PVC Data Delivery Analysis

For a more complete view of network traffic, this graph summary brings together the information needed to determine the cause of frame relay lost packets and/or excessive network latency. A patent is pending on this graphical report.

Network service providers can use this screen to help determine whether their network or the customer’s data was the cause for a missed service level agreement (SLA).


PVC Data Delivery Analysis
File View Help
Throughput
Congestion
Analysis
Device Explorer
Bits
Frames
Stop Poll
Link Status
DLCI
DLCI
Link Status
Transmit Frame Burst Analysis as % CIR
Round Trip Network Latency
End-to-End Data Delivery Success
Transmit Frame Size Distribution

You can view the Transmit Burst Analysis As % CIR and End-to-End Data Delivery Success graphs in either Bits or Frames by changing the radio button selection. In this example, the Frames radio button was selected.

- If Bits is selected, the Transmit Burst Analysis As % CIR graph is measured in Total Mbps Tx, and the End-to-End Data Delivery Success graph is measured in Total Kbps Tx.
- If Frames is selected, both the Transmit Burst Analysis As % CIR and End-to-End Data Delivery Success graphs are measured in Total Frames Tx.

In most cases, transmission characteristics of the customer's data rather than the network is the cause of apparent network problems. This summary allows you to determine the following:

- Overutilization of the network, trying to deliver amounts of data well over CIR.
- Data frames that are too large or small.
- More packets are being sent than the receiving node can receive due to differences in physical circuit capacity.

Any of these will cause the network switch's egress queue to fill, increasing latency and data loss.

Correlate the time at which a problem occurred to the following graphs.

- **Transmit Bit Burst Analysis As % CIR** – Shows network utilization bursting details to aid in determining the cause of frame relay lost packets and/or excessive network latency. Tx Bit Burst Analysis is measured in megabits and shows the exact distribution of transmitted data in relation to the DLCI's CIR and excess burst size.

  The color displayed indicates whether the DLCI is or is coming close to exceeding its purchased CIR and excess burst size.

Color	% of CIR	Indication
Blue	Less than or equal to 99%	Packets are within CIR.
Gold	100–199%	Packets are at or over CIR.
Pink	200–299%	Packets are two times greater than the contracted CIR.
Aqua	300–399%	Packets are three times greater than the contracted CIR.
Yellow	More than 399%	Packets are four times greater than the contracted CIR.

When zero CIR has been configured, the percentage breakdowns are based on link speed instead of CIR.

If utilization is consistently under 50% of CIR, the CIR contracted for should be downgraded. If over 100%, the DLCI may be ready for its CIR to be upgraded.

When a DLCI is overutilizing the network, compare the Tx Bit Burst Analysis graph against the following graphs to determine the cause:

— End-to-End Data Delivery Success to see if frames are being dropped.

— Round Trip Network Latency to see if the bursting is impacting latency.

- **Round Trip Network Latency** – Shows how fast the network is moving traffic. Latency is the amount of time it takes a frame relay frame to travel from one CPE end point to another and back. The times at which an average of the frame relay frames are calculated is shown along the bottom, while the delay is shown in milliseconds.

  Any excessive spikes or increases in latency should be investigated further. It could indicate a network problem, or it could indicate that the DLCI is oversubscribed, exceeding CIR, and is sending frames that are filling up the network switch's egress queue, delaying network traffic.

  To determine the exact cause of the delay, compare the Round Trip Network Latency graph against the following graphs to determine the cause:

  — Transmit Bit Burst Analysis As % CIR to see distribution of transmitted data in relation to the DLCI's CIR.

  — Transmit Frame Size Distribution to see the size of the packets that were transmitted.

- **End-to-End Data Delivery Success** – Shows the exact number of bits that were successfully delivered, as well as those that did not get delivered to the end point node for a selected DLCI.

  Data Delivery Success is measured in kilobits over time. The color displayed indicates whether data are being delivered.

Color	Indication
Green	Data that has been delivered successfully.
Red	Data that has been dropped by the network.
Blue	CIR contracted.
Gold	Local line speed.
Pink	Remote line speed.

When frames are being dropped, compare this graph against the following graphs to determine the cause:

— Transmit Bit Burst Analysis As % CIR to see distribution of transmitted data in relation to the DLCI's CIR.

— Transmit Frame Size Distribution to see the size of the packets that were transmitted.

- **Transmit Frame Size Distribution** – Various service level agreement parameters may be based on frame size, which may contribute to latency and frames being lost. This graph shows the size of the packets being transmitted, so you can compare frame size to your service level agreement.

  Transmit Frame Size Distribution is measured over time in percent of all transmitted packets within each of the following ranges:

Color	Packet Size in Bytes
Blue	Less than or equal to 127
Gold	128–255
Pink	256–511
Aqua	512–1023
Yellow	More than or equal to 1024

  Compare this graph with the following graphs:

  — End-to-End Data Delivery Success to see if frames are being dropped.

  — Round Trip Network Latency to see if frame size is impacting latency.

Creating OpenLane Service Level Management (SLM) Reports

The OpenLane SLM Reports (part of Performance Wizard) enables network administrators of FrameSaver SLV devices to provide securely partitioned access for their users to create and view reports, via the World Wide Web, that pertain only to their portion of the frame relay network. These reports include a summary of overall network performance, as well as detailed statistics on a per PVC basis of network latency, availability, and frame delivery success rate (throughput) for accurate service level agreement verification. This measurement of throughput uses the Paradyne proprietary TruePut technology which precisely measures both within and above CIR, eliminating inaccuracies due to averaging. Reports are also available for physical inventory of the network's device names, locations, serials numbers, DLCIs, and port speeds.

Network performance data is gathered from all FrameSaver SLV RMON-2 user history buckets at configurable intervals for 24 hours, allowing for offline or after hours retrieval of all needed report data. Also, the FrameSaver SLV units can be polled in real time for online troubleshooting and performance monitoring. All devices must first be added to the OpenLane Device Explorer database.

Web Browsers Supported

Users interact with the system via a Web browser. The following are recommended:

- Netscape Communicator 4.04 or higher
- Microsoft Internet Explorer 4.0

The SLM Reports have been tested with the Apache Web server, although other Web servers may work as well, including Web servers that use Secure Socket Layer (SSL) for data encryption. Be aware that encryption greatly slows the throughput of the system. If the Apache Web server is not installed, refer to the Apache Web site at http://www.apache.org for installation instructions.

Installation and Setup of SLM Reports

Refer to the *OpenLane Performance Wizard User's Guide* for installation and operation instructions for the Performance Wizard, and follow the instructions applicable to your network platform.

All of these reports can be seen online as well as provided on printed reports.

Displaying the Log-in Screen

The SLM Reports package is available for both network administrators and customers via the Web. You define the URL to access the SLM Reports, based on where you have located the SLM server directories, e.g., *x/OpenLane/index.html*

Upon entering the URL of the server, a login screen appears. The following screens differ, depending on whether you are

- Administering customer profiles and data collection as the network administrator, or
- Viewing selected reports as a customer.

Enter your customer ID. In the resulting pop-up window, enter your User ID or enter as an administrator, then your Password.

Reports Administration

As the network administrator, you have the ability to perform the following functions:

- Create, modify and delete customer profiles. Customer profiles contain information such as the customer's name, account number, address (including e-mail), phone number, a contact name, and any additional comments. Customer profiles also contain the customer's access level (either reports-only or administrative). Via customer profiles, you determine which Web server users have access to what FrameSaver SLV devices for the SLM Reports.
- Modify authorized user logins. Determine which Web server users are authorized to log in as the customer listed in the profile.
- Modify assigned devices. Determine which FrameSaver SLV devices in the network the customer listed in the profile can access.
- Administer data collection. Enable data collection on devices that have already been added to the OpenLane Device Explorer database. For data collection, a 12-hour window is recommended. Any data collection errors causing a delay of over 24 hours will result in a loss of data.

Viewing Reports

As a Web user with a customer profile defined by your network administrator, you have the ability to view reports for the FrameSaver SLV devices assigned to you. Upon entering your customer ID, your User ID and Password in the pop-up window, the FrameSaver SLV Reports window displays, giving you the opportunity to select one the reports.

For specific information on SLM Reports, refer to the SLM Reports online Help, which contains detailed information consisting of a description and typical uses for each report. An example is also provided to show how a company could use the information provided by this powerful tool.

Using NetScout Manager Plus

6

This chapter includes:

- Significant features of NetScout Manager Plus.
- Installation and setup of NetScout Manager Plus software.
- Configuration of NetScout Manager Plus.

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

The NetScout Advantage

NetScout Manager Plus features:

- Large central site location: Layers 2 through 7 monitoring
  Remote Probe location: Layers 1 through 3 monitoring
- RMON1 and RMON2 customization
- Flexible, customized, drill-down tool set
- Historical and real time analysis and reporting
- LAN, WAN, and switched LAN support
- Protocol analysis
- Threshold alarming
- Web access
- Familiar interface (almost identical to both Motif and Windows environments)
- Integrates with other management systems

See the sections that follow to make sure you have the necessary hardware and software to support this application.

For the latest hardware requirements, see the *NetScout Manager Plus Set Up & Installation Guide.* For the latest software requirements, see the *NetScout Manager/Plus & NetScout Server Administrator Guide*.

Using a NetScout Manager Plus NMS Application

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 and configure NetScout Probe on network segments you want to monitor, as shown in *SLV Frame Relay Access* in Chapter 3, *Typical Applications*.

Installing NetScout Manager Plus

Installation instructions are located in Chapter 2 of the *NetScout Manager/Plus & NetScout Server Administrator Guide.* Depending upon your platform, see either:

- *Installing NSS/NSM/NSM+ Unix Version*
- *Installing NSS/NSM/NSM+ Windows Version*

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 will need to:

- Copy the OpenLane Performance Wizard 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.

Before You Get Started

Before getting started, you need to copy some OpenLane Performance Wizard directories to a NetScout Manager Plus user directory. Performance Wizard 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.

The Performance Wizard paradyne directories include the following:

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

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

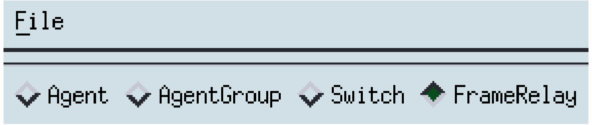
See *Adding SLV Alarms Using a Template* on page 6-8 and *Creating History Files* on page 6-13 for additional information.

Adding FrameSaver SLV Units to the NetScout Manager Plus Network

▶ Procedure

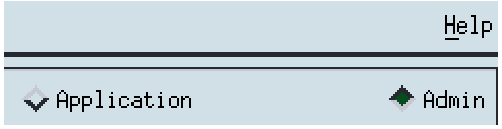
1. Bring up the NetScout Manager Plus main window.

2. Select the FrameRelay radio button from the agent type selection bar (on the left side of the window).

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

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

4. Click on the Config Manager icon to open the Configuration Manager main window.

5. Select the Add... button (down the center of the screen).

6. Minimally, enter the following:

   — Agent name

   — IP address

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

   — Properties File: Select paradyne.

7. Select the OK button at the bottom of the screen to add the agent, discover its DLCIs, and return to the Configuration Manager main window.

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

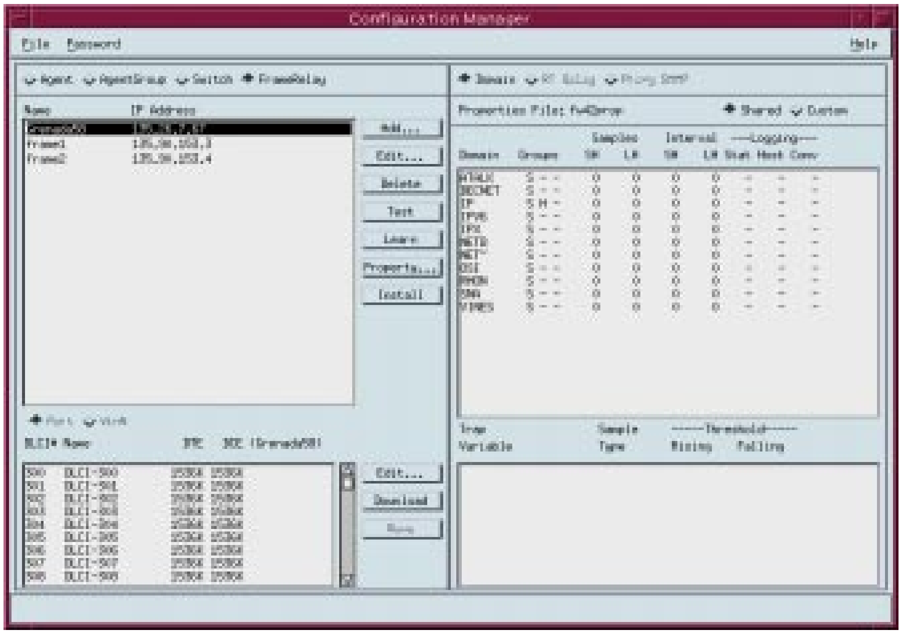
8. Select the Test button (fourth button down, center of the screen) to make sure you can communicate with the agent.

Refer to *Adding Frame Relay Agents* in Chapter 5 of 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.



Name	IP Address
[illegible]	[illegible]
Frame1	135.38.153.3
Frame2	135.38.153.4

DLCI#	Name	DTE	DCE (Grenada50)
500	DLCI-500	1536K	1536K
501	DLCI-501	1536K	1536K
502	DLCI-502	1536K	1536K
503	DLCI-503	1536K	1536K
504	DLCI-504	1536K	1536K
505	DLCI-505	1536K	1536K
506	DLCI-506	1536K	1536K
507	DLCI-507	1536K	1536K
508	DLCI-508	1536K	1536K

Properties File: fv4Group

		Samples		Interval		---Logging---		
Domain	Groups	SH	LH	SH	LH	Stat	Host	Conv
ATALK	S - -	0	0	0	0	-	-	-
DECNET	S - -	0	0	0	0	-	-	-
IP	S H -	0	0	0	0	-	-	-
IPV6	S - -	0	0	0	0	-	-	-
IPX	S - -	0	0	0	0	-	-	-
NETB	S - -	0	0	0	0	-	-	-
NET~	S - -	0	0	0	0	-	-	-
OSI	S - -	0	0	0	0	-	-	-
RMON	S - -	0	0	0	0	-	-	-
SNA	S - -	0	0	0	0	-	-	-
VINES	S - -	0	0	0	0	-	-	-

Trap	Sample	-----Threshold-----	
Variable	Type	Rising	Falling

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

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

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.

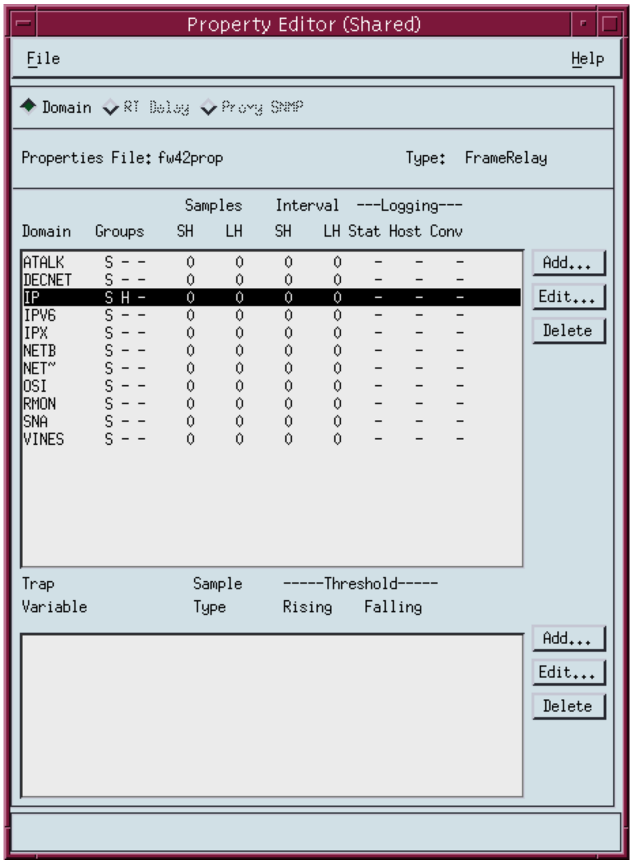
Correcting Domains and Groups

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* on page 6-5.

Procedure

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



Properties File: fw42prop   Type: FrameRelay

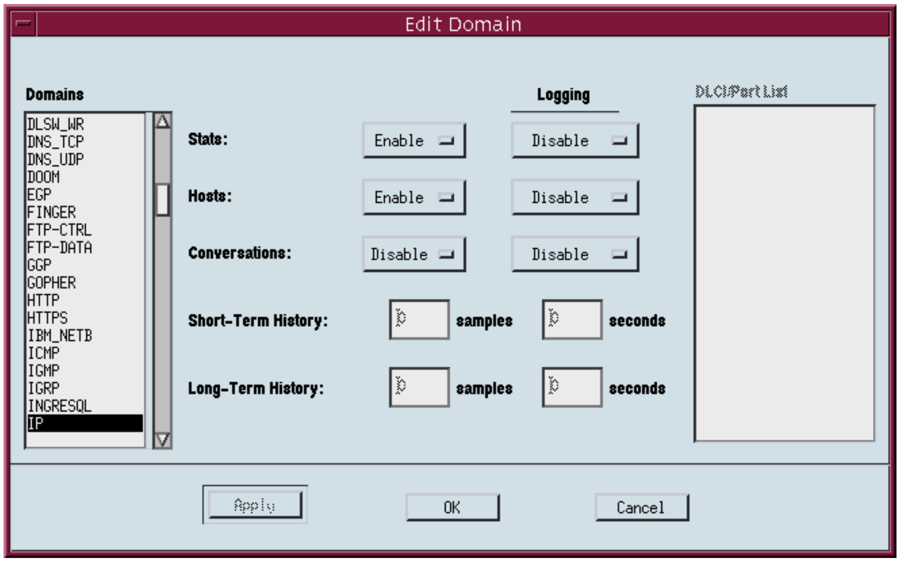
		Samples		Interval		---Logging---		
Domain	Groups	SH	LH	SH	LH	Stat	Host	Conv
ATALK	S - -	0	0	0	0	-	-	-
DECNET	S - -	0	0	0	0	-	-	-
IP	S H -	0	0	0	0	-	-	-
IPV6	S - -	0	0	0	0	-	-	-
IPX	S - -	0	0	0	0	-	-	-
NETB	S - -	0	0	0	0	-	-	-
NET~	S - -	0	0	0	0	-	-	-
OSI	S - -	0	0	0	0	-	-	-
RMON	S - -	0	0	0	0	-	-	-
SNA	S - -	0	0	0	0	-	-	-
VINES	S - -	0	0	0	0	-	-	-

	Sample	-----Threshold-----	
Trap Variable	Type	Rising	Falling

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.



Stats: Enable Disable

Hosts: Enable Disable

Conversations: Disable Disable

Short-Term History: samples seconds

Long-Term History: samples seconds

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 Chapter 5 of 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. Paradyne provides a template for configuring alarms. DLCI alarms can be configured manually, but using the Paradyne alarm defaults template greatly reduces configuration time.

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

— Frames Sent (SLVFramesSnt)

— Tx CIR Utilization (SLVTxCIRUtil)

— Tx DLCI Utilization (SLVTxDLCIUtil)

— Frames Received (SLVFramesRec)

— Rx DLCI Utilization (SLVrxDLCIUtil)

— Frames Sent Above CIR (SLVFramesTxAbvCIR)

— Average Latency (AverageLatency)

— Current Latency (CurrentLatency)

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

To configure alarms manually, see *Adding SLV Alarms Manually* on page 6-11.

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 (see the window on page 6-5).

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* on page 6-9 if any default settings need to be changed.

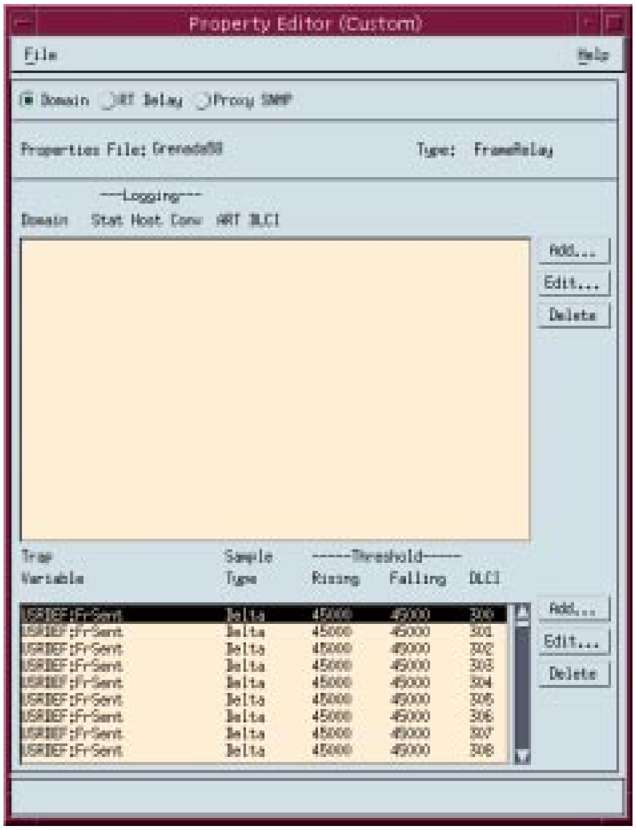
Editing Alarms

▶ 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 (see the window on page 6-5).

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.



● Domain ○ ART Delay ○ Proxy SNMP

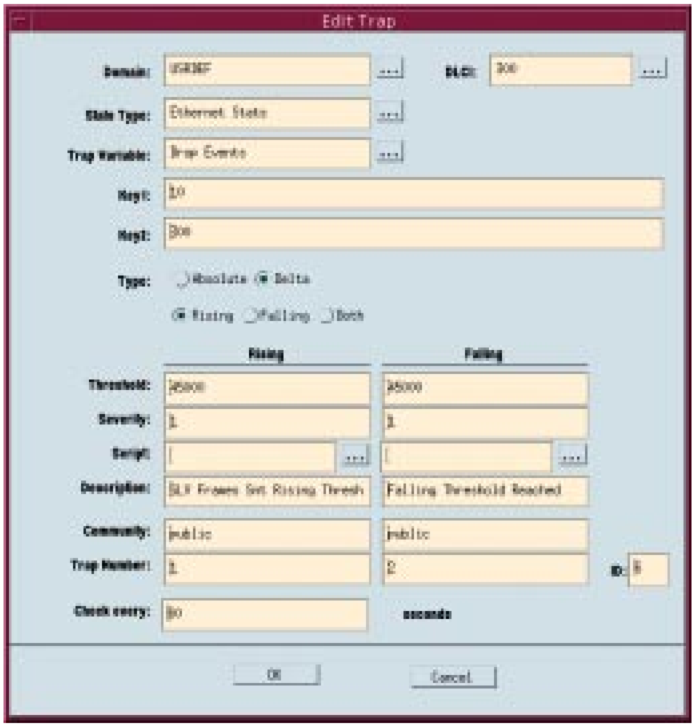
Properties File: Grenada88 Type: FrameRelay

	---Logging---				
Domain	Stat	Host	Conv	ART	DLCI

Trap	Sample	-----Threshold-----		
Variable	Type	Rising	Falling	DLCI
USRDEF:Fr-Sent	Delta	45000	45000	300
USRDEF:Fr-Sent	Delta	45000	45000	301
USRDEF:Fr-Sent	Delta	45000	45000	302
USRDEF:Fr-Sent	Delta	45000	45000	303
USRDEF:Fr-Sent	Delta	45000	45000	304
USRDEF:Fr-Sent	Delta	45000	45000	305
USRDEF:Fr-Sent	Delta	45000	45000	306
USRDEF:Fr-Sent	Delta	45000	45000	307
USRDEF:Fr-Sent	Delta	45000	45000	308

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

   The Edit Trap window opens.



Edit Trap

Domain: USR36F

DLCI: 300

Stats Type: Ethernet Stats

Trap Variable: Drop Events

Key1: 10

Key2: 300

Type: ○ Absolute ● Delta

● Rising ○ Falling ○ Both

	Rising	Falling
Threshold:	25000	25000
Severity:	1	1
Script:		
Description:	SLF Frames Snt Rising Thresh	Falling Threshold Reached
Community:	public	public
Trap Number:	1	2

ID: 8

Check every: 30 seconds

4. Edit any trap defaults that may be required. See Step 4 on page 6-12 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 Chapter 8 of 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.

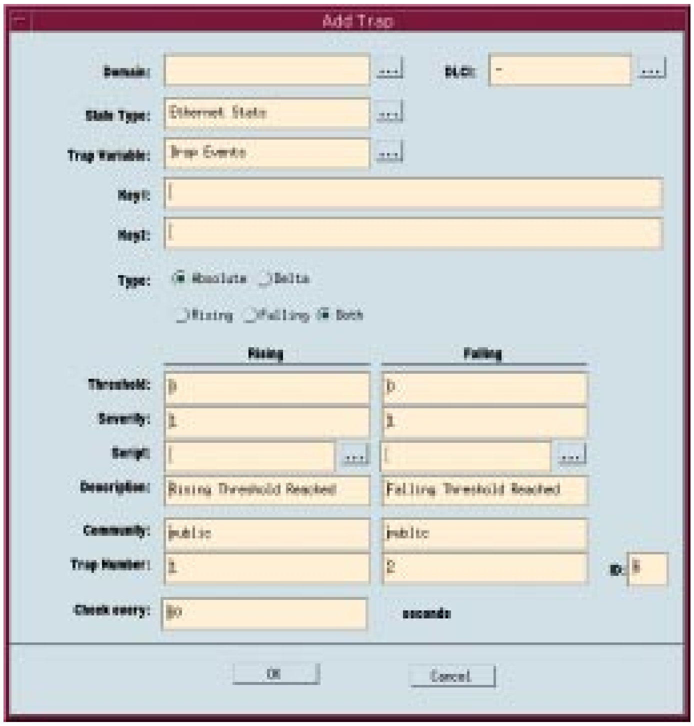
When configuring alarms manually, every alarm must be configured for each DLCI; that is, if there are eight alarms and 20 DLCIs, 160 trap configurations must be created (8 x 20). For this reason, it is recommended that the Paradyne defaults be used. Follow the procedure below to configure alarms manually.

To load Paradyne default settings for alarms, follow the procedure on page 6-8.

▶ 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 (see the window on page 6-5).
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 on page 6-9).
3. Select a DLCI from the Trap list, and select the Add... button (to the right of the list). The Add Trap window opens.



Domain:

DLCI: -

Stats Type: Ethernet Stats

Trap Variable: Drop Events

Key1:

Key2:

Type: ● Absolute ○ Delta

○ Rising ○ Falling ● Both

	Rising	Falling
Threshold:	0	0
Severity:	1	1
Script:		
Description:	Rising Threshold Reached	Falling Threshold Reached
Community:	public	public
Trap Number:	1	2

ID: 8

Check every: 30 seconds

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 Chapter 8, *Configuring Alarms,* of 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.

Paradyne 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 **`PerfWiz/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. Paradyne uses these two tables 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. The frame relay interface number 101015001 must replace @IFN, and the DLCI number to be monitored must replace @DLCI.

   Example: frCircuitSentFrames
   Change "**`1.3.6.1.2.1.10.32.2.1.6.@IFN.@DLCI`**"
   to "**`1.3.6.1.2.1.10.32.2.1.6.101015001.301`**"

   The only valid interface number for a FrameSaver 9126 or 9128 is 101015001.
4. Edit the new file, as needed.

Refer to *Creating .UDH Files* in Chapter 28, *Using Custom History*, of the *NetScout Manager Plus User Guide* for additional information.

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 User History Data* on page 6-17 to verify that the user-defined history files have been loaded.

Refer to *installing .UDH Files* in Chapter 28, *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.

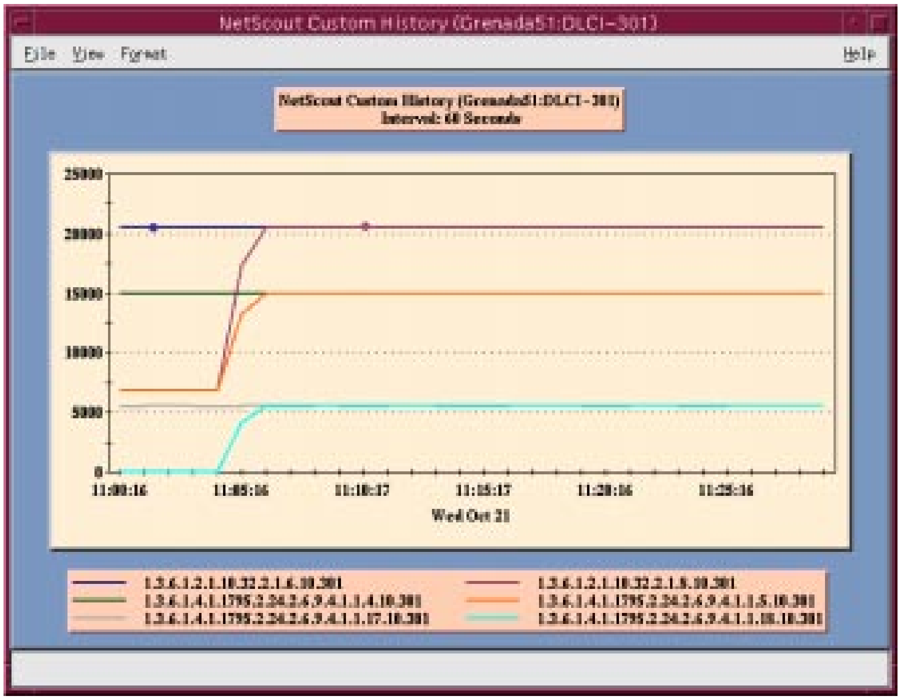
   The appropriate icons appear.

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.

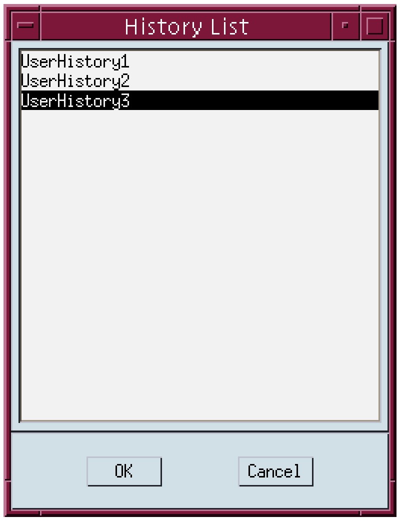
4. Click on the Custom History icon. The NetScout Custom History window opens.

   Adjust the size of the window so the entire report is shown.



5. Select History List from the View menu. The History List window opens.

   The newly defined user history variables should appear on this list.

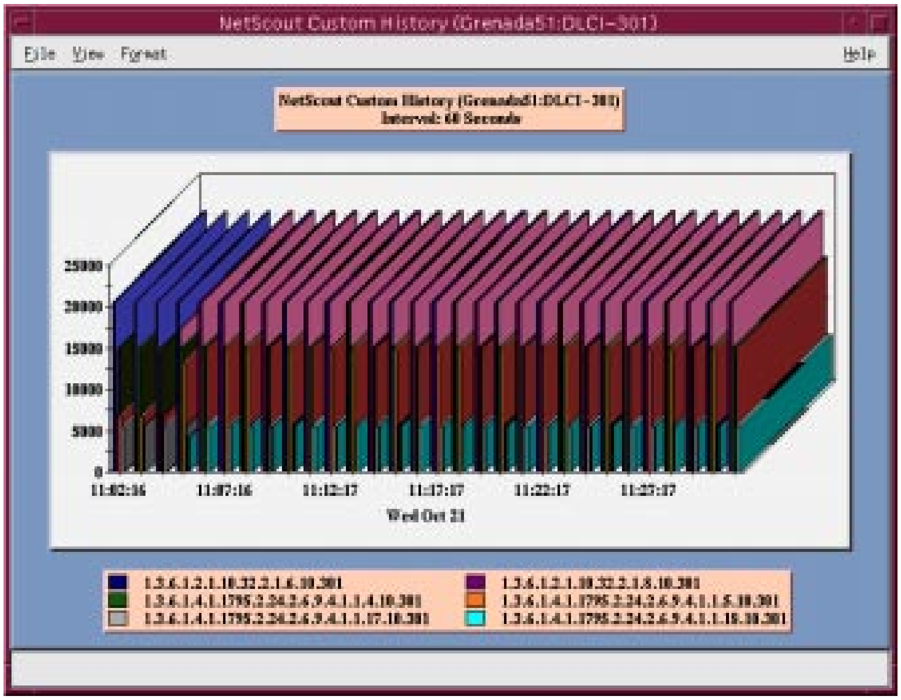


UserHistory1
UserHistory2
UserHistory3

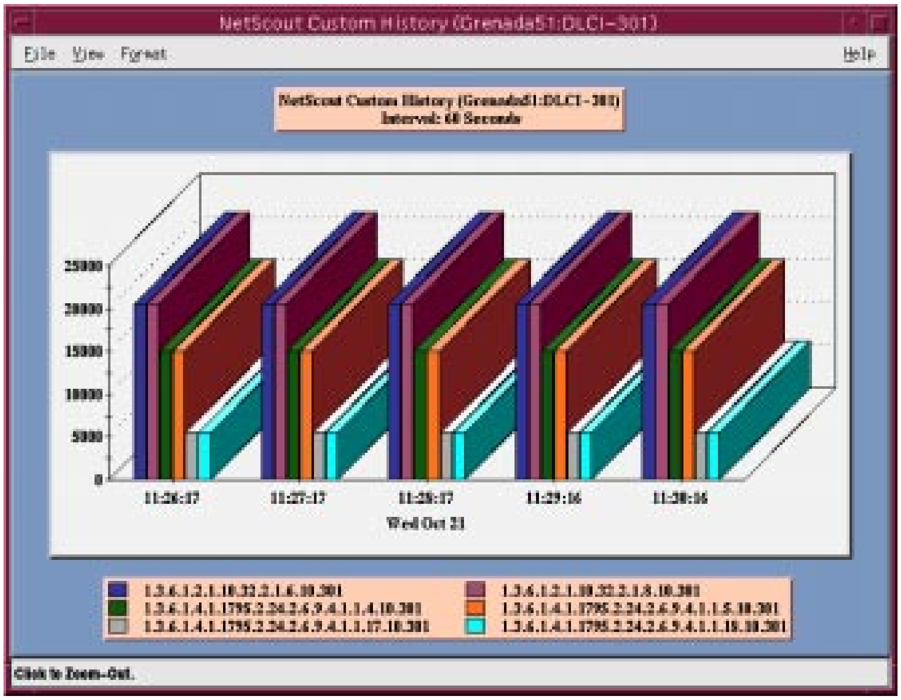
6. Highlight the desired set of user history variables, and select the OK button.

   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.



Click to Zoom-Out.

8. Click anywhere on this window to return to the previous window view (see Step 7 on page 6-17).

Refer to *Launching User History* and *Understanding Custom History Display* in Chapter 28, *Using Custom History*, of the *NetScout Manager Plus User Guide* for additional information.

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:

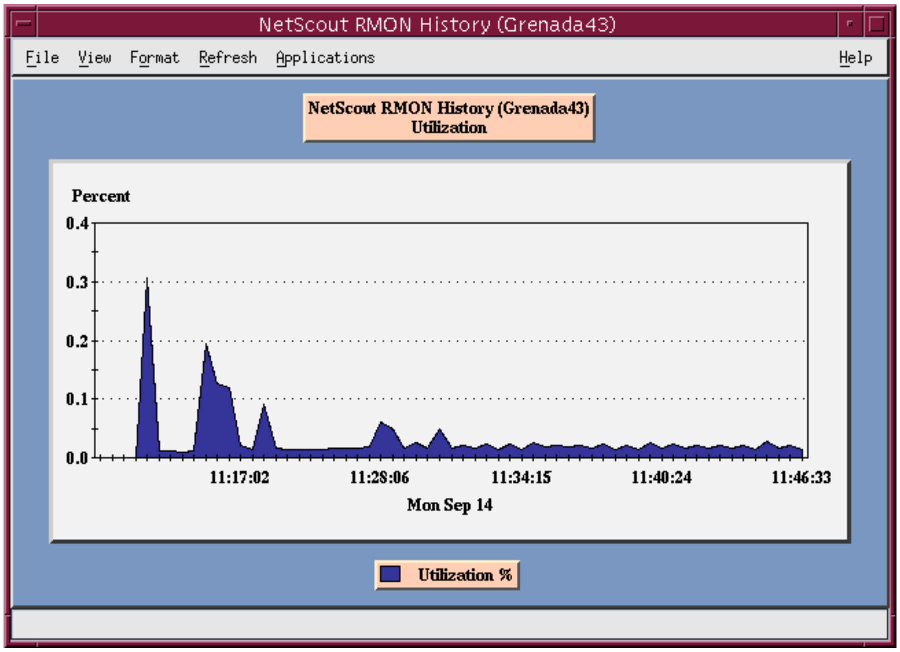
Only the Traffic and Protocol radio buttons on the application selection bar are supported for FrameSaver SLV agents.

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 Performance Wizard, 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.

Concord's Network Health

7

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 integrates FrameSaver SLV enhanced performance statistics into its reporting package (see the At-a-Glance report on page 7-19). To get this report, you need Network Health R4.01 or higher.

This chapter includes Network Health information as it relates to FrameSaver SLV products.

- *Installation and Setup of Network Health* and reports on page 7-2.
- *Viewing Network Health Charts and Tables* on page 7-3.
- *Reports Applicable to SLV Units* on page 7-9.

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

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 that you license the Poller application so you can poll SLV units and collect data.

Before starting the installation:

- Verify the amount of disk and swap space required for your network.
- Make sure that your operating system is appropriately configured.
- Have user account information ready so you can access licensed applications.

To use this application:

1. Install the Concord Network Health software and open the application.
2. Enter license information from the Network Health License Information form so specific Network Health applications can be used.
3. Discover network elements, devices, and interfaces in the network (see page 7-3).
4. Configure the Network Health applications, then save them (see page 7-4).
5. Organize elements into groups for reporting purposes (see page) 7-5).
6. Set up and run reports (see page 7-6).

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 to provide 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 creates definitions in the Poller Configuration, which are used to poll the units.

IP addresses and the Community String (Community Names in the FrameSaver unit) must be entered for Network Health to find the SLV units on the network and discover their elements. *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 unit 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 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, it could take anywhere from a few minutes to an hour, or longer, depending upon the size of your network, to discover all elements in the network.

See *Discovering Elements* in the *Network Health User Guide* for additional information and 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.

If an SLV unit does not have CIR configured, or it is not configured correctly, Network Health sets the unit's CIR to 0 kbps. For this reason, you should reconfigure the unit's CIR before Network Health polls it. If 0 kbps is the speed setting, you will need to edit the unit's CIR from Network Health.

Additional information that can be edited includes:

- Element name
- Community string
- Polling status and rates
- SNMP index for the interface
- Agent type
- Desciption information

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. It 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. The following are defined when specifying a report:

- Report to be run
- Group
- Daily, a specific day(s) of the week, weekly, or monthly report
- Destination of the report

NOTE:

Not all reports can be ordered or scheduled on a monthly basis. See the *Network Health Reports Guide* to determine what reports can be generated on a monthly basis.

▶ Procedure

To run a Health report:

1. From the console, select Run from the Reports menu, then Health Reports.

   The Run Health Report dialog box opens.
2. In the Report section, select a report from the drop-down list.
3. In the Subject section, select WAN from the drop-down list.
4. From the drop-down list next to Group, select the newly created group.
5. In the Time Range section, specify the day to be included on the report.
6. In the Output section, select either the Screen or Printer radio button. A check mark will appear in the selected box.
7. Select the OK button to run the selected report.

   The Generating Report window opens, showing the report's progress. The window closes when the report screen comes up or the report is printed.

See *Running Reports from the Console* in the *Network Health Reports Guide* for additional information. It also tells you how to schedule automatic report generation.

Viewing Network Health Charts and Tables

Network Health already supports the service level verifier capability provided by NetScout probes, FrameSaver SLVs.

The following frame relay reports support frame relay and FrameSaver SLV products.

Report	Description	Page
Exceptions Reports	Provide summary and detail information that identifies DLCIs with the highest incidence of errors, high bandwidth utilization, and trends.	7-9
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.	7-10
■ Leaders Summary Report	Identifies DLCIs having the highest volume and errors.	7-11
■ Elements Summary Report	Compares DLCI traffic with volume and the baseline, bandwidth utilization, and errors.	7-12
Supplemental Report	Shows DLCI availability and latency.	7-13
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 information for an enterprise.	7-14
■ IT Manager Service Level Report	Provides service level information for various groups.	7-15
■ Customer Service Level Report	Provides service level information for customers.	7-16
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.	7-18
■ Paradyne SLV Plus At-a-Glance Report	Consolidates transmit burst analysis, network latency, dropped frames, frame size distribution, and availability information.	7-19
Trend Reports	Performs trend analysis on up to ten specified variables for DLCIs.	7-20

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 the 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 report on page 7-18, 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.

Using the report on page 7-19, all the enhanced network statistics that only an SLV unit 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 on page 7-9 for information about Health Index ratings.

Printed Reports

All of the charts and tables seen online can also be provided on printed reports. The following pages show an example of a printed *LAN/WAN Health Report*.

Reports Applicable to SLV Units

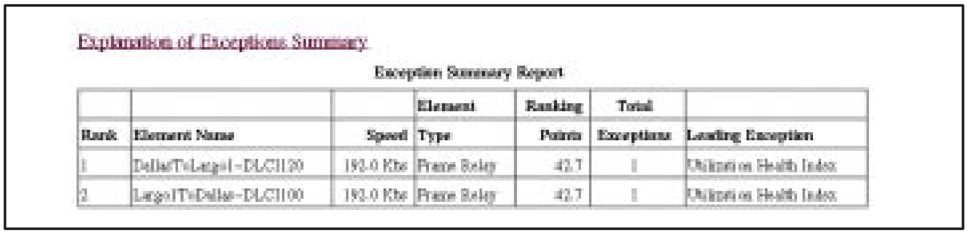
This section identifies the Network Health reports that apply to FrameSaver SLV products, summarizes relevant information, and tells you how to use the reports.

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*.

Exceptions Reports

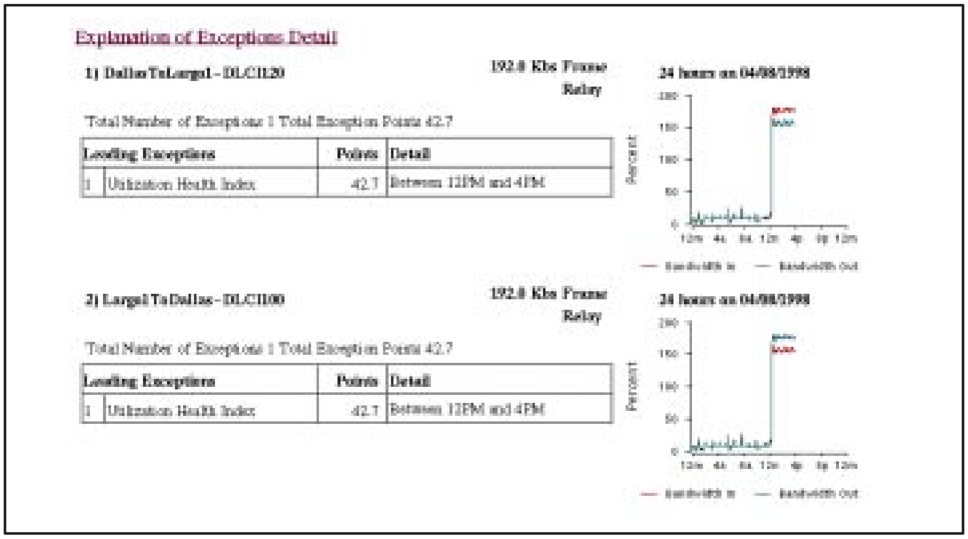
These reports identify those DLCIs that have exceeded a specified number of accumulated *exception points*. It is a good idea to run this report daily so that DLCIs having the most problems can be attended to first. DLCIs contained on this report need immediate attention.



Explanation of Exceptions Summary

Exception Summary Report

			Element	Ranking	Total	
Rank	Element Name	Speed	Type	Points	Exceptions	Leading Exception
1	DallasToLargo1-DLCI120	192.0 Kbs	Frame Relay	42.7	1	Utilization Health Index
2	Largo1ToDallas-DLCI100	192.0 Kbs	Frame Relay	42.7	1	Utilization Health Index



Explanation of Exceptions Detail

1) DallasToLargo1 - DLCI120

192.0 Kbs Frame Relay

Total Number of Exceptions 1 Total Exception Points 42.7

Leading Exceptions		Points	Detail
1	Utilization Health Index	42.7	Between 12PM and 4PM

2) Largo1ToDallas - DLCI100

192.0 Kbs Frame Relay

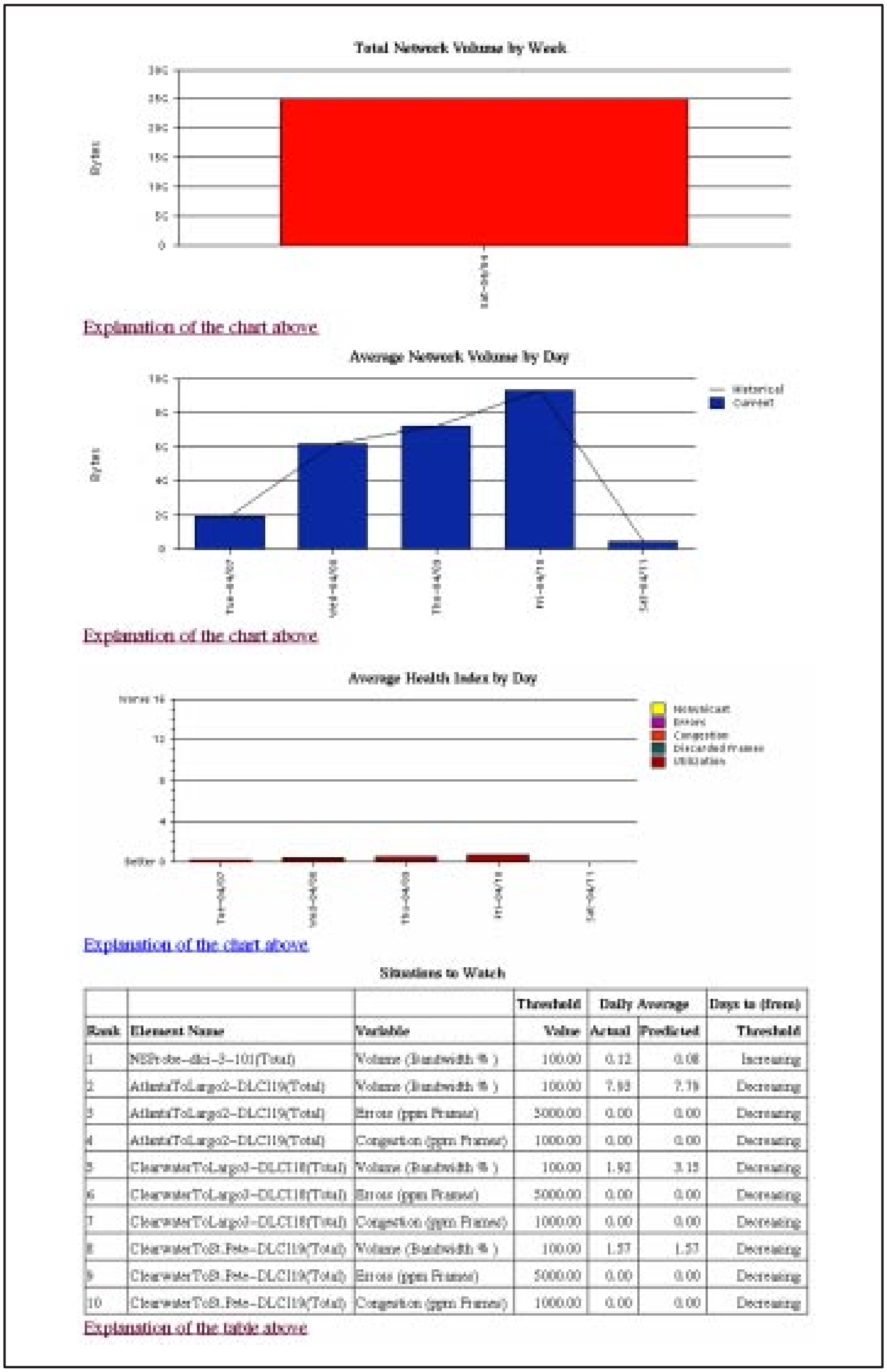
Total Number of Exceptions 1 Total Exception Points 42.7

Leading Exceptions		Points	Detail
1	Utilization Health Index	42.7	Between 12PM and 4PM

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.

Network Summary Report

This set of charts and the table provides a summary of the frame relay network. Use this report for planning and to predict when a DLCI might run into problems



Explanation of the chart above

Explanation of the chart above

Explanation of the chart above

Situations to Watch

			Threshold	Daily Average		Days to (from)
Rank	**Element Name**	**Variable**	**Value**	**Actual**	**Predicted**	**Threshold**
1	NEProbe-dlci-3-101(Total)	Volume (Bandwidth %)	100.00	0.12	0.08	Increasing
2	AtlantaToLargo2-DLCI19(Total)	Volume (Bandwidth %)	100.00	7.93	7.78	Decreasing
3	AtlantaToLargo2-DLCI19(Total)	Errors (ppm Frames)	5000.00	0.00	0.00	Decreasing
4	AtlantaToLargo2-DLCI19(Total)	Congestion (ppm Frames)	1000.00	0.00	0.00	Decreasing
5	ClearwaterToLargo3-DLCI18(Total)	Volume (Bandwidth %)	100.00	1.92	3.15	Decreasing
6	ClearwaterToLargo3-DLCI18(Total)	Errors (ppm Frames)	5000.00	0.00	0.00	Decreasing
7	ClearwaterToLargo3-DLCI18(Total)	Congestion (ppm Frames)	1000.00	0.00	0.00	Decreasing
8	ClearwaterToSt.Pete-DLCI19(Total)	Volume (Bandwidth %)	100.00	1.57	1.57	Decreasing
9	ClearwaterToSt.Pete-DLCI19(Total)	Errors (ppm Frames)	5000.00	0.00	0.00	Decreasing
10	ClearwaterToSt.Pete-DLCI19(Total)	Congestion (ppm Frames)	1000.00	0.00	0.00	Decreasing

Explanation of the table above

Leaders Summary Report

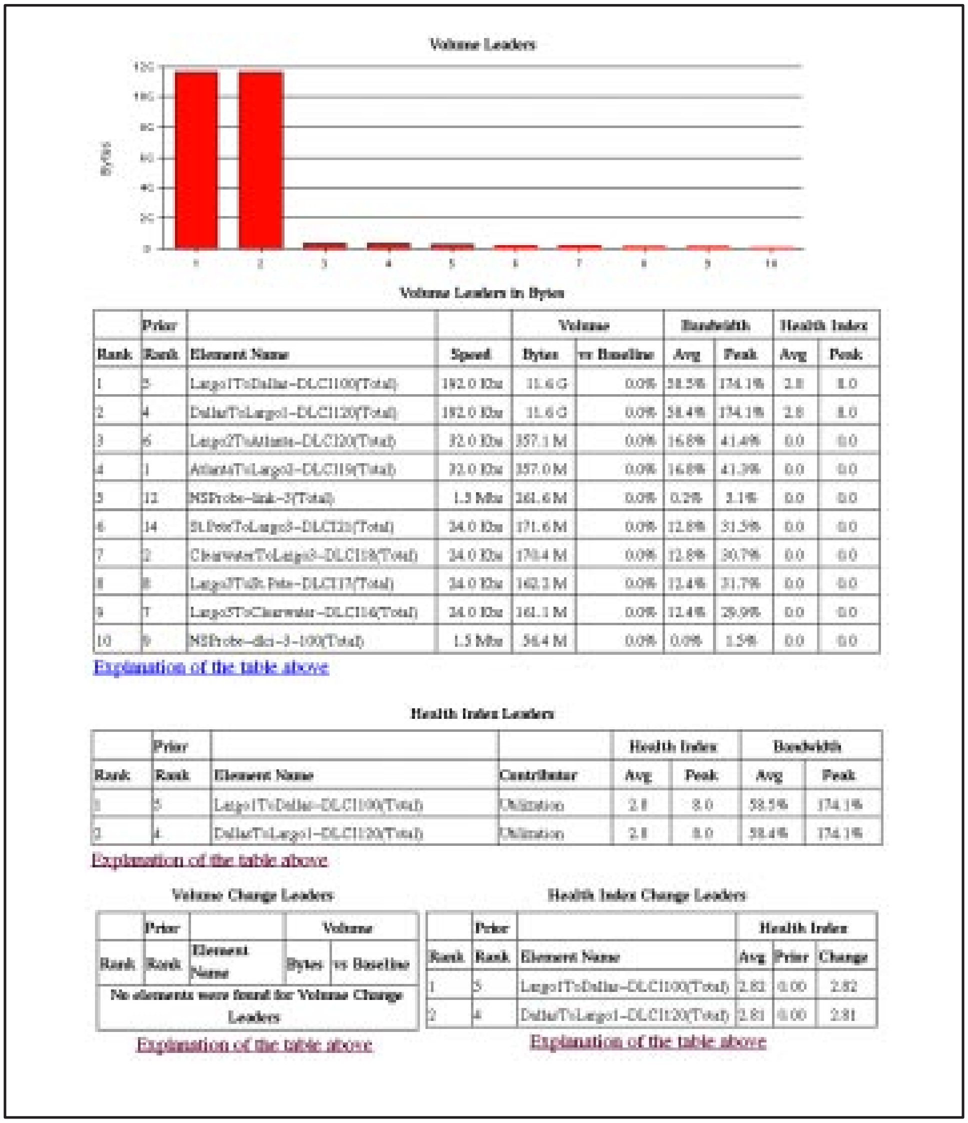
The following chart and tables list the ten highest-volume DLCIs. High traffic volume may be increasing latency, and the high Health Index rating indicates problems. It is a good idea to run these reports daily so a norm can be established. The same DLCIs should appear. Use this chart and table to alert 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.



Volume Leaders in Bytes

	Prior			Volume		Bandwidth		Health Index	
Rank	Rank	Element Name	Speed	Bytes	vs Baseline	Avg	Peak	Avg	Peak
1	5	Largo1ToDallas-DLCI100(Total)	192.0 Kbs	11.6 G	0.0%	58.5%	174.1%	2.8	8.0
2	4	DallasToLargo1-DLCI120(Total)	192.0 Kbs	11.6 G	0.0%	58.4%	174.1%	2.8	8.0
3	6	Largo2ToAtlanta-DLCI20(Total)	32.0 Kbs	357.1 M	0.0%	16.8%	41.4%	0.0	0.0
4	1	AtlantaToLargo2-DLCI19(Total)	32.0 Kbs	357.0 M	0.0%	16.8%	41.3%	0.0	0.0
5	12	NSProbe-link-3(Total)	1.5 Mbs	261.6 M	0.0%	0.2%	3.1%	0.0	0.0
6	14	St.PeteToLargo3-DLCI21(Total)	64.0 Kbs	171.6 M	0.0%	12.8%	31.5%	0.0	0.0
7	2	ClearwaterToLargo3-DLCI18(Total)	64.0 Kbs	170.4 M	0.0%	12.8%	30.7%	0.0	0.0
8	8	Largo3ToSt.Pete-DLCI17(Total)	64.0 Kbs	162.2 M	0.0%	12.4%	31.7%	0.0	0.0
9	7	Largo5ToClearwater-DLCI16(Total)	64.0 Kbs	161.1 M	0.0%	12.4%	29.9%	0.0	0.0
10	9	NSProbe-dlci-3-100(Total)	1.5 Mbs	56.4 M	0.0%	0.0%	1.5%	0.0	0.0

Explanation of the table above

Health Index Leaders

	Prior			Health Index		Bandwidth	
Rank	Rank	Element Name	Contributor	Avg	Peak	Avg	Peak
1	5	Largo1ToDallas-DLCI100(Total)	Utilization	2.8	8.0	58.5%	174.1%
2	4	DallasToLargo1-DLCI120(Total)	Utilization	2.8	8.0	58.4%	174.1%

Explanation of the table above

Volume Change Leaders

	Prior		Volume	
Rank	Rank	Element Name	Bytes	vs Baseline
No elements were found for Volume Change Leaders				

Explanation of the table above

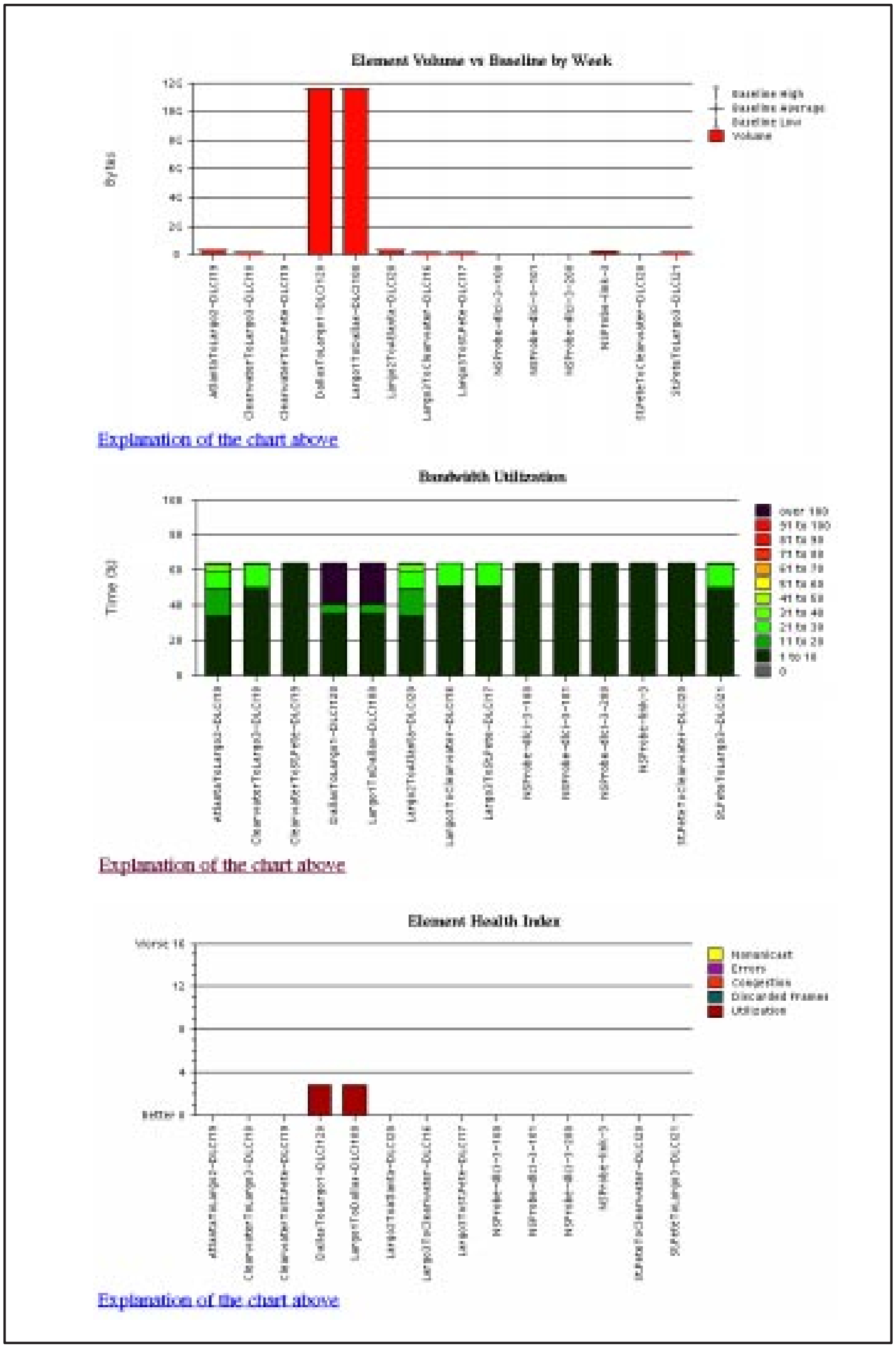
Health Index Change Leaders

	Prior		Health Index		
Rank	Rank	Element Name	Avg	Prior	Change
1	5	Largo1ToDallas-DLCI100(Total)	2.82	0.00	2.82
2	4	DallasToLargo1-DLCI120(Total)	2.81	0.00	2.81

Explanation of the table above

Elements Summary Report

Use this report for DLCI detail information and comparison. Several views of these charts are available. Use this chart to identify DLCIs with above or below average volume, and investigate. When there are any significant changes, investigate the cause.



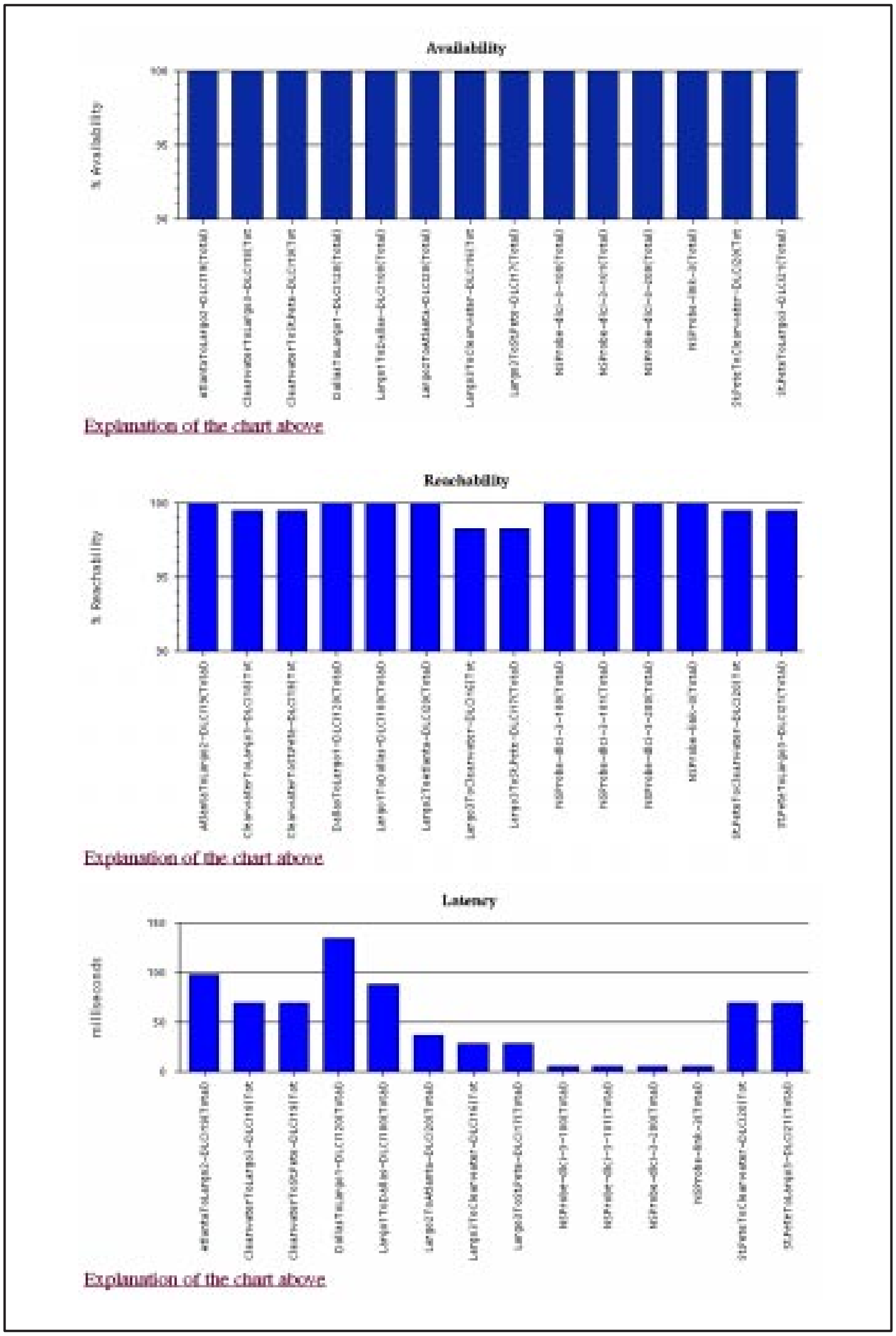
Explanation of the chart above

Explanation of the chart above

Explanation of the chart above

Supplemental Report

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.



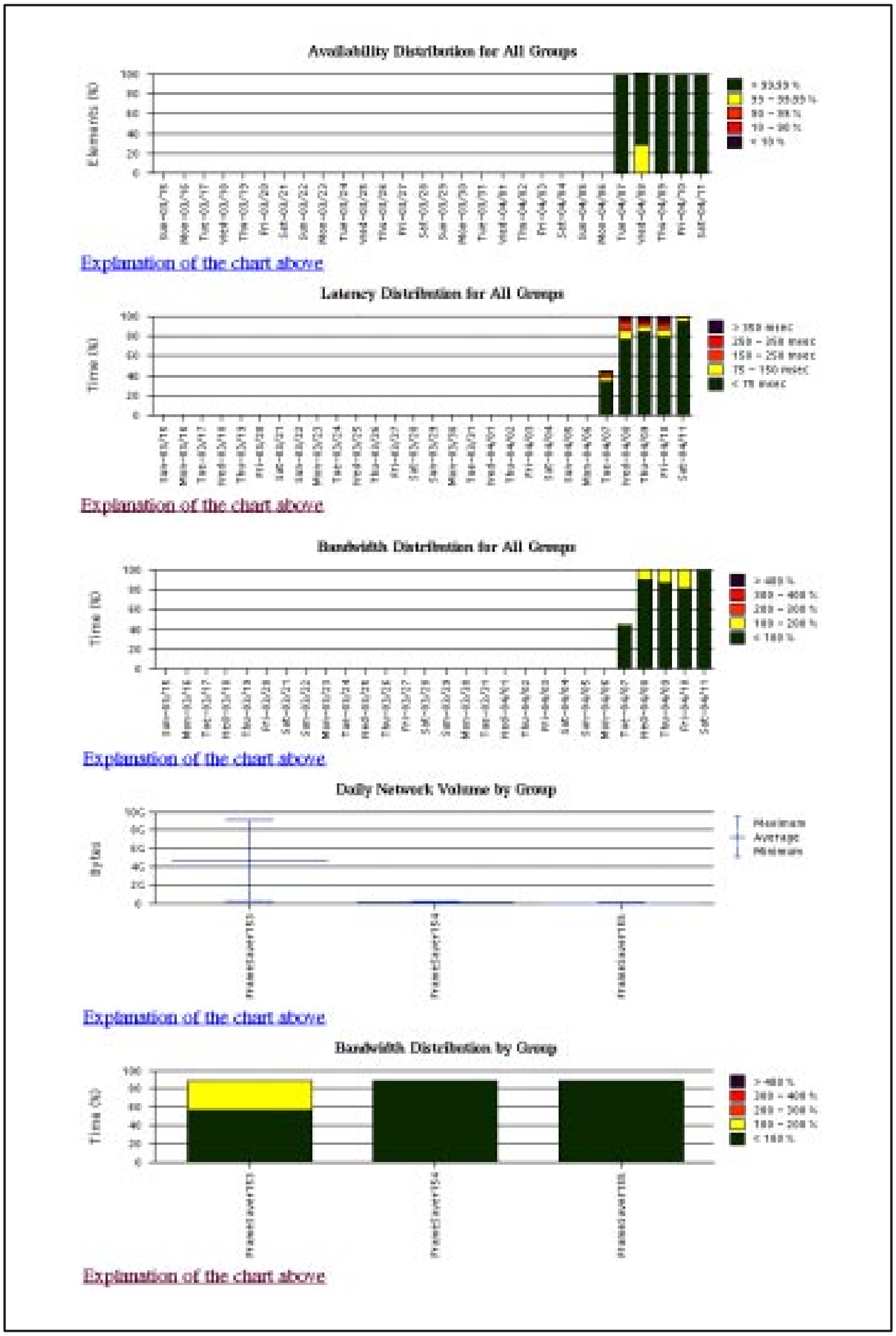
Explanation of the chart above

Explanation of the chart above

Explanation of the chart above

Executive Service Level Report

This report summarizes 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.



Availability Distribution for All Groups

Explanation of the chart above

Latency Distribution for All Groups

Explanation of the chart above

Bandwidth Distribution for All Groups

Explanation of the chart above

Daily Network Volume by Group

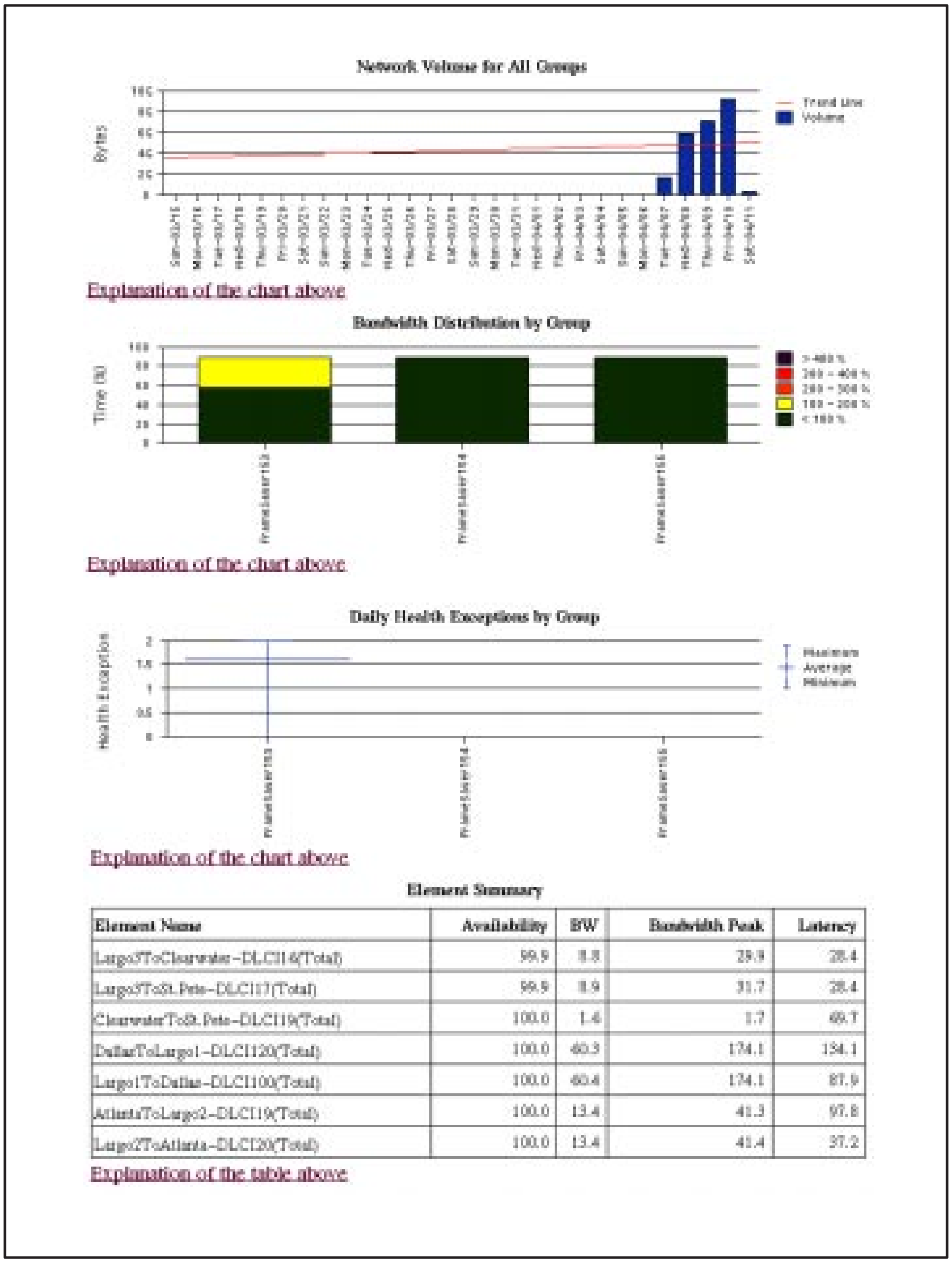
Explanation of the chart above

Bandwidth Distribution by Group

Explanation of the chart above

IT Manager Service Level Report

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.



Explanation of the chart above

Explanation of the chart above

Explanation of the chart above

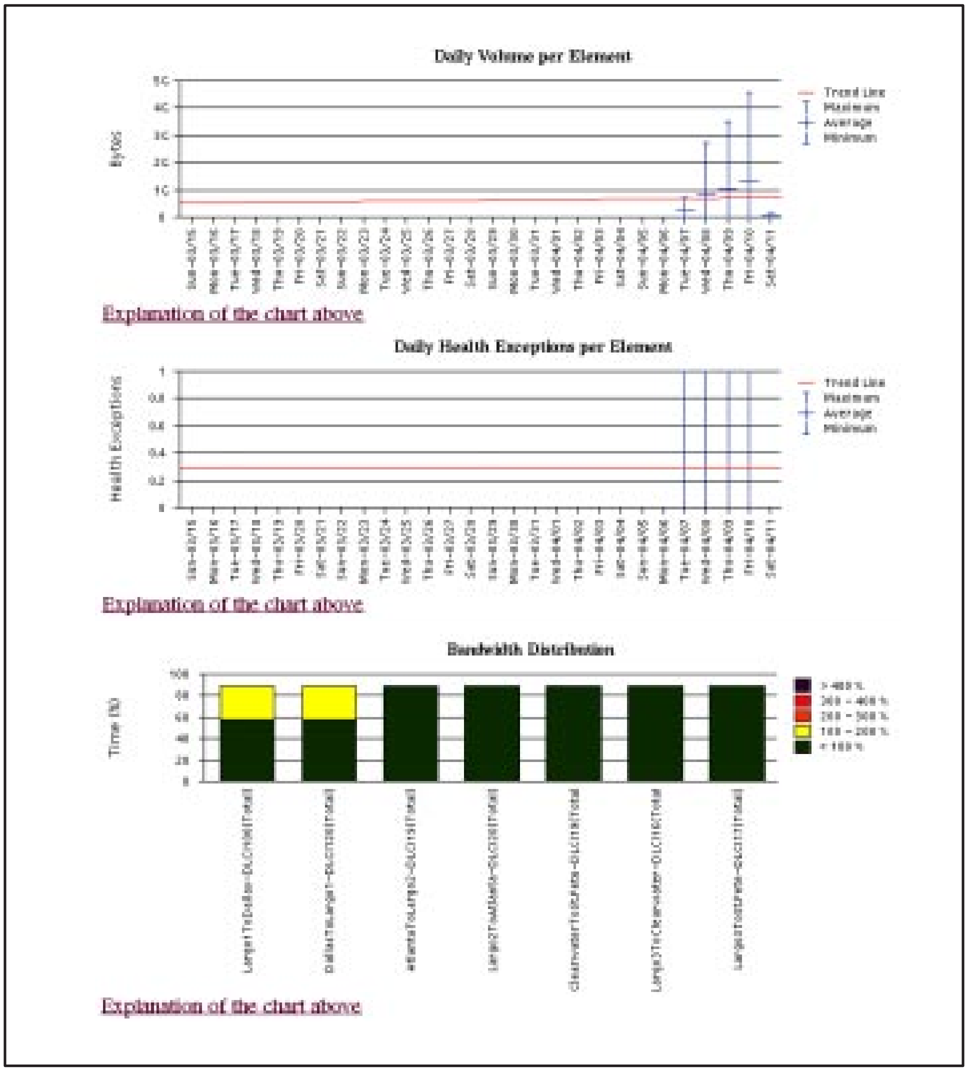
Element Summary

Element Name	Availability	BW	Bandwidth Peak	Latency
Largo3ToClearwater-DLCI16(Total)	99.9	8.8	29.9	28.4
Largo3ToSt.Pete-DLCI17(Total)	99.9	8.9	31.7	28.4
ClearwaterToSt.Pete-DLCI19(Total)	100.0	1.6	1.7	69.7
DallasToLargo1-DLCI120(Total)	100.0	40.3	174.1	134.1
Largo1ToDallas-DLCI100(Total)	100.0	40.4	174.1	87.9
AtlantaToLargo2-DLCI19(Total)	100.0	13.4	41.3	97.8
Largo2ToAtlanta-DLCI20(Total)	100.0	13.4	41.4	37.2

Explanation of the table above

Customer Service Level Report

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.

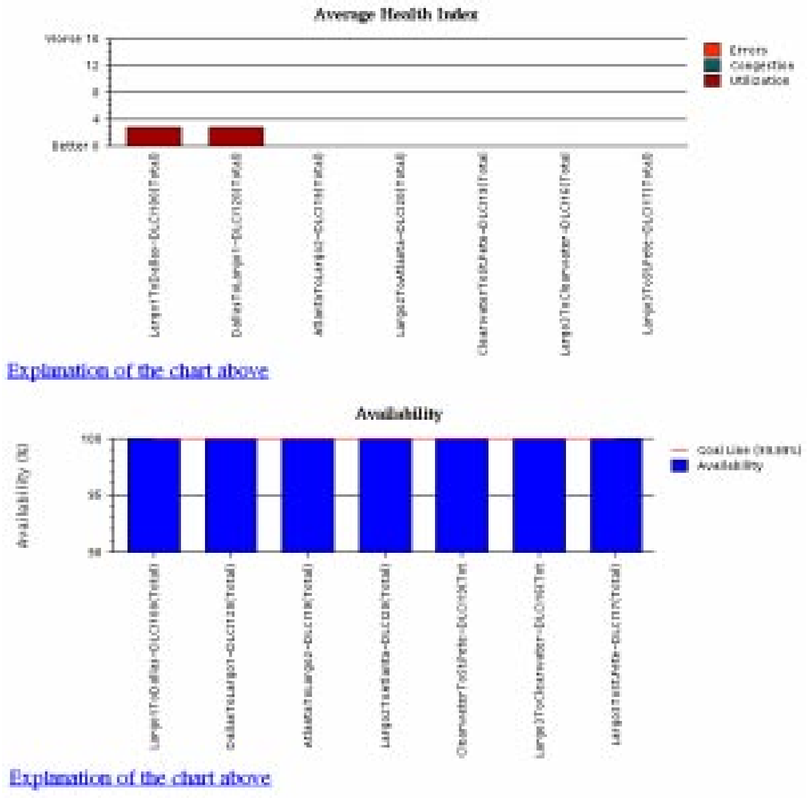


Explanation of the chart above

Explanation of the chart above

Explanation of the chart above

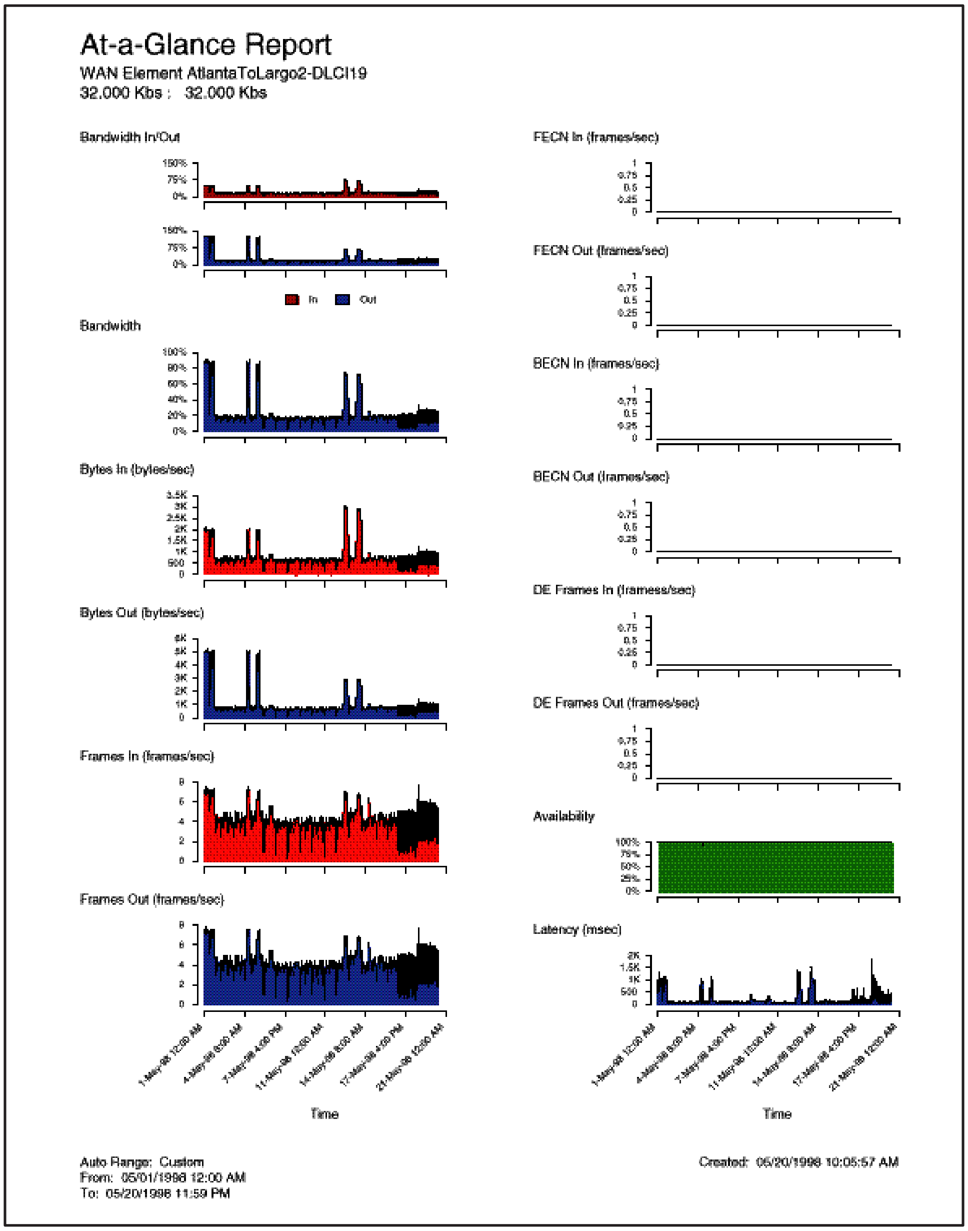
(The rest of this report is on the next page.)



See *LAN/WAN Service Customer Report* in the *Network Health Reports Guide* for information about this report.

At-a-Glance Reports

These reports consolidate a frame relay circuit’s performance over a specified period onto single page summaries. Use this report to compare the DLCI’s volume and utilization to the network performance indicators.



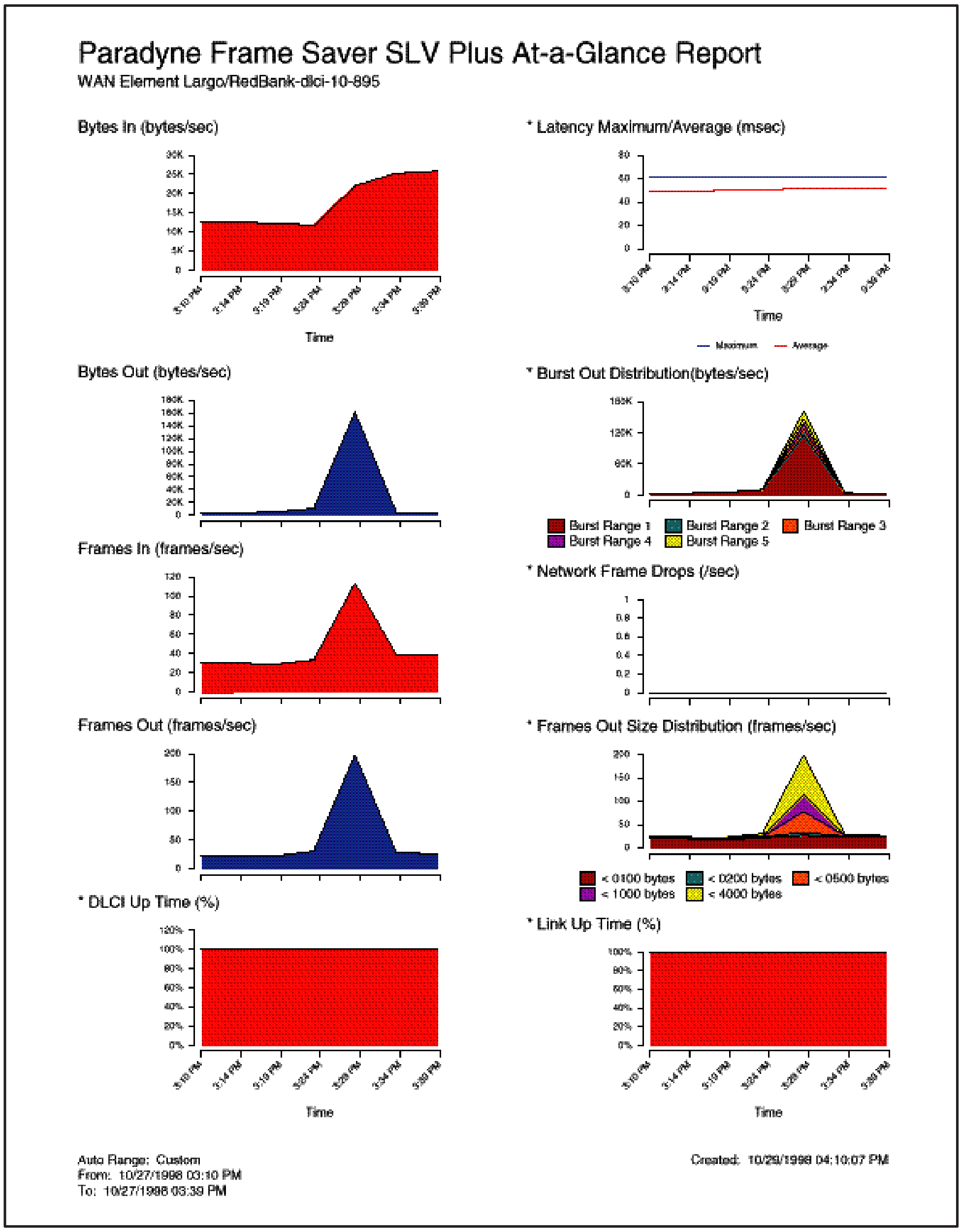
At-a-Glance Report

WAN Element AtlantaToLargo2-DLCI19
32.000 Kbs : 32.000 Kbs

Auto Range: Custom
From: 05/01/1998 12:00 AM
To: 05/20/1998 11:59 PM

Created: 05/20/1998 10:05:57 AM

The At-a-Glance report below is the first Network Health report to integrate the FrameSaver SLV's unique monitoring capabilities, using the unit's SLV-enhanced network statistics.



Paradyne Frame Saver SLV Plus At-a-Glance Report

WAN Element Largo/RedBank-dlci-10-895

Bytes In (bytes/sec)

* Latency Maximum/Average (msec)

Bytes Out (bytes/sec)

* Burst Out Distribution(bytes/sec)

Frames In (frames/sec)

* Network Frame Drops (/sec)

Frames Out (frames/sec)

* Frames Out Size Distribution (frames/sec)

* DLCI Up Time (%)

* Link Up Time (%)

Auto Range: Custom
From: 10/27/1998 03:10 PM
To: 10/27/1998 03:39 PM

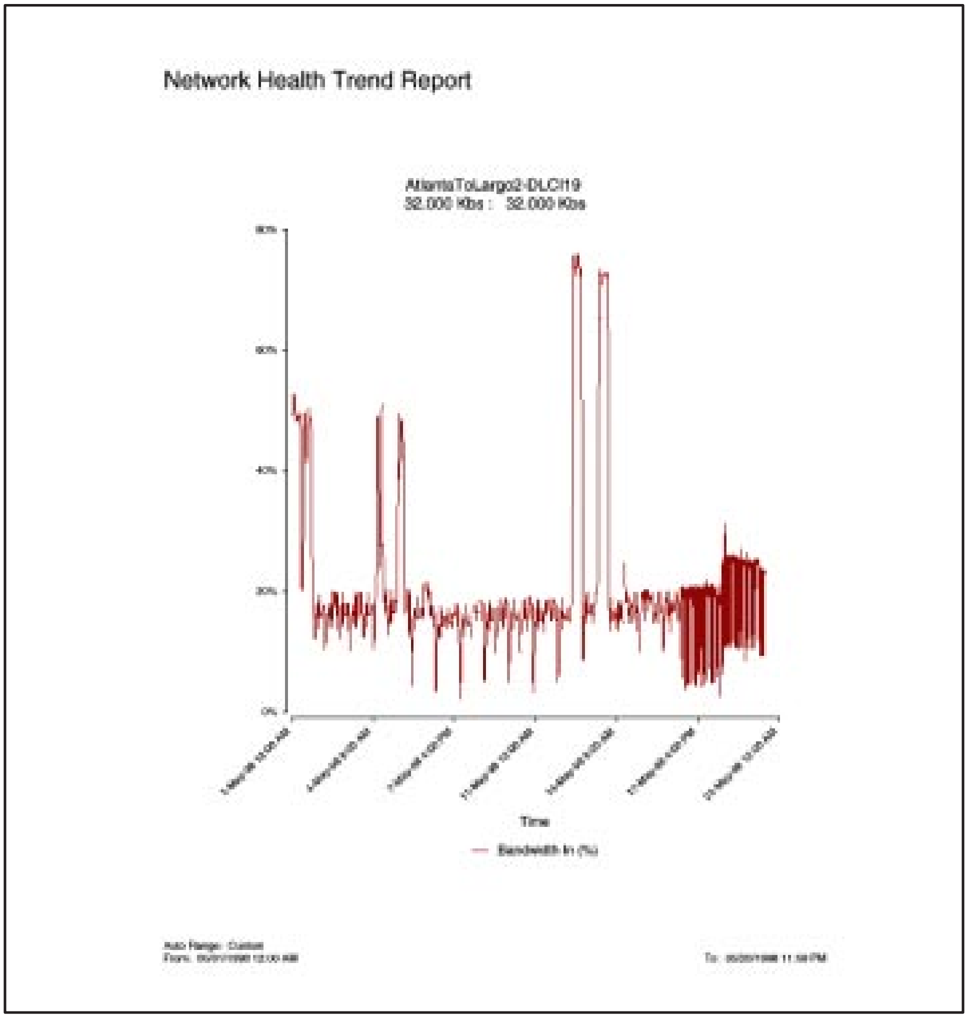
Created: 10/29/1998 04:10:07 PM

Trend Reports

Variables other than bandwidth can be selected for a trend report (e.g., burst octets); however, a bandwidth trend report (shown here) should be generated when investigating problems that appear on:

- Exceptions Reports (see page 7-9)
- Supplemental Report (see page 7-13)
- Health Reports

You can specify total bandwidth (both incoming and outgoing data), only incoming data bandwidth, or only outgoing data bandwidth. The trend report calculates the bandwidth for the data based upon the data rate and the amount of data in bytes.



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. For additional information about trend reports, see *LAN/WAN Trend Reports* in the *Network Health Reports Guide*.

Configuration

8

Setup and configuration instructions are included in the *FrameSaver SLV 9124 Installation Instructions*. This chapter provides additional information about the FrameSaver unit's features and a detailed description of the all the configuration options available.

- *Assigning Time Slots/Cross Connections* on page 8-36.
  - *Assigning Frame Relay Time Slots to the Network Interface* on page 8-36.
  - *Assigning DSX-1 Time Slots to the Network Interface* on page 8-37.
  - *DSX-1 Signaling Assignments and Trunk Conditioning* on page 8-39.
- *Configuring the System* on page 8-22. The following configuration option tables are included in this chapter:
- Table 8-1. System Frame Relay and LMI Options on page 8-23.
- Table 8-2. Service Level Verification Options on page 8-25.
- Table 8-3. General System Options on page 8-26.
- Table 8-5. DSX-1 Physical Options on page 8-32.
- Table 8-6. Data Ports Physical Options on page 8-34.
- Table 8-8. Frame Relay Options on page 8-42.
- Table 8-9. DLCI Record Options on page 8-49.
- Table 8-10. PVC Connection Options on page 8-52.
- Table 8-11. Node IP Options on page 8-54.
- Table 8-12. Management PVC Options on page 8-57.
- Table 8-13. General SNMP Management Options on page 8-61.
- Table 8-14. Telnet and FTP Session Options on page 8-62.
- Table 8-15. SNMP NMS Security Options on page 8-65.
- Table 8-16. SNMP Traps and Traps Dial-Out Options on page 8-68.
- Table 8-17. Communication Port Options on page 8-72.
- Table 8-18. External Modem (on Com Port) Options on page 8-76.

Setting Up the Unit

When configuring the system:

You need to . . .	**See . . .**
1. Configure the overall system options.	*Configuring System Options* on page 8-22.
2. Set up node IP information.	*Configuring Node IP Information* on page 8-54.
3. Configure physical interfaces.	*Setting Up Each Physical Interface* on page 8-28. *Configuring the Communication Port* on page 8-72, and RIP.
4. Change Auto-Configuration, if necessary.	*Setting Up Auto-Configuration* on page 8-10.
5. Configure frame relay LMI for interfaces.	*Configuring Frame Relay LMI for Interfaces* on page 8-42.
6. Create DLCI Records for interfaces.	*Configuring DLCI Records for Each Interface* on page 8-49.
7. Configure PVC connections.	*Configuring PVC Connections* on page 8-52.
8. Create a management PVC.	*Configuring Management PVCs* on page 8-57. *Setting Up So the Router Can Receive RIP* on page 8-19.
9. Set up access and management.	*Configuring General SNMP Management* on page 8-61. *Configuring Telnet and/or FTP Session Support* on page 8-62. *Configuring SNMP Traps and Trap Dial-Out* on page 8-66.

Considerations When Setting Up

We recommend that you decide how to configure the FrameSaver unit before actually configuring it.

When setting up the FrameSaver unit, you need to:

- Arrange for T1 service.
- Determine where PVCs will be required in your network. Refer to Chapter 3, *Typical Applications*, for assistance.
- Determine whether you will be using the Auto-Configuration feature. Refer to *Setting Up Auto-Configuration* on page 8-10.
- Determine whether you want SNMP traps generated, and how you would like them communicated to the management system.
- Decide how you want to manage this unit within the context of your network, and choose a management configuration:
  - Locally, via a PVC between the FrameSaver unit and a router attached to its DTE port.
  - Locally, through the COM port.
  - Remotely, through dedicated or multiplexed PVCs.
  - Remotely, from a remote terminal via a modem or Telnet connection.
- If managing the FrameSaver unit using an SNMP NMS or Telnet, select an IP addressing scheme. See Chapter 2, *Management Control*, for different management alternatives. See Appendix B, *IP Addressing*, for sample IP addressing schemes.
- Plan your T1 timeslot assignments, if applicable.

Selecting a Management Interface

Select one of the following management interfaces:

- **Asynchronous terminal access to the menu-driven user interface** – Over the FrameSaver unit's COM port or modem connection for local configuration and control.

  An asynchronous terminal is required for initial setup to enable external management.
- **Telnet access to the menu-driven user interface** – Over the FrameSaver unit's COM port, through an in-band management channel (PVC), or over the COM port using a LAN adapter.
- **SNMP** – Over the FrameSaver unit's COM port using a modem, over the network interface or a DTE port using an in-band management channel (PVC), or over the COM port using a LAN adapter.

Minimal Configuration Before Deploying Remote Units

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

- Node IP Address
- Node Subnet Mask

See *Configuring Node IP Information* in Chapter 8, *Configuration Options*, for these options.

Entering and Displaying System Information

Use the Device Name screen to name the system, and to change or display the general SNMP system name, location, and contact for the unit.

▶ Procedure

1. Follow this menu selection sequence:

   Main Menu → Control → System Information

2. Move the cursor to the field (Tab to the field, or press the arrow keys) where you want to add or change information.

   The following information is available for viewing. Use the right and left arrow keys to scroll additional text into view.

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.

3. Press Ctrl-a and Save your entriesSetting Up LoginsSee Chapter 9, *Security and Logins*, to set up and administer logins.

Basic Configuration

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

See Chapter 8, *Configuration Options*, when configuring the FrameSaver unit. It contains tables describing all configuration options and their possible settings.

Changing the Auto-Configuration setting can also change the FrameSaver unit's configuration. See *Setting Up Auto-Configuration* on page 8-10 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:

- *Quick Reference*
- Configuration option tables in Chapter 8

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

▶ Procedure

To change configuration option settings:

1. Access and display configuration options and their settings.
2. Change the settings, as needed.
3. Save the changes to one of three configuration option areas.

   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.

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.

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 configuration option set into the configuration edit area:

1. Follow this menu selection sequence:

   Main Menu → Configuration

   The **Load Configuration From:** menu appears.

2. Select the configuration option area you want to load and press Return (Current Configuration, Customer Configuration 1, Customer Configuration 2, or Default Factory Configuration).

   The selected configuration option set is loaded into the configuration edit area and the Configuration Edit/Display screen 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.

Changing Configuration Options

▶ Procedure

To change configuration option settings:

1. From the Configuration Edit/Display screen, select the configuration option set you want to view or make changes to and press Enter.

2. Select the configuration options applicable to your network, and make appropriate changes to the setting(s).

   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.

Saving Configuration Options

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

To save the configuration option changes from:

- DCE Manager for Windows – Click on the Set button at the bottom of the file folder where the change was made.
- DCE Manager for Unix – Click on the Apply button at the bottom of the window where the change was made.
- Menu-Driven User Interface – Select the Save function key. The procedure is described below.

▶ Procedure

To save the configuration options changes:

1. Press Ctrl-a to switch to the screen's function keys area.
2. Type **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 where you want to save the changes to (usually Current Configuration) and press Return.

   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 Auto-Configuration

The auto-configuration feature allows you to select a method of automatic configuration and connection of DLCIs within the FrameSaver unit.

When Frame Relay Discovery is selected, the FrameSaver unit “discovers” network DLCIs from the network LMI status response message (see the procedure on page 8-12). It configures a network DLCI, required port DLCI, and automatically connects them to create a PVC.

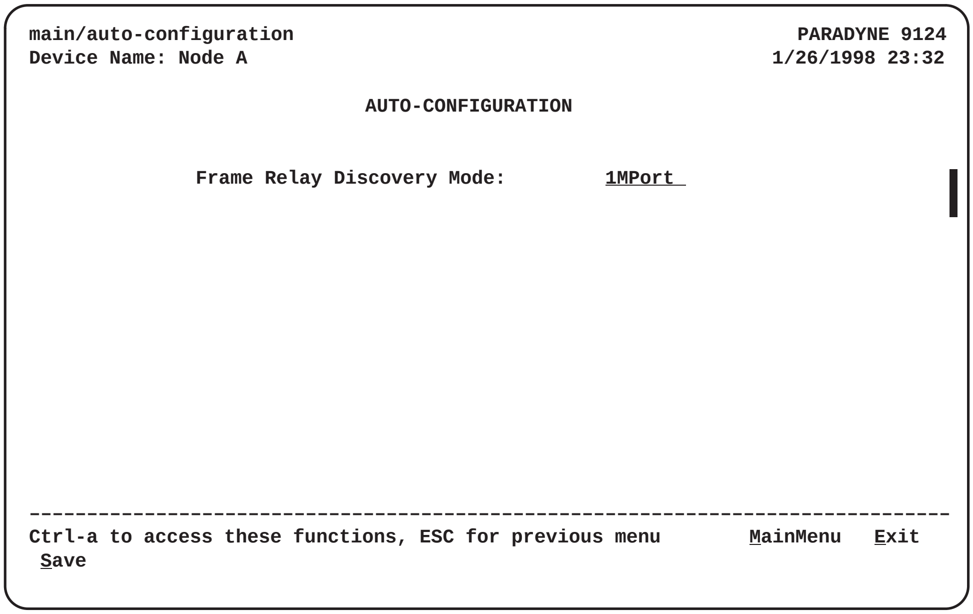
Automatically configured network DLCIs are multiplexed, and each automatically configured port DLCI carries the same DLCI Number as its corresponding network DLCI. These are the same DLCI numbers that would have been available had the FrameSaver unit not been inserted in the link between your equipment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

Frame Relay Discovery mode defaults to 1MPort (management DLCIs multiplexed with data DLCIs on Port-1), which creates two embedded DLCIs (EDLCIs) – one EDLCI for Port-1 user data, and another EDLCI for management data. When LMI is active on the network interface and PVC status information (with provisioned DLCI numbers) is next received from the network, the system automatically saves the settings listed in the table on page 8-13 to the Current Configuration area.

NOTE:

Local Management PVCs (e.g., PVCs between a router and the FrameSaver unit’s user data port) must be configured manually.

Auto-Configuration Screen Example



```
main/auto-configuration                                                PARADYNE 9124
Device Name: Node A                                                 1/26/1998 23:32

                                AUTO-CONFIGURATION


               Frame Relay Discovery Mode:        1MPort









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

Changing the Frame Relay Discovery Mode

Configuration options set by 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.

If setting up a FrameSaver unit going to a remote site, only the unit's Node IP Address and Subnet Mask need to be preconfigured; the default 1MPort setting automatically configures the unit.

If 1MPort 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 if it occurs:

If . . .	Then . . .
Any DLCIs or PVC connections have been configured manually	Select a "discovered" DLCI or PVC connection, and edit as needed using the Configuration menus.
Only a local management PVC between the router and the FrameSaver unit has been configured	Select the desired Frame Relay Discovery mode, and Save. Save causes the **`Delete All DLCIs and PVC Connections?`** prompt to appear. ■ If **Yes** (**y**) is entered, clears all discovered and manually configured DLCI records and PVC connections, except for the management PVC between a data port and router. This is so communication with the unit remains. ■ If **No** (**n**) is entered, no previously discovered or manually configured DLCIs or PVC connections are removed and newly discovered DLCIs will be configured according to the new discovery mode.

NOTE:

If non-FrameSaver units are at the other end of a PVC connection, PVC diagnostic tests are disruptive to data. Only FrameSaver units currently support PVC multiplexing and nondisruptive PVC diagnostics.

▶ Procedure

To select a Frame Relay Discovery mode:

1. Follow this menu selection sequence:

   Main Menu → Auto-Configuration → Frame Relay Discovery Mode

2. Select a Frame Relay Discovery mode:

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

[1] See page 8-13 to see the auto-configuration that takes place.

3. Save your selection. Respond yes or no to the **`Delete All DLCIs and PVC Connections?`** prompt (see page 8-11).

   — If **Yes** (**y**) is entered, clears all discovered and manually configured DLCI records and PVC connections, except for the management PVC between a data port and router. This is so communication with the unit remains.

   — If **No** (**n**) is entered, no previously discovered or manually configured DLCIs or PVC connections are removed and newly discovered DLCIs will be configured according to the new discovery mode.

4. Go to the Configuration menu and change any node-specific configuration options that may be needed.

The following table shows the automatic configuration that occurs within the FrameSaver unit when a Frame Relay Discovery Mode is selected.

Automatic Configuration for Selected Frame Relay Discovery Mode (1 of 4)

If the mode selected is . . .	Then setup configuration is . . .
Multiplexed Management: ■ **1MPort** (For DLCI Record information: see Table 8-9, DLCI Records Options.	■ DLCI Records : – *Network:* DLCI Number is automatically created from the LMI status response message. This DLCI will contain multiple EDLCIs: one for Port-1 and one for management. *Port-1:* DLCI Number is automatically created for the port from the multiplexed network DLCI. *Example:* Network DLCI 1001 → Port-1 DLCI 1001 – *Network:* DLCI Type is set to Multiplexed. – *Network:* CIR (bps) is automatically determined from LMI status update message if switch provides this information. Otherwise, the port rate is configured. *Port-1:* CIR (bps) is set to the network DLCI's CIR. – Committed Burst Size Bc (Bits) is set to the network DLCI's CIR. – Excess Burst Size Be (Bits) is set to the network port rate minus the network DLCI's CIR. – DLCI Priority is set to High.

[1] The port rate is calculated at the time of discovery as the number of DS0s allocated to frame relay. It is automatically configured once for each DLCI. Should the number of DS0s change, this value must be manually recalculated and changed via the Configuration branch.

Automatic Configuration for Selected Frame Relay Discovery Mode (2 of 4)

If the mode selected is . . .	Then setup configuration is . . .
■ **1MPort** (cont'd) For Management PVC information: see Table 8-12, Management PVC Options.)	■ Management PVCs:[2] – Name is automatically created from the network DLCI as Mgm*nnnn* (*nnnn* being the discovered multiplexed network DLCI number).[2] *Example:* Network DLCI 1001 → Port-1 DLCI 1001 and Mgm1001 – Intf IP Address is taken from the Node IP Address.[2] – Intf Subnet Mask is taken from the Node Subnet Mask.[2] – Primary Link is set to Net1-FR1. – Primary DLCI is automatically created from the network DLCI. – Primary EDLCI is set to 2 (management data). – Set DE is set to Enable. – RIP is set to Proprietary.
(For PVC Connection information: see Table 8-10, PVC Connection Options.)	■ PVC Connections: – Source Link set to Port-1. – Source DLCI – Port-1 DLCI is automatically created. – Source EDLCI is left blank. – Primary Destination Link is set to Net1-FR1. – Primary Destination DLCI is the automatically created network DLCI. – Primary Destination EDLCI is set to 0.

[2] If the same DLCI/EDLCI combination already exists, no changes are made to the existing management PVC.

You may want to configure a unique Node IP Address and Subnet Mask, and create a management PVC for this address and subnet mask prior to Frame Relay Discovery.

Automatic Configuration for Selected Frame Relay Discovery Mode (3 of 4)

If the mode selected is . . .	Then setup configuration is . . .
No Management: ■ **1Port** (For DLCI Record information: see Table 8-9, DLCI Records Options.	■ DLCI Records : – *Network:* DLCI Number is automatically created from the LMI status response message. *Port-1:* DLCI Number is automatically created from the network DLCI. *Example:* Network DLCI 1001 → Port-1 DLCI 1001 – *Network:* DLCI Type is set to Multiplexed.[3] – *Network:* CIR (bps) is automatically determined from LMI status update message if switch provides this information. Otherwise, the port rate is configured.[1] *Port-1:* CIR (bps) is set to the network DLCI's CIR. – Committed Burst Size Bc (Bits) is set to the network DLCI's CIR. – Excess Burst Size Be (Bits) is set to the network port rate minus the network DLCI's CIR. – DLCI Priority is set to High.
(For PVC Connection information: see Table 8-10, PVC Connection Options.)	■ PVC Connections: – Source Link set to Port-1. – Source DLCI is automatically created from the LMI status response message. – Source EDLCI is left blank. – Primary Destination Link is set to Net1-FR1. – Primary Destination DLCI is automatically created from the network/source DLCI. – Primary Destination EDLCI is set to 0 (Port-1 data).

[1] The port rate is calculated at the time of discovery as the number of DS0s allocated to frame relay. It is automatically configured once for each DLCI. Should the number of DS0s change, this value must be manually recalculated and changed via the Configuration branch.

[3] When non-FrameSaver units are at the other end of the PVC connection, change the network DLCI Type setting to Standard before sending data.

Automatic Configuration for Selected Frame Relay Discovery Mode (4 of 4)

If the mode selected is . . .	Then setup configuration is . . .
■ **NetOnly** (For DLCI Record information: see Table 8-9, DLCI Record Options.)	■ Network DLCI Records: – DLCI Number is automatically created from the LMI status response message. – DLCI Type is set to Multiplexed.[3] – CIR (bps) is automatically determined from LMI status update message if switch provides this information. Otherwise, the port rate is configured. – Committed Burst Size Bc (Bits) is set to the network DLCI's CIR. – Excess Burst Size Be (Bits) is set to the network port rate minus the network DLCI's CIR. – DLCI Priority is set to High. ■ No PVC connections are made within the FrameSaver unit. The user must manually create port and management DLCIs, then connect them to the DLCIs discovered on the network interface.

[3] When non-FrameSaver units are at the other end of the PVC connection, change the network DLCI Type setting to Standard before sending data.

Setting Up for Trap Dial-Out

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

To set up an external modem, you need to:

1. Set up SNMP trap managers (see page 8-65).
2. Set up Modem Directory phone numbers (see page 8-17).
3. Configure trap dial-out (see page 8-66).

Entering Modem Directory Phone Numbers

Phone numbers must be entered into the directories before the modem can dial out.

▶ Procedure

1. Follow this menu selection sequence:

   Main Menu → Control → Modem Call Directories

2. Press the spacebar until the desired Directory Number appears (A or 1–5).

   Set up the A (Alarm) directory as the primary directory. You can also set up an alternate directory. Press Return and the cursor is moved to the Directory Phone Number field.

3. Enter the phone number for the remote unit that this system will dial. Use valid characters only:

Enter . . .	**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.
T	one dialing.
W	Wait for dial tone.

4. Save your entries.

See *Configuring SNMP Traps and Trap Dial-Out* on page 8-66 for trap and alarm information. See *Configuring SNMP NMS Security* on page 8-65 to set up SNMP trap managers.

Setting Up Management

For remote sites, only SNMP management needs to be set up. For the central site, local management between the unit and the router must be set up along with SNMP management.

▶ Procedure

To set up SNMP management:

1. Select General SNMP Management.

   Configuration → Management and Communication → General SNMP Management

2. Minimally, set Name 1 Access to Read/Write.

3. Save your entries.

▶ Procedure

To set up local management at the central site unit:

1. Create a DLCI for the data port.

   Main Menu → Configuration → Data Ports → DLCI Records

2. Select Management PVC.

   Configuration → Management and Communication → Management PVC

3. Make the DLCI Record a management DLCI to create a Management PVC. Minimally, enter the following options for each of the DLCI Records created:

   — Name for the management DLCI

   — Special and the IP Address for the interface if it is different from the Node IP Address

   — Primary Link for this DLCI (i.e., the DLCI's primary destination interface)

   — Primary DLCI (i.e., the DLCI number at the other end of the PVC)

4. Save your changes.

Setting Up So the Router Can Receive RIP

Using the FrameSaver unit's standard routing Information protocol (RIP) feature, a management interface is created so management data can pass between FrameSaver SLV units.

▶ Procedure

1. Configure the port's router to receive RIP.

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

2. Create a Standard DLCI for the data port (see *Configuring DLCI Records for Each Inrterface* on page 8-46).

   Main Menu → Configuration → Data Ports → Port-n → DLCI Records

3. Change it to a Management PVC (see *Configuring Management PVCs* on page 8-57).

4. Make sure that Node IP Information has been set up (see *Configuring Node IP Information* on page 8-11).

5. Set Primary Link RIP to Standard_Out.

6. Save your configuration.

Setting Up Service Provider Connectivity

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

▶ Procedure

To set up NOC management:

1. Select DLCI Records on the network interface:

   Configuration → Network → DLCI Records

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

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

4. Change the DLCI Type from Multiplexed to Standard.

   The **`Delete EDLCI Connections and Make it a Mgmt Only PVC?`** prompt appears.

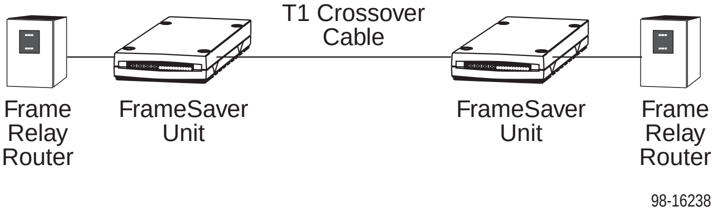
5. Type **y** (Yes) and press Enter.

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

Setting Up for 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.

This configuration is shown in the illustration below.



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.

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

   The Change Operating Mode screen appears, with two modes:
3. Select Back-to-Back Operation, and type **y** (Yes) at the **Are you sure?** prompt.
4. Press Ctrl-a and Save the change.

▶ Procedure

To return the unit to normal operation:

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

Configuring the System

Configuration option settings determine how the FrameSaver unit operates. The unit can be configured using:

- Menu-driven user interface via a direct connection or Telnet session.
- DCE Manager, based upon the following platforms:
  - HP OpenView Network Node Manager (Unix)
  - HP OpenView for WorkGroup Node Manager for Windows
  - IBM NetView/AIX

Changing the Auto-Configuration setting can also change the unit's configuration. See *Setting Up Auto-Configuration* on page 8-10, for additional information.

Configuring System Options

Select System to set the following options:

- Frame Relay and LMI Options (below)
- Service Level Verification Options on page 8-25.
- General Options, like user-initiated test time-out, test duration, and clock source on page 8-26.

Configuring System Frame Relay and LMI Options

Select Frame Relay and LMI to display or change the Frame Relay and LMI options for the system (see Table 8-1). Follow this menu selection sequence:

Main Menu → Configuration → System→ Frame Relay and LMI

Table 8-1. System Frame Relay and LMI Options (1 of 2)

LMI Behavior
Possible Settings: **Independent, Port-1_Follows_Net1-FR1, Net1-FR1_Follows_Port-1, Port-1_Codependent_with_Net1-FR1** Default Setting: **Independent**
Configures the network data port to allow the state of the LMI to be passed from one interface to another, determining how the FrameSaver unit will handle a change in the LMI state. Sometimes referred to as LMI pass-through. **Independent** – Handles the LMI state of each interface separately so that the LMI state of one interface has no effect on the LMI state of another interface. Provides LMI Spoofing. This is the recommended setting for Network Service Providers (NSPs). **Port-1_Follows_Net1-FR1** – Brings LMI down on Port-1 when LMI on the network interface goes down, disabling Port 1 and deasserting its control leads. When LMI on the network interface comes back up, Port-1 is reenabled and its control leads are reasserted. The LMI state on Port-1 has no effect on the LMI state on the network interface. That is, Port-1's LMI follows the network interface's LMI. This setting is useful if the router connected to Port-1 is used to initiate recovery when network failures are detected. **Net1-FR1_Follows_Port-1** – Brings LMI down on the network interface when LMI on Port-1 goes down, disabling the network interface and deasserting its control leads. When LMI on Port-1 comes back up, the network interface is reenabled. The LMI state on the network interface has no effect on the LMI state on Port-1. That is, the network interface's LMI follows Port-1's LMI. Used at central sites, this setting is useful when the remote site router on the other end of the PVC connection can initiate recovery via a redundant central site when there is a catastrophic central-site LAN or router failure. Not recommended for NSPs. **Port-1_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 both interfaces. That is, the LMI state for one interface is dependent on the other. Use this setting when backup will be performed by the router. It is *not* recommended since it makes fault isolation more difficult.
LMI Error Event (N2)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **3**
Configures the N2 parameter which sets the number of errors that can occur on the LMI link before reporting an error. Applies to both the user and network sides of the UNI. **1 – 10** – Specifies the number of errors that can occur on the LMI link (inclusive).

Table 8-1. System Frame Relay and LMI Options (2 of 2)

LMI Clearing Event (N3)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **1**
Configures the LMI-defined N3 parameter which sets the number of error-free messages that must be received before clearing an error event. Applies to both the user and network sides of the UNI. **1 – 10** – Specifies the number of error-free messages that must be received (inclusive).
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 only to the user side of the UNI. **1 – 255** – Specifies the number of status enquiry polling cycles that can be initiated (inclusive).
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 only to the user side of the UNI. **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 only to the network side of the UNI. **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 interval time (in seconds) that the Network side of the LMI uses to measure the maximum status enquiry messages received (N4) from the User side. Applies only when LMI Personality is set to Network Side of the UNI. **5 – 30** – Specifies the interval of time in increments of 5.

Configuring Service Level Verification Options

Select Service Level Verification to display or change the Service Level Verification (SLV) System configuration options (see Table 8-2). Follow this menu selection sequence:

Main Menu → Configuration → System→ Service Level Verification

Table 8-2. Service Level Verification Options

SLV Sample Interval (secs)
Possible Settings: **15 – 3600** Default Setting: **60**
Sets the inband communications interval between FrameSaver SLV units. Inband communications are used to pass frames that calculate latency, as well as transmission success and other SLV information. **15 – 3600** – Sets the SLV Sample Interval (secs) period in seconds (inclusive).
SLV Delivery Ratio
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether communication of Frame and Data Delivery Ratios (FDR/DDR) between FrameSaver units is enabled. To use this capability, units at both ends of all PVCs must be FrameSaver SLV units. 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. These statistics are used to determine the amount of data dropped by the network. (Be aware that increasing bandwidth used for SLV communications reduces bandwidth available for user data). **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 moniotred along with the LMI status to determine the status of PVC connections to remote FrameSaver units. NOTE: This option only applies to multiplexed DLCIs. **Enable** – After the configured threshold for missed SLV packets has been exceeded, an alarm and SNMP trap are generated, a Health and Status message created, and the DLCI’s status turns Inactive. If an ISDN DBM is installed, backup is initiated. **Disable** – Missed SLV communications will not be monitored.

Table 8-2. Service Level Verification Options

SLV Timeout Error Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **3**
Specifies the number of consecutively missed SLV commnications that willl be tolerated before an SLV Timeout Error Event is declared. **1–20** – Sets the limit for these error events.
SLV Timeout Clearing Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **1**
Specifies the number of consecutively missed SLV communications that willl be received before the SLV Timeout Error Event is cleared. **1–20** – Sets the limit for the clearing event.

Configuring General System Options

Select General to display or change the general system configuration options (see Table 8-3). Follow this menu selection sequence:

Main Menu → Configuration → System→ General

Table 8-3. General System Options (1 of 2)

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 8-3. General System Options (2 of 2)

Primary Clock Source

Possible Settings: **Net1, DSX, Internal**
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 is derived from the DSX-T1 interface. This setting only appears if the DSX-1 interface is installed and enabled (see Configuring the DSX-1 Interface, page 8-32).

Internal – The primary clock is the internal clock.

Secondary Clock Source

Possible Settings: **Net1, DSX, Internal**
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 is derived from the DSX-T1 interface. This setting only appears if the DSX-1 interface is installed and enabled (see *Configuring the DSX-1 Interface Physical Options*, page 8-32).

Internal – The secondary clock is the internal clock.

Setting Up Each Physical Interface

Configure physical characteristics using the following interface options:

- T1 Network Physical Options (below)
- DSX-1 Interface Physical Options on page 8-32.
- Data Port Physical Options on page 8-34.

Configuring the FrameSaver T1 Network Interface Physical Options

Select Physical to display or change the physical configuration options for the T1 Network interface (see Table 8-4) following this menu selection sequence:

Main Menu → Configuration → Network → Physical

Table 8-4. T1 Network Physical 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. If you attempt to disable the Network 2 interface for which cross connections exist, the message **`This action will clear all Network n Cross Connections. Are You Sure? No`** appears. If you select: **No** – The operation is cancelled. **Yes** – The following occurs: ■ All existing cross-connect assignments for this interface are cleared. ■ Alarms or traps associated with this interface are not generated. ■ LEDs associated with this interface are held in an "off" state. ■ All time slot assignments associated with the Network physical interface will be deallocated. NOTE: No Frame Relay DLCI or PVC connections will be deleted.
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 8-4. T1 Network Physical 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.
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 FrameSaver unit is not in compliance with ANSI T1.403 or AT&T TR 62411.

Table 8-4. T1 Network Physical Options (3 of 4)

Network Initiated PLB
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Allows the initiation and termination of the payload loopback (PLB) to be controlled by the receipt of PLB-Actuate and PLB-Release commands from the network. *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 FrameSaver unit to enter a payload loopback (provided a PLB can be performed in the FrameSaver 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 8-4. T1 Network Physical 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: **Text Field, Clear** Default Setting: **blank**
Identifies the transmission vendor’s circuit information to facilitate troubleshooting. **Text Field** – Edit or display circuit identifier information (maximum 255 characters). **Clear** – Removes the circuit identifier information.

Configuring the DSX-1 Interface Physical Options

Select DSX-1 to display or change the physical configuration options when a DSX-1 interface is installed (see Table 8-5).

▶ Procedure

1. Follow this menu selection sequence:

   Main Menu → Configuration → DSX-1

2. Choose whether or not the DSX-1 interface will be provided by the port.

Table 8-5. DSX-1 Physical 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? <u>No</u>** 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 8-5. DSX-1 Physical Options (2 of 2)

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

Configuring Data Port Physical Options

Select Physical to display or change the physical characteristics of the data port connected to the DTE (see Table 8-6).

Main Menu → Configuration → Data Ports → Physical

Table 8-6. Data Port Physical Options (1 of 2)

Transmit Clock Source
Possible Settings: **Internal, External** Default Setting: **Internal**
Determines whether the DTE's transmitted data is clocked into the FrameSaver unit by 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.
Invert Transmit Clock
Possible Settings: **Auto, Enable, Disable** Default Setting: **Auto**
Determines whether the clock supplied by the FrameSaver unit on interchange circuit DB (ITU 114) – Transmit Signal Element Timing (DCE Source) TXC is phase inverted with respect to the clock used to time the incoming Transmitted Data (TD). **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.
Port (DTE) Initiated Loopbacks
Possible Settings: **Local**, **Disable** Default Setting: **Disable**
Allows a local external DTE Loopback to be started or stopped via the port's attached data terminal equipment using the port's interchange lead LL (ITU 141). **Local** – The DTE attached to the port controls the local external DTE Loopback. **Disable** – The DTE attached to the port cannot control the local external DTE Loopback.

Table 8-6. Data Port Physical Options (2 of 2)

Monitor DTR
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies the conditions on the data port that determine when valid data is not being sent from the DTE. When this condition is detected, all ones are sent to the network on the DS0 channels allocated to the port. *Display Conditions* – This option only appears when Port Use is set to Synchronous Data and Port Type is not set to X.21. **Enable** – Interchange circuit CD (ITU 108/1/2) – DTR is monitored to determine when valid data is sent from the DTE. When DTR is off, all ones are sent to the network. **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
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies the conditions on the data port that determine when valid data is not being sent from the DTE. When this condition is detected, all ones are sent to the network on the DS0 channels allocated to the port. **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.

Assigning Time Slots/Cross Connections

The system allows you to assign data paths between the various interfaces to share the T1 network. Assuming that the Network Port interface is enabled, you can make the following cross connection assignments:

- Frame relay links to Network interface time slots
- DSX-1 to the Network interface time slots

You can also clear cross-connection assignments for the system, or for a selected slot or interface (see page 8-42).

NOTE:

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

Use the following procedures to assign cross connections.

Assigning Frame Relay Time Slots to the Network Interface

Before assigning Network time slots for use by Frame Relay, 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.

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 LMI failure. This option allows additional time slots to be added without manual device reconfiguration.
N*xx*	This field represents time slot *xx* 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	Time slot *ss* is assigned to Frame Relay service, Link 1.

Time Slot Assignment Rule:

Valid Network time slots are either labeled as **Available**, or contain a Frame Relay link 1 assignment.

▶ Procedure

1. Follow this menu sequence:

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

2. 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.

3. Enable or disable Time Slot Discovery. When enabled, the unit will examine 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, you must make time slot assignments manually.

4. 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.

5. Repeat Step 4 until all desired time slots are assigned.

6. To save changes, select Save and press Return, or press ESC to return to the Time Slot Assignment menu.

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 8-5, DSX-1 Physical Options).

Value	Meaning
N*xx*	The upper field represents time slot *xx* 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*-*p*/*yy*	Time slot *yy* of DSX-1 interface *p* in slot *s* is assigned to the Network time slot identified right above it (N*xx*).

Time Slot Assignment Rules:

- Valid Network time slots are either labeled as **Available**, or contain a DSX-1 time slot assignment
- Valid DSX-1 time slots are those that are unassigned, and the currently assigned time slot
- Order of display is as follows:
  - — **Available** is the first selection
  - — Then, from lowest DSX-1 interface to the highest DSX-1 interface
  - — Then 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*xx*, 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*/*yy* 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

2. 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.
3. Move the cursor to the next editable time slot (underlined). Use the spacebar or type in the desired time slot to display the desired time slot assignment.
4. Repeat Step 3 until all desired time slots are assigned. Select Save to save the assignments, or press Esc to return to the Time Slot Assignment menu.

DSX-1 Signaling Assignments and Trunk Conditioning

The second page of the DSX-1 to Network Assignments screen enables 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 interface if a Carrier Group Alarm (CGA) occurs on a T1 interface.

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 8-7 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 8-7. Signaling and Trunk Conditioning Values (1 of 3)

Network Side Value	Meaning	DSX-1 Side Default Value
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

Table 8-7. Signaling and Trunk Conditioning Values (2 of 3)

Network Side Value	Meaning	DSX-1 Side Default Value
The following values will configure the cross-connect for RBS, as well as perform the trunk conditioning, indicated when a CGA condition occurs. Although the ABCD signaling bits for each setting are described, only AB bits are transmitted when the cross-connected T1 interface is using D4 framing.		
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

Table 8-7. Signaling and Trunk Conditioning Values (3 of 3)

Network Side Value	Meaning	DSX-1 Side Default Value
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
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.

Clearing Assignments

Clearing assignments sets all time slots to unassigned. Follow this menu selection sequence:

Main Menu → Configuration → Time Slot Assignment → Clear Assignments

Configuring Frame Relay LMI for an Interface

Select Frame Relay from the selected Network or Data Ports menu. Based upon the information about the local management interface (LMI) and assigned line conditions supplied by the service provider, edit the Frame Relay configuration options (see Table 8-8).

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

Table 8-8. Frame Relay and LMI Options (1 of 4)

LMI Protocol
Possible Settings: **Initialize_From_Net1FR1**, **Initialize_From_Interface, Auto_On_LMI_Fail, Standard, Annex-A, Annex-D** Default Setting: For data port links: I**nitialize_From_Net1FR1** For network links: **Auto_On_LMI_Fail**
Specifies either the LMI protocol supported on the frame relay interface or the discovery source for the LMI protocol. **Initialize_From_Net1FR1** – The LMI type supported on this frame relay link will be configured to match the LMI protocol initially discovered on the primary Network frame relay link (Net1FR1). LMI Protocol is set to None internally, but once a protocol has become active or is set on the primary Network link, the protocol will be set to the same value on this link (Standard, Annex-A or Annex-D). The protocol will *not* be updated based on changes to Net1FR1 after being set initially. **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. **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 8-8. Frame Relay and LMI Options (2 of 4)

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 8-1, System Frame Relay and LMI Options). **Custom** – Use the following options in this table to configure LMI parameters.
LMI Error Event (N2)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **3**
Configures the LMI-defined N2 parameter which sets the number of errors that can occur on the LMI link before reporting an error. *Display Conditions* – This option only appears when LMI Parameters is set to Custom. **1 – 10** – Specifies the number of errors that can occur on the LMI link (inclusive).
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. *Display Conditions* – This option only appears when LMI Parameters is set to Custom. **1 – 10** – Specifies the number of error-free messages that must be received (inclusive).
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 and configured for the user side of the UNI only. *Display Conditions* – This option only appears when LMI Parameters is set to Custom, and only on the network interface. **1 – 255** – Specifies the number of status enquiry polling cycles that can be initiated (inclusive).
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 and configured for the user side of the UNI only. *Display Conditions* – This option only appears when LMI Parameters is set to Custom, and only on the network interface. **5 – 30** – Specifies the number of seconds between the initiation of status enquiry messages in increments of 5.

Table 8-8. Frame Relay and LMI Options (3 of 4)

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 and configured for the network side of the UNI only. *Display Conditions* – This option only appears when LMI Parameters is set to Custom, and only on a user data port. **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 received (N4) from the user side. Applies to and configured for the network side of the UNI only. *Display Conditions* – This option only appears when LMI Parameters is set to Custom, and only on a user data port. **5 – 30** – Specifies the interval of time in increments of 5.
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.

Table 8-8. Frame Relay and LMI Options (4 of 4)

Network Initiated DCLB
Possible Settings: **Disable, V.54, ANSI_FT1, Both** Default Setting: **Both**
Allows the initiation and termination of the Data Channel Loopback (DCLB V.54 loop 2) to be controlled by the receipt of a DCLB-actuate or DCLB-release sequence (either V.54 or FT1-ANSI compliant) from the network. When enabled, this option causes a NextEDGE device 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).

Configuring DLCI Records for Each Interface

If Auto-Configuration is not used, it is necessary to create DLCI records manually for each interface. If you do use Auto-Configuration, then it may only be necessary to create a management DLCI between the FrameSaver unit and the router attached to the data port.

Configure the DLCI records for the following interfaces:

- Network
- Data port

DLCI records for all interfaces are created and configured in the same manner. Procedures for creating DLCI Records are shown in the following examples.

▶ Procedure

To create and configure DLCI records:

1. Select the desired DLCI records.
2. Select New and press Enter to create a new DLCI.

   The DLCI Records Entry screen appears for the frame relay link selected. The DLCI Number field is blank, while the rest of the fields are filled with the default value settings.

   NOTE:

   If the maximum number of DLCIs have already been defined, the message **`No more DLCIs allowed`** appears.

3. Enter the DLCI number to be created.
4. Change DLCI option settings, as required.

   NOTE:

   Do not multiplex a DLCI unless a NextEDGE or FrameSaver device is at both ends of the connection.

5. Press Crtl-a and Save the DLCI Record.

▶ Procedure

To change DLCI records:

1. Select the desired DLCI records.
2. Select Modify to change a DLCI record.

   The message **`Modify DLCI record for DLCI Number?`** appears.
3. Select the DLCI record to be modified from the list of all DLCIs on the frame relay link and interface displayed. Then, press Enter.

   The DLCI record entry screen displays with the fields initialized for the selected DLCI.
4. Make the desired changes.
5. Press Crtl-a and Save your changes.

If a connected network DLCI's type is changed from Multiplexed to Standard, the following prompt will appear if the DLCI is part of a connection: **`DLCI in Connection. Update DLCI usage as follows:`**

Select one of the following choices:

- **Delete EDLCI Connections and Make a Mgmt Only PVC**

If you choose this selection, the following actions occur. All of this is typically done by frame relay service providers so there is management connectivity from the network operation/control center (NOC or NCC):

- — Removes this DLCI on all PVC Connections (see Table 8-10, PVC Connection Options), and Management PVC Connections (see Table 8-12, Management PVC Options).
- — Resets any Trap Manager Destination (see Table 8-16, SNMP Traps and Trap Dial-Out Options), or Default Network Destination (see Table 8-11, Node IP Options) that is configured for a Management PVC with this DLCI to the factory default setting.
- — Deletes all PVC Connections (see *Configuring PVC Connections* on page 8-51) and Management PVC Connections (see *Configuring Management PVCs* on page 8-57) involving this DLCI as the source or primary destination.
- — Deletes all excess DLCIs (on the user data port) that were used only in deleted connections.
- — Changes DLCI Type from **Multiplexed** to **Standard** for the selected Network DLCI.
- — Configures the Network DLCI as a Management PVC (see *Configuring Management PVCs* on page 8-57).

- **Delete EDLCI Connections and Make a standard PVC to *frame relay link*, DLCI *nnnn***

  If you choose this selection, the following actions occur:

  — Removes this DLCI on all PVC Connections (see Table 8-10, PVC Connection Options), and Management PVC Connections (see Table 8-12, Management PVC Options).

  — Resets any Trap Manager Destination (see Table 8-16, SNMP Traps Options), or Default Network Destination (see Table 8-11, Node IP Options) that is configured for a Management PVC with this DLCI to the factory default setting.

  — Deletes all PVC Connections (see *Configuring PVC Connections* on page 8-51) and Management PVC Connections (see *Configuring Management PVCs* on page 8-57) involving this DLCI as the source or primary destination.

  — Deletes all excess DLCIs (other than *frame relay link*, DLCI *nnnn*) that were used only in deleted connections.

  — Changes DLCI Type from **Multiplexed** to **Standard** for the selected Network DLCI.

  — Creates a standard PVC connection between this Network DLCI and *frame relay link*, DLCI *nnnn* (see *Configuring PVC Connections* on page 8-51).

- **Leave as Multiplexed DLCI**

  The DLCI Type remains unchanged. You must delete the DLCI connection before you can change the DLCI Type.

▶ Procedure

To create additional DLCI records:

1. Press Esc to return to the previous DLCI Records screen.

   Helpful Hint:

   Once you create the first DLCI record, you can use the CopyFrom function to create additional records, assigning a unique number to each new DLCI record.

   Example:
   First DLCI numbered 16
   Second DLCI numbered 17

2. Select New, or the CopyFrom function, and press Enter.

Table 8-9. DLCI Record Options (1 of 2)

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: **Standard**
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. **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 –** *maximum line rate on port* 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.
Committed Burst Size Bc (Bits)
Possible Settings: **CIR, Other** Default Setting: **CIR**
Specifies the committed amount of transmitted data in bits that the network will accept without discarding frames (Bc). **CIR** – Specifies the CIR amount of data that will be accepted before frames are discarded. **Other** – Allows you to specify a rate other than the CIR in the Port Rate-Bc field. In this case, Tc is calculated according to I.370.

Table 8-9. DLCI Record Options (2 of 2)

Bc
Possible Settings: **0 –** *maximum line rate on port* Default Setting: CIR rate
Allows you to display or change the committed burst size for the DLCI. *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 –** *maximum line rate on port* Default Setting: *maximum port rate* minus the default CIR
Allows you to display or change the excess burst size for the DLCI.
DLCI Priority
Possible Settings: **Low, Medium, High** Default Setting: **High**
Specifies the relative priority for data received on the DLCI from an attached device (also known as *quality of service*). All data on Port 1 is cut-through, as long as there is no higher-priority data queued from another user port. The DLCI priority set for an interface applies to data coming into that interface. For example, the priority set for DLCIs on Port 1 applies to data coming into Port 1 from the attached equipment (such as a router). *Display Conditions* – This option only appears when Committed Burst Size is set to Other. **Low** – Data configured for the DLCI has low priority. **Medium** – Data configured for the DLCI has medium priority. **High** – Data configured for the DLCI has high priority.
Outbound Management Priority
Possible Settings: **Low, Medium, High** Default Setting: **Medium**
Specifies the relative priority for management traffic sent on management PVCs transmitted 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

Select PVC Connections to display or change the configuration options for the PVC connections (see Table 8-10). DLCI records must have been configured for the interface first. See Maximum PVCs, EDLCIs, and Management PVCs in Chapter 1, *About the FrameSaver SLV*, for a table of the maximum number of PVCs that you can configure.

▶ **Procedure**

1. Follow this menu selection sequence:

   Main Menu → Configuration → PVC Connections

   The PVC Connection Table screen appears.

2. Select New or Modify from the PVC Connection Table screen to add or change PVC connections between a source DLCI (link) and destination DLCI (link) on a frame relay interface.

3. When New is selected, the configuration option field is blank. Tab to the first configuration option and press the spacebar. The first valid selection appears in the field.

   NOTE:

   Management links are not created using this screen. Go to the Management PVC Entry screen:

   Main Menu → Configuration → Management and Communication → Management PVCs

Table 8-10. PVC Connection Options (1 of 2)

Source Link
Possible Settings: **Port-1, Net1-FR1** Default Setting: Initially blank; no default.
Specifies the frame relay interface that starts a PVC connection; the *from* end of a from-to link. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined that are not part of a PVC connection or management link. For example, if Port-1 has no DLCIs defined, Port-1 would not appear as a valid setting. **Port-1** – Specifies the user data port as the source link. Refers to frame relay links on the user data port that are capable of having the Port Use option set to Frame Relay (see Table 8-6, Data Port Physical Options). **Net1-FR1** – Specifies the Network interface as the source link. **Clear** – Clears the Source Link and Source DLCI settings, and suppresses Source EDLCI.
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 (inclusive).
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 (inclusive).
Destination Link
Possible Settings: **Net1-FR1** Default Setting: Initially blank; no default.
Specifies the frame relay interface used as the destination link; the *to* end of a from-to link. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined which are not part of a PVC connection or management link. For example, if the network interface has no DLCIs defined, this interface would not appear as a valid setting. **Net1-FR1** – Specifies the Network interface as the destination link. **Clear** – Clears the Destination Link and Destination DLCI settings, and suppresses Destination EDLCI.

Table 8-10. PVC Connection Options (2 of 2)

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

Setting Up Management and Communication Options

Select Management and Communication to display the Management and Communications Options menu. The following Management and Communication Options can be selected from the menu:

- Node IP Options on page 8-54.
- Management PVC Options on page 8-57.
- General SNMP Management Options on page 8-61.
- Telnet and FTP Sessions Options on page 8-62.
- SNMP NMS Security Options on page 8-65.
- SNMP Traps and Trap Dial-Out Options on page 8-68.
- Communication Port Options on page 8-72.

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 8-11).

Main Menu → Configuration → Management and Communication → Node IP

Table 8-11. Node IP Options (1 of 3)

Node IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the node. Since an IP address is not bound to a particular port, it can be used for remote access via a management PVC. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the node, which can be viewed or edited. **Clear** – Fills the node IP address with zeros.
Node Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the node. Since the subnet mask is not bound to a particular port, it can be used for remote access via a management PVC. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the node, which can be viewed or edited. **Clear** – Fills the node subnet mask with zeros. When the node's subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.

Table 8-11. Node IP Options (2 of 3)

Default IP Destination

Possible Settings: **None, COM, *PVCname***
Default Setting: **None**

Specifies where a default IP destination or route is connected so that data without a specifically defined PVC will have a route. Examples: If the default IP network is connected to the communications port, you would select COM. If the default IP network is connected to a far-end device over the management PVC named Tpa (as defined by the Name configuration option (see Table 8-12, Management PVCs Options), you would select the PVC name Tpa.

NOTE: If the link to the IP destination selected as the default route becomes disabled or down, the unrouteable data will be discarded. Make sure that the link selected is operational, and if that link goes down, change the default destination.

CAUTION: Use care when configuring a default route to an interface that has a subnet route configured at a remote end where the NMS, router, LAN adapter, terminal server, etc. is connected. Communicating with an unknown IP address on the subnet will cause temporary routing loops, which will last 16 iterations times the retry count.

None – No default network destination is specified. Unrouteable data will be discarded. This is the recommended setting.

COM – Specifies that the default destination is connected to the COM port. Only appears when Port Use is set to Net Link (see Table 8-17, Communication Port Options).

PVCname – Specifies a name for the management PVC. Only appears when a management PVC name is defined for the node. For example, when the network is connected to a remote device located in Tampa, Tpa can be specified as the PVC name, which is the link between the local FrameSaver unit and the one located in Tampa. PVCTpa would appear as one of the available selections.

TS Management Link

Available Settings: **None, *PVCname***
Default Setting: **None**

Specifies a troubleshooting management link for the special needs of network service providers.

If the option is changed from the management PVC name to None, the **`Delete the Management PVC`** ***`PVCname`*** **`and the associated DLCI Record?`** prompt appears. If you select:

- No – The link designation is removed and the option is set to None.
- Yes – The link designation is removed and the option is set to None, and the link and its DLCI will be deleted, as well.

None – Disables or does not specify a TS Management Link.

PVCname – Specifies the name of the TS Management PVC.

Display Conditions – This selection only appears when a dedicated Management PVC has been defined on the network frame relay link as a DLCI with DLCI Type set to Standard.

Table 8-11. Node IP Options (3 of 3)

TS Management Link Access Level
Available Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the highest access level allowed when accessing the unit via a Telnet or FTP session when the service provider is using the TS Management Link. *Display Conditions* – This option does not appear when TS Management Link is set to None. NOTES: Telnet and FTP sessions on this link *are not* affected by the access level set by the Session Access Level, Login Required, or FTP Login Required option settings (see Table 8-14, Telnet and FTP Sessions, on page 8-62). 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 8-12). First, DLCI records must have been configured for the interface where the Management PVC will reside. See *Configuring DLCI Records for Each Interface* on page 8-46.

▶ Procedure

1. Follow this menu selection sequence:

   Main Menu → Configuration → Management and Communication → Management PVCs

2. Select New or Modify to add or change DLCI and EDLCI 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 that you specified.

Table 8-12. 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., Tpa for Tampa, Florida). **ASCII text entry** – Where you 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 8-11, Node IP Options). **Special** (001.000.000.000 – 223.255.255.255) – Allows you to display/edit an IP address for the unit's management PVC when the IP address for this interface is different from the node's IP address.

Table 8-12. 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 8-11, Node IP Options). **Calculate** – Calculates the subnet mask created by the IP protocol based on the class of the IP address (Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000). Cannot be displayed or edited. **Special** (000.000.000.000 – 255.255.255.255) – Allows you to edit/display the subnet mask for the management PVC when the subnet mask is different for this interface. A text field displays where you can enter the subnet mask for this unit's management PVC.
Set DE
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether frames (packets) sent on a management PVC have the Discard Eligible (DE) bit set. This bit is used by the network to prioritize which frames to discard first during periods of network congestion. This allows management traffic to be viewed as lower priority than customer data. **Enable** – Sets the DE bit to one on all frames sent on the management PVC. **Disable** – Sets the DE bit to zero on all frames sent on the management PVC. This is the recommended setting, particularly for NSPs providing a managed network service.
Primary Link
Possible Settings: **Net1-FR1, Port-1, Clear** Default Setting: Initially blank; no default.
Specifies the frame relay interface to use for this management PVC. The interface selected must have at least one DLCI (or DLCI with EDLCI) defined, which is not part of a PVC connection or already assigned as a management PVC. **Net1-FR1** – Specifies the network interface as the source link for the connection. **Port-1** – Specifies the frame relay link on Port 1 as the destination link for the connection. **Clear** – Clears the link and the DLCI field, and suppresses the EDLCI field if the DLCI was multiplexed.

Table 8-12. 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 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).

Table 8-12. Management PVC Options (4 of 4)

Primary Link RIP
Possible Settings: **None, Proprietary, Standard_out** Default Setting: Multiplexed DLCIs: **Proprietary** 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 8-9, DLCI Records Options). **Standard_out** – The device will send standard RIP messages to communicate routing information only about other FrameSaver SLV units in the network. This is the factory default for management PVCs configured on standard DLCIs. NOTE: The router must be configured to receive RIP on the port connected to the FrameSaver unit for the management interface (e.g., Cisco: config-t, router RIP, int serial*x*, IP RIP Receive version 1, ctl-z WR). To create this management interface: – Create a Standard DLCI for the data port (see *Configuring DLCI Records for Each Interface* on page 8-46). – Change it to a Management PVC (see *Configuring Management PVCs* on page 8-57). – Make sure that Node IP Information has been set up (see *Configuring Node IP Information* on page 8-11). – Set Primary Link RIP to Standard_Out.

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.

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

See Table 8-13 for General SNMP Management configuration options.

Table 8-13. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the FrameSaver unit can be managed as an SNMP agent by an SNMP-compatible NMS. **Enable** – Can be managed as an SNMP agent. **Disable** – Cannot be managed as an SNMP agent. The FrameSaver unit will not respond to SNMP messages nor send SNMP traps.
Community Name 1
Possible Settings: **ASCII text entry, Clear** Default Setting: **Public** in ASCII text field
Specifies the first of two names that are allowed to access the objects in the FrameSaver unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB. **ASCII text entry** – Adds to or changes Community Name 1 (maximum 255 characters). **Clear** – Clears Community Name 1.
Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
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 8-13. General SNMP Management Options (2 of 2)

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

Configuring Telnet and/or FTP Session Support

Select Telnet and FTP Session to enable or disable a Telnet or download session. Telnet configuration options control whether a Telnet session is allowed through an interconnected IP network and the access security applicable to the session (see Table 8-14). Two Telnet sessions can be active at a time.

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

Table 8-14. Telnet and FTP Session Options (1 of 3)

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

Table 8-14. Telnet and FTP Session Options (2 of 3)

Session Access Level

Possible Settings: **Level-1, Level-2, Level-3**
Default Setting: **Level-1**

Specifies the highest security level allowed when accessing the menu-driven user interface via a Telnet session. If a login is required for the session, the effective access level is also determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. This option does not affect the TS 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.

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.

NOTE: Changing this setting does not affect the current session; it changes all subsequent sessions.

Enable – Terminates the session after the Disconnect Time expires.

Disable – Does not terminate Telnet session during inactivity.

Disconnect Time (Minutes)

Possible Settings: **1 – 60**
Default Setting: **10**

Sets the amount of keyboard inactive time allowed before a user session is disconnected.

Display Conditions – This option does not appear when Inactivity Timeout is disabled.

NOTE: Changing this setting does not affect the current session; it changes all subsequent sessions.

1 – 60 – Up to an hour can be set.

Table 8-14. Telnet and FTP Session Options (3 of 3)

FTP Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the system responds as a server when an FTP (file transfer protocol) client on an interconnected IP network requests an FTP session. This option must be enabled when downloading files. **Enable** – Allows an FTP session between the system and an FTP client. **Disable** – Does not allow FTP sessions.
FTP Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether a login ID and password are required for an FTP session. If required, the login used is the same login used for a menu-driven user interface session. This option does not affect the TS 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 rate of file transfer to the system. This option allows new software and configuration files to be downloaded using selected bandwidth without interfering with normal operation. Using this option, new software and configuration files can be downloaded quickly using the default settings, or at a slower rate over an extended period of time by selecting a slower speed. Based upon TCP flow control, the FTP server in the system throttles bandwidth to match this setting. **1 – 1536** – Sets the download line speed from 1 kilobits per second to the full network line speed.

Configuring SNMP NMS Security

Select SNMP NMS Security to display, add, or change the SNMP security configuration options for the FrameSaver unit. A table is displayed consisting of the network management systems identified by IP address that are allowed to access the FrameSaver unit by SNMP.

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

See Table 8-15 for SNMP NMS Security configuration options.

Table 8-15. 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 8-15. 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 to display, add, or change the SNMP trap configuration options for the FrameSaver unit.

Main Menu → Configuration → Management and Communication → SNMP Traps

To configure the FrameSaver unit for SNMP traps you must set:

- The number of SNMP managers that are to receive SNMP traps from the FrameSaver unit.
- An IP address for each SNMP manager specified.
- The type of SNMP traps to be sent from the FrameSaver unit.

Use the SNMP Trap Options screen to configure the necessary configuration options needed to support the SNMP traps. Select and set the following configuration options, as appropriate (see Table 8-16).

See Appendix C, *SNMP MIBs and Trap, ands 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.

NOTE:

Be sure to choose an operational link for the default. Should the default link become disabled, unrouteable traps will be discarded.

To . . .	**Set the configuration option . . .**
Enable sending of SNMP trap messages	SNMP Traps to Enable.
Specify the number of SNMP managers that will receive SNMP trap messages from the FrameSaver unit	Number of SNMP Managers to the desired number (maximum of 6) of SNMP managers to receive SNMP traps.
Specify an IP address for each SNMP manager specified in the Number of SNMP Managers configuration option	NMS *n* IP Address to the IP address that identifies each SNMP manager(s) indicated in the Number of SNMP Managers configuration option.
Specify the network destination for the Trap Manager	Destination to one of the following: Default COM *PVCname*
Select the type of SNMP trap messages to be sent from the FrameSaver unit	■ General Traps to enable or disable warmStart and authenticationFailure traps. ■ Enterprise Specific Traps to enable or disable enterpriseSpecific traps. ■ Link Traps to enable or disable linkDown and linkUp traps. ■ Link and DLCI Traps Interfaces to specify which interfaces will generate linkDown, linkUp and enterpriseSpecific traps. ■ RMON traps

Table 8-16. SNMP Traps and Trap Dial-Out Options (1 of 4)

SNMP Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the FrameSaver unit sends trap messages to the currently configured SNMP trap manager(s). **Enable** – Sends trap messages. **Disable** – Does not send trap messages.
Number of Trap Managers
Possible Settings: **1 – 6** Default Setting: **1**
Specifies the number of SNMP management systems that will receive SNMP trap messages from the FrameSaver unit. An NMS IP Address must be configured in the NMS *n* IP Address configuration option for each trap manager to receive trap messages. **1 – 6** – Specifies the number of trap managers (inclusive).
NMS *n* IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address that identifies the SNMP manager(s) to receive SNMP traps. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **001.000.000.000 – 223.255.255.255** – Adds to or changes the IP address for the trap manager. **Clear** – Fills the NMS IP address with zeros.
Destination
Possible Settings: **Default, COM, *PVCname*** Default Setting: **Default**
Specifies the network destination for the Trap Manager number configuration option. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **Default** – Uses the default network. **COM** – Uses the COM port. This selection is only available when Communication Port Use is set to Net Link (see Table 8-17, Communication Port Options). ***PVCname*** – Uses the defined management *linkname* (the name given the Management PVC). This selection only appears when at least one Management PVC is defined for the node.

Table 8-16. SNMP Traps and Trap Dial-Out Options (2 of 4)

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.
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, All** Default Setting: **All**
Specifies which interfaces will generate linkUp, linkDown, and enterpriseSpecific trap messages. These traps are not supported on the COM port. **Network** – Generates these trap messages on the T1 Network interface only. **DSX-1** – Generates these trap messages on the DSX-1 interface only, if applicable. **T1s** – Generates trap messages for linkUp, linkDown, and enterpriseSpecific events on both the T1 Network and DSX-1 interfaces only. **Ports** – Generates trap messages for linkUp, linkDown, and enterpriseSpecific events on user data port only. **All** – Generates trap messages for linkUp and enterpriseSpecific events on the network and user data ports.

Table 8-16. SNMP Traps and Trap Dial-Out Options (3 of 4)

DLCI Traps on Interfaces
Possible Settings: **Network, Ports, 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 the user data port only. **All** – Generates these trap messages on all frame relay interfaces.
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 alarm or 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. **Enable** – Automatically calls the phone number contained in the Control menu's Modem Call Directories, Directory Number A (Alarm). **Disable** – For traps, where the COM port-connected external device has not completed the connection, holds the messages.
Trap Disconnect
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the modem disconnects after the SNMP trap message has been sent. This configuration option only applies to external device 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.

Table 8-16. SNMP Traps and Trap Dial-Out Options (4 of 4)

Call Retry
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls whether an incomplete call (busy, no answer, etc.) is retried when an SNMP trap message is sent to the COM port-connected external device. **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. 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). **Disable** – Does not retry an incomplete call.
Dial-Out Delay TIme (Min)
Possible Settings: **1 – 10** Default Setting: **5**
Specifies the amount of time between call retries when an SNMP trap message is sent; the wait between call attempts (see Call Retry). **1 – 10** – Sets the number of minutes for the delay between call retry attempts (inclusive).
Alternate Dial-Out Directory
Possible Settings: **None, 1 – 5** Default Setting: **None**
Specifies whether an incomplete call (busy, or no answer, etc.) resulting from an attempt to send an SNMP trap message is retried using an alternate telephone number. Up to 5 alternate call directories can be set up, but only one at a time can be used. When Call Retry is enabled, the alarm directory's telephone number is called first. If the call cannot be completed after one additional try, then the specified alternate directory's telephone number is called. **None** – Does not dial-out using one of the alternate directory telephone numbers. **1 – 5** – Specifies the call directory containing the telephone number to call if a call cannot be completed using the telephone number in the alarm directory (Directory Number A in the Control menu's Modem Call Directories), inclusive.

Configuring the Communication Port

Select Communication Port to display or change the communication port configuration options (see Table 8-17).

Main Menu → Configuration → Management and Communication → Communication Port

Table 8-17. 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 8-11, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. **Terminal** – The COM port is used for the asynchronous terminal connection. **Net Link** – The COM port is the network communications link to the IP network or IP device port.
Data Rate (Kbps)
Possible Settings: **9.6, 14.4, 19.2, 28.8, 38.4, 57.6, 115.2** Default Setting: **19.2**
Specifies the rate for the COM port in kilobits per second. **9.6 – 115.2 kbps**
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 8-17. Communication Port Options (2 of 4)

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

Table 8-17. 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. NOTE: Changing this setting does not affect the current session; it changes all subsequent sessions. **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. NOTE: Changing this setting does not affect the current session; it changes all subsequent sessions. **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, see Table 8-17). *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, see Table 8-17, Communication Port Options). *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 8-17. 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, see Table 8-17, Communication Port Options). *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 only between devices to enable routing of IP traffic. **Standard_out** – The device will send standard RIP messages to communicate routing information about other FrameSaver units in the network. Standard RIP messages received on this link are ignored. NOTE: The router must be configured to receive RIP on the port connected to the COM 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* on page 8-11).

Configuring the COM Port to Support an External Modem

Select External Modem (on Com Port) to display or change the configuration options that control call processing for an external device attached to the COM port (see Table 8-18).

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

NOTE:

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

Table 8-18. External Modem (on Com Port) Options (1 of 2)

External Device Commands
Possible Settings: **Disable, AT** Default Setting: **Disable**
Specifies the type of commands to be sent over the COM port. CAUTION: You must *not* use this setting if you have an async terminal connected to the COM port. **Disable** – Commands will not be sent over the COM port. **AT** – Standard Attention (AT) Commands are sent over the COM port to control the external device. All AT command strings will end with a carriage return (hex 0x0D) and a line feed (hex 0x0A).
Dial-In Access
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls whether external devices can dial-in to the FrameSaver unit through the COM port (based on the Port Use option setting). *Display Conditions* – This option does not appear if External Device Commands is disabled. **Enable** – Answers incoming calls and establishes connection to the remote terminal or IP network. **Disable** – Does not answer incoming calls. Refer to the Control Characters table on page 8-78.

Table 8-18. External Modem (on Com Port) Options (2 of 2)

Alternate IP Address

Possible Settings: **001.000.000.000 – 223.255.255.255, Clear**
Default Setting: **Clear** (000.000.000.000)

Specifies the Alternate IP Address for the COM port when the alternate phone directory is used. If this configuration option is not configured (i.e., it is zero), the COM port's primary IP Address is used when the alternate telephone directory is used.

Display Conditions – This option:

- Only appears if External Modem Commands is set to AT.
- Is only in effect when the COM port is configured as a network communication lonk (Port Use is set to Net Link, see Table 8-17, Communication Port Options).

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.

Alternate Subnet Mask

Possible Settings: **000.000.000.000 – 255.255.255.255, Clear**
Default Setting: **000.000.000.000**

Specifies the Alternate Subnet Mask for the COM port when the alternate phone directory is used.

Display Conditions – This option:

- Only appears if External Modem Commands is set to AT.
- Is only in effect when the COM port is configured as a network communication lonk (Port Use is set to Net Link, see Table 8-17, Communication Port Options).

000.000.000.000 – 255.255.255.255 – Shows the subnet mask for the COM port, which you can view or edit.

Clear – Clears the subnet mask for the COM port and fills the address with zeros. 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.

Control Characters

Sequence	**ASCII**	**Hex**
^A or ^a	SOH	0x01
^B or ^b	STX	0x02
^C or ^c	ETX	0x03
^D or ^d	EOT	0x04
^E or ^e	ENQ	0x05
^F or ^f	ACK	0x06
^G or ^g	BEL	0x07
^H or ^h	BS	0x08
^I or ^i	HT	0x09
^J or ^j	LF or NL	0x0A
^K or ^k	VT	0x0B
^L or ^l	FF or NP	0x0C
^M or ^m	CR	0x0D
^N or ^n	SO	0x0E
^O or ^o	SI	0x0F
^P or ^p	DLE	0x10
^Q or ^q	DC1	0x11
^R or ^r	DC2	0x12
^S or ^s	DC3	0x13
^T or ^t	DC4	0x14
^U or ^u	NAK	0x15
^V or ^v	SYN	0x16
^W or ^w	ETB	0x17
^X or ^x	CAN	0x18
^Y or ^y	EM	0x19
^Z or ^z	SUB	0x1A
^{ or ^[	ESC	0x1B
^\ or ^|	FS	0x1C
^] or ^}	GS	0x1D
^^ or ^~	RS	0x1E
^–	US	0x1F

Security and Logins

9

This chapter provides information about the following:

Limiting Access

The FrameSaver unit provides access security through the following:

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

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 async terminal session, or two simultaneous async terminal sessions.

Controlling Asynchronous Terminal Access

The FrameSaver unit provides the following methods for limiting direct access to the menu-driven user interface on the communication (COM) port:

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

See *Configuring the Communication Port* in Chapter 8**,** *Configuration Options,* for more information about communication port configuration options.

▶ Procedure

To limit COM port access to the menu-driven user interface:

1. Follow this menu selection sequence:

   Main Menu → Configuration → Management and Communication → Communication Port

   The Communication Port Options screen appears.

2. Select and 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* on page 9-11.
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 FrameSaver Unit* in Chapter 10, *Operation and Maintenance*, should you inadvertently be locked out.

3. Save your changes.

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 it can be on a service provider's troubleshooting (TS) management link.

Limiting Telnet Access

Methods for limiting access through a Telnet session include the following:

- Disabling Telnet access completely.
- Requiring a user ID or password to login for Telnet Sessions not on the TS Management Link.
- Assigning an access level for Telnet sessions.
- Disabling special TS Management Link access (see page 9-5).

To limit Telnet access via a service provider's troubleshooting management link, follow the procedure on page 9-5.

▶ Procedure

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

1. Go to the Telnet and FTP Session Options screen.

   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* on page 9-11.
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 8**,** *Configuration Options,* for more information about communication port configuration options.

Limiting FTP Access

The FrameSaver unit provides the following methods for limiting access through a FTP session:

- Disabling FTP access completely.
- Requiring a user ID or password to login.
- Bandwidth of FTP.

▶ Procedure

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

1. Follow this menu selection sequence:

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

2. Select and 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* on page 9-11. 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 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 8**,** *Configuration Options,* for more information about setting FTP 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. Go to the Telnet and FTP Session Options screen.

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

2. Set the following configuration options, as appropriate.

   — Set Telnet Session to Disable.

   — Set FTP Session to Disable.

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

4. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Disable access via a TS Management Link	TS Management Link to None.
Assign an access level to the TS Management Link	TS Management Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the session (e.g., if a user has a Level-1 login and Level-2 telnet access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow users to configure the unit, keep the access at Level-1.

5. Save your changes.

See *Configuring Telnet and/or FTP Session Support* or *Configuring Node IP Information* in Chapter 8**,** *Configuration Options,* for more information about these configuration options.

Controlling SNMP Access

The FrameSaver unit supports SNMP Version 1, which only 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 access type.
- Assigning IP addresses of NMSs that can access the FrameSaver unit.

Disabling SNMP Access

The General SNMP Options screen provides the configuration option to disable SNMP access to the unit. When this configuration option is disabled, the FrameSaver unit will not respond to any SNMP messages.

▶ Procedure

To disable SNMP access:

1. Follow this menu selection sequence:

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

   The General SNMP Options screen appears.

2. Set SNMP Management to Disable.

3. Save your changes.

See *Configuring SNMP Management* in Chapter 8**,** *Configuration Options,* for more information about General SNMP Management configuration options.

Assigning SNMP Community Names and Access Levels

The General SNMP Options screen provides the configuration options that allow the FrameSaver unit to be managed by an SNMP manager supporting the SNMP protocol. Use this screen to:

- Assign the SNMP community names that are allowed to access the FrameSaver unit's Management Information Base (MIB).
- Specify the type of access allowed for each SNMP community name.

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

▶ Procedure

To assign SNMP community names and access levels:

1. Follow this menu selection sequence:

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

   The General SNMP Management Options screen appears.

2. Select and 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 SNMP Management* in Chapter 8**,** *Configuration Options,* for more information about General SNMP Management configuration options.

Limiting SNMP Access Through IP Addresses

The FrameSaver unit provides an additional level of security by:

- Limiting the IP addresses of the 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 SNMP Management* in Chapter 8**,** *Configuration Options,* for more information about SNMP management configuration options.

▶ Procedure

To limit SNMP access through IP addresses:

1. Follow this menu selection sequence:

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

   The SNMP NMS Security Options screen appears.

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 8**,** *Configuration Options,* for more information about SNMP NMS Security configuration options.

Controlling External COM Port Device Access

The FrameSaver unit allows you to control whether dial-in access for an external device (modem) is allowed on the communication port. Use the External Device Options screen to set the necessary configuration options to allow dial-in access through the COM port.

▶ Procedure

To control dial-in access:

1. Follow this menu selection sequence:

   Main Menu → Configuration → User Interface →
   External Modem (on Com Port)

   The External Modem Options screen appears.

2. Enable the Dial-In Access configuration option.

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

3. Save your changes.

See *Configuring the COM Port to Support an External Device* in Chapter 8**,** *Configuration Options,* for more information about external device communication port configuration options.

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* on page 9-11.
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 FrameSaver Unit* in Chapter 10, *Operation and Maintenance*, should you inadvertently be locked out.

4. Save your changes.

See *Configuring the Communication Port* in Chapter 8**,** *Configuration Options,* for more information about communication port configuration options.

Creating a Login

A login ID and password is required if security is enabled.* You can define a combination of six login/passwords. Each login must be unique and have a specified access level.

▶ Procedure

To create a login ID and password:

1. Follow this menu selection sequence:

   Main Menu → Control → Administer Logins

2. Select New from the function keys area and press Enter.

3. Enter the login ID, password, and security level for each login.

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. **Note:** Make sure at least one login is setup for Level-1 access or you may be inadvertently locked out.

NOTE:

See *Resetting the FrameSaver Unit* in Chapter 10, *Operation and Maintenance*, should you inadvertently be locked out.

4. Save your changes.

   When Save is complete, **`Command Complete`** appears at the bottom of the screen and the cursor is repositioned at the Login ID field, ready for another entry.

See *Configuring SNMP NMS Security* in Chapter 8**,** *Configuration Options,* for more information about security configuration options.

* Security is enabled by the Communication Port's Login Required option. For a Telnet or FTP session, the Telnet or FTP Session's Telnet Login Required or FTP Login Required option is also enabled.

Modifying a Login

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

Deleting a Login

A login record can be deleted.

▶ Procedure

To delete a login record:

1. Follow this menu selection sequence:

   Main Menu → Control → Administer Logins

2. Press Ctrl-a to switch to the screen function key area.

3. Select PgUp or PgDn and press Return to page through login pages/records until you find the one to be deleted.

4. Once the correct record is displayed, select Delete and press Enter.

5. Save your deletion.

   When the deletion is complete, **`Command Complete`** appears at the bottom of the screen. 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

10

This chapter includes the following information:

- — *Changing Software* on page 10-39.
- — *Transferring Collected Data* on page 10-40.

Displaying System Information

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

▶ Procedure

To view system information:

1. Access the Identity menu.

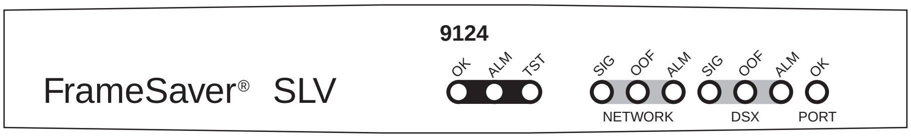
   Main Menu → Status → Identity

2. Select System & NAM to view the following information:

View this field . . .	To find the . . .
System Name	Domain name for this SNMP-managed node (up to 255 ASCII characters).
System Contact	Contact person for this SNMP-managed node.
System Location	Physical location for this SNMP-managed node.
NAM	
NAM Type	Type of unit installed, referred to as a network access module, or NAM (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.

Viewing LEDs and Control Leads

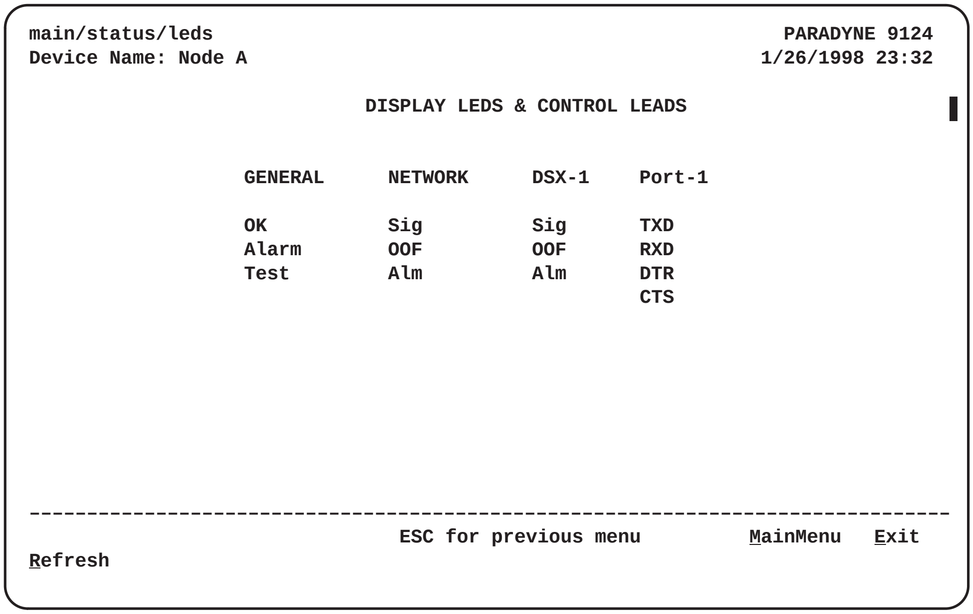
The FrameSaver 9124 unit's faceplate includes LEDs (light-emitting diodes) that provide status on the unit and its interfaces.



99-15821-02

The Display LEDs and Control Leads feature allows you to monitor a remote unit, and is useful when troubleshooting control lead problems. This feature is selected from the Status menu.

Main Menu → Status → Display LEDs and Control Leads



```
main/status/leds                                                  PARADYNE 9124
Device Name: Node A                                             1/26/1998 23:32

                             DISPLAY LEDS & CONTROL LEADS


                   GENERAL     NETWORK      DSX-1    Port-1

                   OK          Sig          Sig      TXD
                   Alarm       OOF          OOF      RXD
                   Test        Alm          Alm      DTR
                                                     CTS








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

LED Descriptions

The following tables describe what these LEDs indicate.

Table 10-1. General Status LEDs

Label	Indication	Color	What It Means
OK	Power and Operational Status	Green	ON – FrameSaver unit has power and is operational. OFF – FrameSaver unit is in a power-up self-test, or there is a failure.
ALM	Operational Alarm (Fail)	Red	ON – FrameSaver unit has just been reset, or an error or fault has been detected. Error/fault/alarm conditions: ■ Out of Frame (OOF) ■ Loss of Signal (LOS) ■ Alarm Indication Signal (AIS) ■ Exceeded Error Rate (EER) ■ Yellow Alarm Signal ■ Device Fail ■ Self-Test Failed ■ Power Supply Failure ■ LMI Down ■ DLCI Down ■ 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.

Table 10-2. Network or DSX Interface LEDs

Label	Indication	Color	What It Means
SIG	Signal	Green	ON – A recoverable signal is present on the Network/DSX interface. OFF – The signal cannot be recovered from the Network/DSX 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 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 interface.

Table 10-3. Data Port Interface 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.

Device Messages

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

Table 10-4. Device Messages (1 of 6)

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.
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.

Table 10-4. Device Messages (2 of 6)

Message	What It Indicates	What To Do
File Transfer Complete (Seen at an FTP terminal.)	A file transfer was performed successfully.	Switch to the newly downloaded software.
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.
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 29th).	Reenter the date in the month/day/4-digit year format.
Invalid time: must be hh:mm	A non-valid system time was entered on the System Information screen.	Reenter the time in the hour:minutes 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.

Table 10-4. Device Messages (3 of 6)

Message	What It Indicates	What To Do
Limit of six Login IDs reached	An attempt to enter a new login ID was made, and the limit of six login/password combinations has been reached.	■ Delete another login/password combination. ■ Reenter the new login ID.
Limit of Mgmt PVCs reached	New was selected from the PVC Connection Table and the maximum number of management PVCs has already been created.	■ Do not create the management PVC. ■ Delete another management PVC, and try again.
Limit of PVC Connections reached	New was selected from the PVC Connection Table and the maximum number of PVCs has already been created.	■ Do not create the PVC connection. ■ Delete another PVC connection, and try again.
Name Must be Unique	Name entered for a management PVC has been used previously.	Enter another 4-character name for the logical/management link.
No Destination Link DLCIs Available	New was selected from the PVC Connection Table, but even though DLCIs are available to form a connection, no DLCIs are available on the network link, which is a suitable PVC Destination.	Configure additional DLCIs for the network link and try again.
No DLCIs available for connection	New was selected from the PVC Connection Table, but all configured DLCIs have been connected.	No action needed, or configure more DLCIs and try again.
No DLCIs available for connection	New was selected from the Management PVCs option screen, but all Link/DLCI pairs have been connected.	Configure more network and/or Port-1 Links/DLCIs pairs and try again.
No DLCIs Available for Mgmt PVC	New was selected from the Management PVCs option screen, but all configured DLCIs have been connected.	Configure more network and/or Port-1 DLCIs and try again.

Table 10-4. Device Messages (4 of 6)

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

Table 10-4. Device Messages (5 of 6)

Message	What It Indicates	What To Do
Permission Denied (Seen at an FTP terminal.)	A file transfer was attempted, but the: ■ User did not have Level 1 security. ■ Wrong file was specified when the **put** command was entered. ■ User attempted to upload a program file from the unit.	■ See your system administrator to get your security level changed. ■ Try again, entering the correct file with the **put** command. ■ Enter the **put** command instead of a **get** command; you can only transfer files to the unit, not from it. See *Performing a Software Upgrade* in Chapter 12, *Operation and Maintenance*.
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.
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 async user interface through the COM or modem port is made. 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 logoff.

Table 10-4. Device Messages (6 of 6)

Message	What It Indicates	What To Do
User Interface Idle	Previously active session is now closed/ended, and access via the COM port or modem port is now available. Previously active session is now closed/ended, and access via the COM port is now available.	Log onto 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 – 1536000).
	Excess Burst Size entered for the DLCI is a number greater than the maximum allowed.	Enter a valid Excess Burst Size (0 – 1536000).
	DLCI Number entered is less than 16 or greater than 1007.	Enter a valid number (16 – 1007).

Status Information

Status information is useful when monitoring the FrameSaver unit. Use the Status menu to display information concerning:

- *System and Test Status Messages* – Health and Status, Self-Test Results, Test Status (see page 10-12)
- *Network LMI Reported DLCIs Status* – DLCIs, Status, and CIR (Kbps) (see page 10-20)
- *PVC Connection Status* – Source and Destination Links, DLCIs, EDLCIs, and connection status (see page 10-21)
- *Time Slot Assignment Status* (see page 10-22)

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* on page 10-12.
- *Health and Status Messages* on page 10-13.
- *Test Status Messages* on page 10-18.

Self-Test Results Messages

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

Table 10-5. Self-Test Results Messages

Message	What It Indicates	What To Do
Failure *xxxxxxxx*	An internal failure occurred *(xxxxxxxx* represents an 8-digit hexadecimal failure code 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

These messages appear in the left column of the System and Test Status screen, or the highest priority Health and Status message appears on the last line at the bottom of the screen (right corner).

Table 10-6. Health and Status Messages (1 of 5)

Message	What It Indicates	What To Do
AIS at DSX-1	An Alarm Indication Signal (AIS) is received by the DSX-1 interface. AIS is an unframed, all ones signal.	Check the DTE attached to the DSX-1 interface.
AIS at Network	An Alarm Indication Signal (AIS) is received by the network interface. AIS is an unframed, all ones signal. The network is transmitting an AIS.	Report problem to carrier.
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.	No action needed unless you want to disable this feature.
Back-to-Back Mode is Active	The operating mode has been configured for back-to-back (*Control → Change Operating Mode).* The FrameSaver unit can be connected to another FrameSaver unit without a frame relay switch between them. See *Back-to-Back Operation* in Chapter 3, *Typical Applications*, for an illustration.	No action needed unless you want to disable this feature. This feature is useful for product demonstrations or for a point-to-point configuration using a leased line.
CTS down to Port-1 Device	The Port-1 CTS control lead on the FrameSaver unit is off.	Check DTR and RTS from Port-1.

Table 10-6. Health and Status Messages (2 of 5)

Message	What It Indicates	What To Do
Device Fail *yyyyyyyy*	An internal error has been detected by the operating software.	1. Provide the displayed 8-digit failure code (*yyyyyyyy*) to your service representative. 2. Clear the Device Fail message. *Main Menu → Control → Clear Device Fail*
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 network provider.
DTR down from Port-1 Device	The DTR control lead on the device connected to Port-*n* is disasserted.	Examine the attached DTE and cable connected to the FrameSaver unit's port. 1. Check that the Port-1 cable is securely attached at both ends. 2. Check the status of the attached equipment.
EER at Network *n*	The error rate of the received network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider.

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

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

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

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

Table 10-6. Health and Status Messages (3 of 5)

Message	What It Indicates	What To Do
LMI Down, *frame relay link* [2]	The Local Management Interface is down for the specified frame relay link.	For the Network interface: 1. If LMI was never up, verify that the proper time slots have been configured. 2. If LMI was never up, verify that the LMI Protocol setting reflects the LMI type being used. 3. 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 network provider.
		For Port-*n*: 1. Check that the DTE cable is securely attached at both ends. 2. Verify that Transmit Clock Source and Invert Transmit Clock options are properly configured. 3. Verify that Frame Relay Performance Statistics show LMI frames being received. If no frames are being received: – Check the attached device. – Verify that the LMI Protocol setting reflects the LMI type being used.

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

Table 10-6. Health and Status Messages (4 of 5)

Message	What It Indicates	What To Do
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%.	
	1. Network cable problem.	1. Check that the network cable is securely attached at both ends.
	2. T1 facility problem.	2. Contact your network provider.
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%.	
	1. DSX-1 cable problem.	1. Check that the DSX-1 cable is securely attached at both ends.
	2. No signal being transmitted from the DTE.	2. Check the DTE status.
NAM Download Failed	A download attempt was interrupted and failed to complete.	■ Retry downloading. ■ Contact service representative.
NAM Fail appears on the System Health and Status screen.	The FrameSaver unit detects an internal hardware failure.	Record the 8-digit code from the System Health and Status screen, then contact your service representative.
Network Com Link Down	The communication link for the COM port is down, and the COM port is configured for Net Link.	Check the router connected to the COM port.
OOF at DSX-1	An Out of Frame (OOF) condition is detected on the DSX-1 interface.	Cleared when a reframe occurs.
	1. Incompatible framing format between the DTE and the FrameSaver unit.	1. Check that the framing format for the DSX-1 (DTE) interface is correct.
	2. DSX-1 cabling problem.	2. Check that the DSX-1 cable is securely attached at both ends.

Table 10-6. Health and Status Messages (5 of 5)

Message	What It Indicates	What To Do
OOF at Network *n*	An Out of Frame (OOF) condition is detected on the network interface. 1. Incompatible framing format between the network and the FrameSaver unit. 2. Network cabling problem. 3. T1 facility problem.	Cleared when a reframe occurs. 1. Check that the framing format for the network interface is correct. 2. Check that the network cable is securely attached at both ends. 3. Contact your network provider.
Primary Clock Failed	A failure of the primary clock source configured for the NAM is detected and the secondary clock is providing the timing for the NAM. This condition clears when the configured primary clock is restored.	1. Check that the cable is securely attached at both ends for the primary clock source interface. 2. Contact the network provider.
Primary & Secondary Clock Failed	A failure of the primary and secondary clock sources configured for the FrameSaver unit are detected and the internal clock is providing the timing for the unit. The clock source will not automatically switch from internal until the primary clock source returns.	1. Check that the cable is securely attached at both ends for the primary and secondary clock source interfaces. 2. Contact the network provider.
Yellow at DSX-1	A yellow alarm signal is received on the DSX-1 interface. DTE has detected a LOS or OOF condition.	1. Check that the DSX-1 cable is securely attached at both ends. 2. Check the status of the attached equipment.
Yellow at Network *n*	A yellow alarm signal is received on the specified network interface. 1. Network cable problem. 2. T1 facility problem.	1. Check that your network cable is securely attached at both ends. 2. Contact your network provider.

[1] Record the failure code before resetting the FrameSaver unit; otherwise, the error information will be lost.

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. Refer to Chapter 13, *Troubleshooting*, for more information on tests, including how to start and stop them.

Table 10-7. Test Status Messages (1 of 2)

Message	What It Indicates
DCLB Active, Port-1 or *frame relay link*	A Data Channel Loopback is active on the data port or a T1 frame relay link.
DTE External LB Active, Port-1	An external DTE Loopback is running on the specified port.
DTE Init. Ext LB Active, Port-1	DTE has initiated an external DTE Loopback on the specified port.
FCC Test Active	Should never see this message.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the faceplate to flash on and off.
Monitor *Pttn* Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	FrameSaver unit is monitoring a test pattern on the specified DLCI on the specified frame relay link.
Monitor *Pttn* Active, *[interface]*	FrameSaver unit is monitoring the selected test pattern on the specified interface.
LLB Active, DSX-1 LLB Active, Network	A Line Loopback (LLB) test is active on the specified network interface.
PLB Active, DSX-1 PLB Active, Network	A Payload Loopback (PLB) test is active on the specified network interface.

Table 10-7. Test Status Messages (2 of 2)

Message	What It Indicates
DTPLB Active, Slot-1, Port-1	A Data Terminal Payload Loopback (DTPLB) is active for the specified slot and port. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
RLB Active, DSX-1	A Repeater Loopback (RLB) test is active on the DSX-1 interface.
No Test Active	No tests are currently running.
PVC Loopback Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	FrameSaver unit is monitoring the selected test pattern on the specified DLCI for the interface.
Monitor *Pttn* Active, *[Inteface]*	A Monitor Pattern test (user-selected pattern) is active on the specified interface (and in the specified slot). This test cannot be activated on user data ports that have Port Use set to Frame Relay.
Send *Pttn* Active, *[Inteface]*	A send pattern test is active on the specified interface.
Send *Pttn* Active, DLCI *nnnn*, *frame_relay_link* [1, 2]	FrameSaver unit is monitoring the selected test pattern on the specified DLCI for the interface.
No Test Active	No tests are currently running.
PVC Loopback Active, DLCI *nnnn*, *frame_relay_link*	A PVC Loopback is active on the specified DLCI and frame relay link.

[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 by for the network port, Network 1.

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

Network LMI-Reported DLCIs Status

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

Main Menu → Status → LMI Reported DLCIs

The LMI Reported DLCIs screen displays the status and CIR (if supported by the switch) for each DLCI, whether the DLCI is configured or not. An asterisk identifies each DLCI contained in the device configuration. Data and LMI status received on DLCIs that are not configured pass transparently through the unit between the network interface and the first data port without monitoring of DLCI traffic or demultiplexing/multiplexing management diagnostics or user data. Data received on DLCIs that are not configured on other frame relay links is discarded.

Table 10-8. Network LMI-Reported DLCIs Status

Field	Status	What It Indicates
DLCI	16 through 1007	Identifies the Local Management Interface-reported DLCI numbers assigned to the selected interface – the identifying number assigned to the path between two frame relay FrameSaver units' ports. DLCI statuses are listed in ascending order (i.e., lowest number first).
Status	Active Inactive Deleted [1] New [1]	LMI-reported status of the DLCI: ▪ Whether the DLCI is active (capable of carrying data) in the frame relay network, ▪ Whether it is inactive, ▪ Whether it has been deleted by the frame relay network, or ▪ Whether it has been created by the frame relay network.
CIR (bps)	0 – 1536000	Displays the committed information rate reported by the Stratacom switch. CIR information only appears in this column when LMI Protocol is set to Standard. If blank, the switch does not support this feature.

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

PVC Connection Status

PVC connection statuses are selected from the Status menu. Only PVC connections with Source DLCIs configured to be Active are shown. See page 10-22 for an example of this screen.

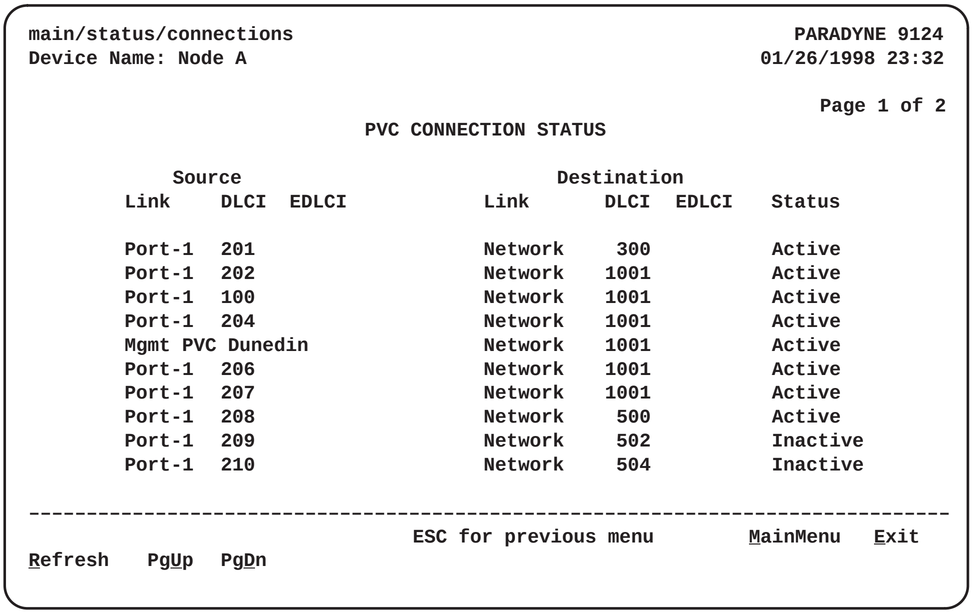
Main Menu → Status → PVC Connection Status

Table 10-9. PVC Connection Status

Field	Status	What It Indicates
—	No PVC Connections.	PVC connections have yet to be defined.
Link	Network Port-1	Identifies the cross-connection of DLCIs configured for the unit. ■ Network – T1 network ■ Port – Port-1 ■ Source/destination is frame relay link *x* on Network *n* ■ 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	Active [1] Inactive	Identifies whether the physical interfaces, LMIs, and DLCIs are all enabled and active for this PVC connection.

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

PVC Connection Status Screen Example



```
main/status/connections                                            PARADYNE 9124
Device Name: Node A                                             01/26/1998 23:32

                                                                     Page 1 of 2
                             PVC CONNECTION STATUS

            Source                                Destination
        Link     DLCI  EDLCI               Link       DLCI  EDLCI    Status

        Port-1   201                       Network     300           Active
        Port-1   202                       Network    1001           Active
        Port-1   100                       Network    1001           Active
        Port-1   204                       Network    1001           Active
        Mgmt PVC Dunedin                   Network    1001           Active
        Port-1   206                       Network    1001           Active
        Port-1   207                       Network    1001           Active
        Port-1   208                       Network     500           Active
        Port-1   209                       Network     502           Inactive
        Port-1   210                       Network     504           Inactive

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

Time Slot Assignment Status

Time slot assignments are made using the Time Slot Assignment configuration option. See *Assigning Time Slots/Cross Connections* in Chapter 9, *Configuration Options*, for making time slot assignments. Use the Timeslot Assignment Status screen to display time slot assignments for:

- Network Channels
- 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.

Use the following menu sequence to display network channel information.

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 time slot of the Network Interface. The bottom field represents the cross connect status of the associated (top field) network time slot.

The following information is available for viewing.

The Network Time Slot Fields (top) . . .	Indicates . . .
N01 to N24	The Network Interface time slot (01 to 24).

The Cross Connect Status Field (bottom) . . .	Indicates . . .
Unassgn	The time slot is unassigned.
FrameRly*x*	The time slot is assigned to Network Frame Relay Link
D*ss-p*/*yy*	The DSX-1 on slot *ss*, port *p*, time slot *yy* is assigned to the Network Interface time slot (01 to 24).
D*ss-p*/*yy*r	The DSX-1 on slot *ss*, port *p*, time slot *yy* is assigned to the Network Interface time slot (01 to 24), using Robbed Bit Signaling (r).

FrameSaver physical slot assignment information appears below the DSX-1 interface time slot fields.

The following information is available for viewing.

Physical Slot . . .	Identifies the assigned card type . . .
01 to 14 (based on model)	**T1 NAM** – T1 NAM. **Empty** – The slot is empty.

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.

Use the following menu sequence to display DSX-1 channel information.

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

Select the desired DSX-1 slot and port.

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.

The following information is available for viewing.

The DSX-1 Time Slot Fields (top) . . .	Indicate . . .
D01 to D24	The DSX-1 Interface time slot (01 to 24).

The Cross Connect Status Field (bottom) . . .	Indicates the . . .
blank	Time slot is unassigned.
Net*nyy*	Network Interface *n* (1 or 2), time slot (*yy*) is assigned to DSX-1 time slot (01 to 24), using Clear Channel.
Net*nyy*r	Network Interface *n* (1 or 2), time slot (*yy*) is assigned to DSX-1 time slot (01 to 24), using Robbed Bit Signaling (r).

FrameSaver physical slot assignment information appears below the DSX-1 interface time slot fields.

The following information is available for viewing.

Physical Slot . . .	Identifies the assigned card type . . .
01 to 14 (based on model)	**T1 NAM** – T1 NAM. **Empty** – The slot is empty.

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

The following performance statistics are collected:

- *Service Level Verification Performance Statistics* on page 10-27.
- *DLCI Performance Statistics* on page 10-28.
- *Frame Relay Performance Statistics* on page 10-30.
- *ESF Line Performance Statistics* on page 10-33.

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.

If you have a Level-1 security access level, you can reset the performance statistics locally using an asynchronous terminal (see *Clearing Performance Statistics* on page 10-26).

Clearing Performance Statistics

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

Statistic counters are not actually cleared using this feature. True statistic counts are always maintained so SLAs can be verified, and they can be viewed from an SNMP NMS. However, since statistics can be cleared locally, the statistics viewed on the asynchronous terminal 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 <u>C</u>lrSLV&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 <u>C</u>lrLinkStats function key to reset the frame relay link performance statistics.

  Performance Statistics → Frame Relay

- Use the Clr<u>N</u>earStats and Clr<u>F</u>arStats function keys to reset ESF line performance statistics.

  Performance Statistics → ESF Line

Determining Whether a Statistic Is Incrementing

Use this procedure when you do not have a Level-1 access and 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 <u>R</u>efresh 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 <u>R</u>efresh the screen until you have a sense of how serious the problem might be.

Service Level Verification Performance Statistics

These statistics appear when Service Level Verification (SLV) is selected from the Performance Statistics menu. These statistics only appear for the network interface and only if DLCIs are multiplexed (see DLCI Type option in Table 8-9, DLCI Records Options).

Main Menu → Status → Performance Statistics → Service Level Verification

Table 10-10. Service Level Verification Performance Statistics

Statistic	What It Indicates
Far End DLCI	Number of the multiplexed DLCI at the other end of the connection. None is displayed if the FrameSaver unit has not communicated with the other end.
Inbound Dropped Frames	Number of frames transmitted by the far-end unit that were dropped in transit. This count continues to accumulate until the maximum count value has been reached, then the count is reset and starts to accumulate dropped frames again.
Dropped SLV Responses	The number of SLV inband sample packets sent that did not receive a response.
Far End IP Addr	IP Address of the unit at the other end of the multiplexed DLCI connection. None is displayed if the FrameSaver unit has not communicated with the other end, or if the unit at the other end of the multiplexed DLCI does not have an IP Address configured.
Inbound Dropped Frames	Number of frames transmitted by the far-end unit that were dropped in transit. This count continues to accumulate until the maximum count value has been reached, then the count is reset and starts to accumulate dropped frames again.
Inbound Dropped Characters	Number of bytes transmitted by the far-end unit that were dropped in transit. This count continues to accumulate until the maximum count value has been reached, then the count is reset and starts to accumulate dropped characters again.

Table 10-10. Service Level Verification Performance Statistics

Statistic	What It Indicates
Avg RdTrip Latency	Average round trip latency, measured in milliseconds, between the FrameSaver unit and the unit at the other end of the multiplexed DLCI connection. Average round trip latency is measured every SLV sampling interval and the average is computed over the previous 15 sampling intervals. Unknown is displayed if communication with the far-end unit over the last five minutes has not been successful.
Max RdTrip Latency	Same as average (Avg RdTrip Latency), but storing the maximum number of milliseconds over the sampling interval instead. Unknown is displayed if communication with the far-end unit over the last 15 sampling intervals has not been successful.

DLCI Performance Statistics

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

Main Menu → Status → Performance Statistics → DLCI

Table 10-11. 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 FrameSaver unit discovered that the DLCI was active in the network.
DLCI Up Time [1]	Days, hours, minutes, and seconds since the DLCI was last declared Active after a period of inactivity. Down is displayed if the DLCI is inactive. If the DLCI was Down, this is the amount of time since the DLCI recovered. If the DLCI was never Down, this is the amount of time since the FrameSaver unit 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.

[1] Appears only for the Network interface.

Table 10-11. DLCI Performance Statistics (2 of 2)

Statistic	What It Indicates
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.
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

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

Main Menu → Status → Performance Statistics → Frame Relay

Table 10-12. Frame Relay Performance Statistics (1 of 4)

Statistic	What It Indicates
Frame Relay Link	
Frames Sent	Number of frames sent over the interface.
Frames Received	Number of frames received over the interface.
Characters Sent	Number of data octets (bytes) sent over the interface.
Characters Received	Number of data octets (bytes) received over the interface.
FECNs Received	Number of FECNs received 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	Number of BECNs 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 10-12. Frame Relay Performance Statistics (2 of 4)

Statistic	What It Indicates
Frame Relay Errors	
Total Errors	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	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	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	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	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	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	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 10-12. Frame Relay Performance Statistics (3 of 4)

Statistic	What It Indicates
Frame Relay LMI	
LMI Protocol	LMI protocol configured for the frame relay link. Normal condition.
Status Msg Received	Number of LMI status messages received over the interface. Normal condition.
Total LMI Errors	Number of LMI errors. Reliability errors, protocol errors, unknown report types, unknown information elements, and sequence errors are included in this total. Network problems.
Number of Inactives	Number of times the LMI has declared the frame relay link Inactive. Network problems.
Frame Relay HDLC Errors	
Rx Total Errors	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	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	Number of receiver overruns (too many bits) on the interface.
Rx DTR Lost Events[1]	Number of times DTR has been lost/lowered on the T1 or ISDN interface.
Rx Non-Octet Frames	Number of non-octet frames received on the interface.
Rx CRC Errors	Number of received CRC (cycle redundancy check) errors.

[1] Does not appear when Port Type is set to X.21 (see Port Type option in Table 9-6, Data Ports Physical Options).

Table 10-12. Frame Relay Performance Statistics (4 of 4)

Statistic	What It Indicates
Tx Total Errors	Total number of transmit errors on the interface, including transmits discards and transmit overruns.
Tx Total Discards	Total number of transmit discards on the interface, including underrun flushes.
Tx CTS Lost Events [1]	Number of times CTS has been lost/lowered.
Tx Underruns	Number of transmitter underruns (too few bits) on the interface.

[1] Does not appear when Port Type is set to X.21 (see Port Type option in Table 9-6, Data Ports Physical Options).

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 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:

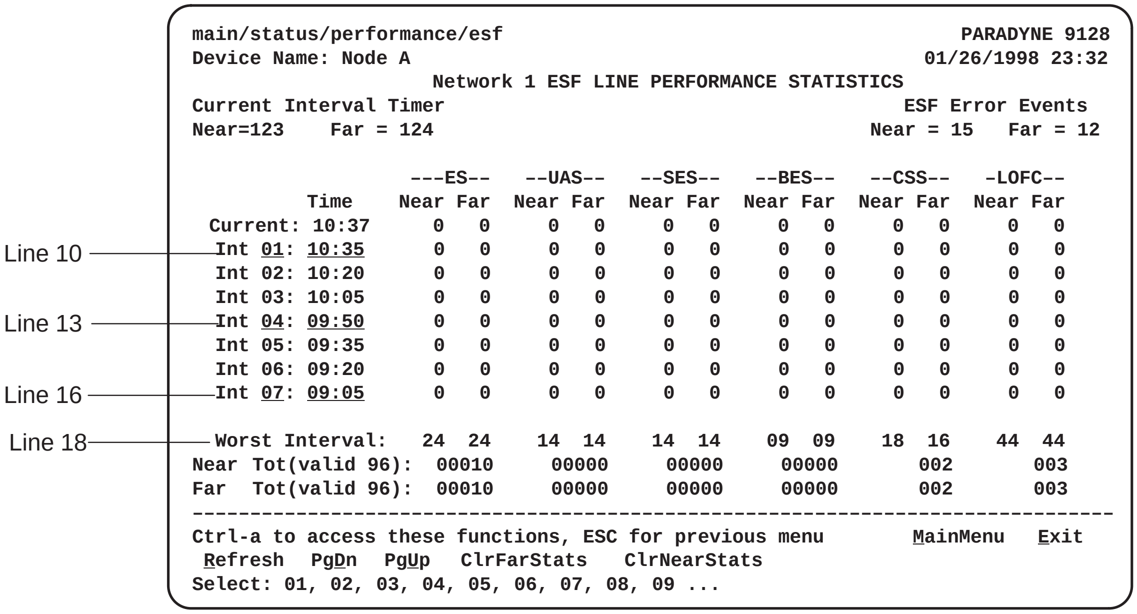
Interval 01 is the interval occurring just prior to the current one;
Interval 02 is 2 intervals prior to the current one, etc.

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                                       PARADYNE 9128
Device Name: Node A                                             01/26/1998 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
  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
  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
  Int 07: 09:05     0   0     0   0     0   0     0   0     0   0     0   0

  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 metrics are kept for each 15-minute interval over the past 24-hour period. A Near set and a Far set are kept for each metric. 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 include:

- **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.

You can collect the following metrics for the network interface.

Table 10-13. ESF Line 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.

FTP File Transfers

The FrameSaver unit supports a standard File Transfer Protocol (FTP) server over Transmission Control Protocol (TCP) to allow software upgrades, copying configurations, and SLV statistics gathering. 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 unit node, program files *to* a FrameSaver unit node, and User History data *from* a FrameSaver unit 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 SLV Statistics to an NMS* on page 10-40).
- 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 unit 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 9, *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 unit 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 unit 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 unit node. If *file2* is not specified, the file will be named *file1* on the FrameSaver unit 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 FrameSaver unit. A different R*xxxxxx*.ocd file will need to be downloaded. Repeat the step or end the FTP session.

NOTE:

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

⚠ 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* on page 10-39 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 on page 10-38, *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* on page 10-2 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 MaxReceive Rate (Kbps) option (see the FTP Max Receive Rate (Kbps) configuration option in Table 8-14, Telnet and FTP Session Options in Chapter 8, *Configuration*).

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 10-38 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 the retrieving . . .	Then . . .
SLV statistics	Perform a **get** of the **uhbcfull.dat** file. ■ File Transfer Complete – Transfer was successful. ■ File Transfer Failed – Transfer was not successful. Try again or end the session.
LMI packet capture data	1. Stop the LMI Packet Capture Utility. *Main Menu → Control → LMI Packet Capture Utility* LMI packet capture data is not available (readable) when the LMI Packet Capture Utility is Active. 2. Perform a **get** of the **lmitrace.syc** file. One of the following will display for the file: – File Transfer Complete – File Transfer Failed – Permission Denied – The LMI Packet Capture Utility was not readable. Stop the LMI Packet Capture Utility and try again.

3. Close the FTP session.

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

Troubleshooting

11

This chapter includes the following:

- *Physical Tests* on page 11-19.
  - *Line Loopback* on page 11-19.
  - *Payload Loopback* on page 11-20.
  - *Repeater Loopback* on page 11-21.
  - *Send Line Loopback* on page 11-22.
  - *Send and Monitor Pattern Tests* on page 11-23.
  - *DTE Loopback* on page 11-24.
- *IP Ping Test* on page 11-25.
- *Lamp Test* on page 11-27.
- *LMI Packet Utility* on page 11-28.

Problem Indicators

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

Indicators . . .	**See . . .**
LEDs	*Displaying LEDs and Control Leads* and *LED Descriptions* in Chapter 10, *Operation and Maintenance*, for faceplate LEDs, their description, as well as the user interface screen. *Main Menu → Status → Display LEDs and Control LEDs*
Health and Status	*Alarms* on page 11-5, and *Health and Status Messages* in Chapter 10, *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 10, *Operation and Maintenance*, to help you determine how long a problem has existed.
Alarm conditions that will generate an SNMP trap	*Alarms* on page 11-5.
SNMP traps	Appendix C, *SNMP MIBs and Traps, and RMON Alarm Defaults.*
Alarm system relay for units installed in a 5-slot housing	*Setting General System Optionss* in Chapter 8, *Configuration*, to enable this feature. *Main Menu → Configuration → System → General*

Resetting the Unit

You can reset the unit in one of four ways:

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

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

Resetting the Unit from the Control Menu

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

▶ **Procedure**

To reset the unit from the Control menu:

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

Resetting the Unit By Cycling the Power

Disconnecting, then reconnecting the power cord resets the unit.

Restoring Communication with a Misconfigured Unit

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

▶ Procedure

To reset COM port settings:

1. Configure the asynchronous terminal to operate at 19.2 kbps, using character length of 8 bits, with one stop-bit, and no parity. In addition, set Flow Control to None.
2. Reset the unit, then hold the Enter key down until the System Paused screen appears. (See *Resetting the Unit* on page 11-3 for other methods of resetting the unit.)
3. Tab to the desired prompt, and type **y** (Yes) at one of the prompts.

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

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

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

Alarms

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

Main Menu → Status → System and Test Status

Table 11-1. Alarm Conditions (1 of 4)

Alarm Condition	What It Indicates	What To Do
AIS at Network 1	An Alarm Indication Signal (AIS) is being received by the interface. AIS is an unframed, all ones signal.	For the network interface, report the problem to your T1 service provider.
AIS at DSX-1	For the DSX-1 interface, the attached DTE is transmitting an AIS.	For the DSX-1 interface, check the DTE attached to the interface.
CTS down to Slot-*s* Port-*p Device*	The CTS control lead on the device's interface is off.	Check DTR and RTS from Port-1.
DLCI *nnnn* Down, *frame_relay_link*	The DLCI for the specified frame relay link is down.	Verify that the network LMI is up. If it is, contact your network service provider.
Device Fail *yyyyyyyy*	An internal error has been detected by the operating software.	1. Provide the 8-digit failure code (*yyyyyyyy*) that follows the alarm to your service representative. 2. Clear the Device Fail message. *Main Menu → Control → Clear Device Fail*
DTR Down from Slot-*s* Port-*p* Device	The DTR control lead on the device connected to the specified port is off. This message applies to data ports that act as DCEs.	Examine the attached DTE and cable connected to the system's port. 1. Check that the port cable is securely attached at both ends. 2. Check the status of the attached equipment.
EER at Network 1	The error rate of the received network signal has exceeded the currently configured threshold. An Excessive Error Rate (EER) condition only occurs when the network interface is configured for ESF framing.	For the network interface: 1. Verify that the cable is securely attached at the Network interface. 2. Contact your network provider.

Table 11-1. Alarm Conditions (2 of 4)

Alarm Condition	What It Indicates	What To Do
LMI Down, *frame_relay_link*	The Local Management Interface is down for the specified frame relay link.	For the Network interface: 1. 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. 2. Verify that Frame Relay Performance Statistics show LMI frames being transmitted. If all of the above have been verified and the physical link is not in Alarm, contact your network provider.
		For User Data Port: 1. Check that the DTE cable is securely attached at both ends. 2. Verify that Transmit Clock Source and Invert Transmit Clock options are properly configured. 3. Verify that Frame Relay Performance Statistics show LMI frames being received. If no frames are being received: – Check the attached device. – Verify that the LMI Protocol setting reflects the LMI type being used.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the interface. For the network, DSX, or ISDN PRI DBM interface, an LOS condition is declared when 175 consecutive zeros are received.	For the network, DSX-1, or ISDN PRI DBM interface: 1. Check that the cable is securely attached at both ends. 2. Verify that the attached device is operational. 3. Contact your network provider.
LOS at DSX-1	For the DSX-1 interface, there may be a cable problem or the DTE may not be transmitting a signal.	

Table 11-1. Alarm Conditions (3 of 4)

Alarm Condition	What It Indicates	What To Do
Network Com Link Down	The communication link for the COM port is down and the COM port is configured for Net Link.	Check the router connected to the COM port.
OOF at Network 1	An Out of Frame (OOF) condition has been detected on the interface. An OOF condition is declared when two out of four frame-synchronization bits are in error. This condition clears when a reframe occurs.	For the network or DSX-1 interface: 1. Check that the cable is securely attached at both ends. 2. Check that the framing format for the interface is correct. 3. Contact your network provider.
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.	1. Check that the network cable is securely attached at both ends. 2. Contact your network provider.
Primary & Secondary Clocks Failed	A failure of both clock sources configured for the unit was detected This condition only applies to T1 network and DSX-1 interfaces. It clears when the configured primary clock is restored.	
Secondary Clock Failed	A failure of the configured secondary clock source for the unit was detected and the internal clock is providing the timing for the unit. The clock source will not automatically switch from internal until the primary clock source returns.	

Table 11-1. Alarm Conditions (4 of 4)

Alarm Condition	What It Indicates	What To Do
Self-Test Failure	The unit did not pass its basic verification tests when it was powered up or reset.	1. Reset the unit. 2. Contact your service representative.
SLV Timeout, DLCI *nnnn*, *frame_relay_link*	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 timeshot assignment.	Verify that the network LMI is up. If it is, contact your network service provider.
Yellow Alarm at Network 1	A yellow alarm signal is being received on the specified interface. The DTE has detected an LOS or OOF condition.	For the network interface: 1. Verify that the cable is securely attached at the Network interface. 2. Contact your network provider.
Yellow Alarm at DSX-1		For the DSX-1 interface: 1. Check that the DSX-1 cable is securely attached at both ends. 2. Check the status of the attached equipment.

Troubleshooting Tables

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

Device Problems

Table 11-2. 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 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 11-4). ■ Contact your service representative.

Table 11-2. Device Problems (2 of 2)

Symptom	Possible Cause	Solutions
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.
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. 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 11-3. 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 or network. 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 Test menu allows you to run loopbacks and test patterns on the FrameSaver unit, and to test the front panel LEDs. It is available to users with a security access level of 1 or 2.

Select . . .	To run the following tests . . .	See . . .
PVC Tests [1]		
Network PVC Tests	■ PVC Loopback ■ Send Pattern ■ Monitor Pattern ■ Connectivity	page 11-17 page 11-18 page 11-18 page 11-19
Data Port PVC Tests		
Physical Tests		
Network Physical Tests	■ Line Loopback ■ Payload Loopback ■ Repeater Loopback ■ Send Line Loopback ■ Send Pattern ■ Monitor Pattern	page 11-19 page 11-20 page 11-21 page 11-22 page 11-18 page 11-18
Data Port Physical Tests	■ DTE Loopback	page 11-24
DSX-1 Physical Tests	■ Line Loopback ■ Payload Loopback ■ Repeater Loopback ■ Send Pattern ■ Monitor Pattern	page 11-19 page 11-20 page 11-21 page 11-18 page 11-18
Other Tests		
IP Ping	IP PING	page 11-25
Lamp Test	LEDs test	page 11-27

[1] Menu selections for PVC Tests are suppressed when no PVCs have been defined for the interface.

Test Timeout

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

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

To use this feature, enable the Test Timeout configuration option, and set a duration for the test to run in the Test Duration (min) configuration option (see *Configuring General System Options* in Chapter 8, *Configuration Options*).

NOTE:

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

Changing the Test Timeout from OpenLane Diagnostic Wizard

The system default for tests is the system's Test Timeout setting, but it can be overridden from Diagnostic Wizard. You can override the test duration for all tests or for a single test.

Prior to running tests from Diagnostic Wizard, the test duration can be set from the Customize drop-down menu.

▶ Procedure

To override the timeout duration for all tests, change the Test Timeout Value prior to running any tests.

Navigation Wizard → Tests button → Customize drop-down menu →
Test Timeout Value

Values range from one minute to 15 hours; the default setting is 10-minutes.

▶ Procedure

To override the timeout duration for one test:

1. Select a DLCI from Navigation Wizard, and the Tests button.
2. Position the cursor over the Connectivity button in the test path, and click the right mouse button. A pop-up menu appears.
3. Select Test Timeout Value, then set the test duration.
4. Run the test.

   When the test is concluded, the Test Timeout Value reverts to the system default.

Starting and Stopping a Test

Use this procedure to start, monitor, or abort specific tests. To abort all active tests on all interfaces, see *Aborting All Tests* on page 11-16.

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

Start or stop an individual test using the same procedure.

▶ Procedure

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

1. Follow this menu selection sequence:

   Main Menu → Test

2. Select an interface to be tested (Network, Data Port, or ISDN PVC Tests, or Network, Data Port, DSX-1, or PRI Physical Tests) and press Return.

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

3. Select the Port number and press Return.

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

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

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

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

6. Press Enter to stop the test.

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

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

Aborting All Tests

Use the Abort All Tests selection from the Test menu to abort all tests running on all interfaces, with exception to DTE-initiated loopbacks. To abort individual tests that are active, see *Starting and Stopping a Test* on page 11-15.

▶ **Procedure**

To abort all tests on all interfaces:

1. Follow this menu selection sequence:

   Main Menu → Test

2. Select Abort All Tests and press Enter.

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

   NOTE:

   Abort All Tests does not interrupt DTE-initiated loopbacks.

Determining Test Status and Results

Current test status and results are available on the:

- Test screen from which you execute the test (Results column)
- System and Test Status screen
- NMS
- Test LED

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 units, 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 unit, PVC tests are on a standard DLCI and are disruptive to data.

Loopback, and send/monitor pattern tests are available for each interface on the selected DLCI. Units 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.

NOTE:

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

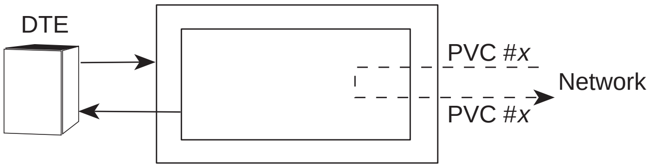
PVC Loopback

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

Main Menu → Test → [Network PVC Tests/Port-1 PVC Tests] → PVC Loopback

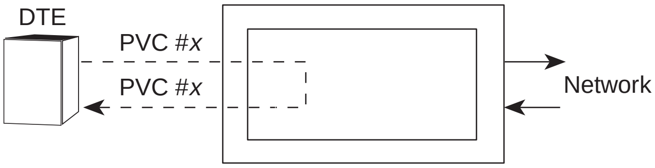
If the selected DLCI is . . .	Then the PVC Loopback is . . .
Standard	Disruptive to data.
Proprietary, multiplexed	Nondisruptive to data.

Network PVC Loopback



98-16186

Port PVC Loopback



98-16187

Send Pattern

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

Main Menu → Test → [Network PVC Tests/Port-1 PVC Tests] → Send Pattern

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

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

Monitor Pattern

This test monitors packets for the 55 test pattern and checks sequence numbers using a proprietary method.

Main Menu → Test → [Network PVC Tests/Port-1 PVC Tests] → Monitor Pattern

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

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

Connectivity

The Connectivity test is only available for multiplexed DLCIs.

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

Main Menu → Test → [Network PVC Tests/Port-1 PVC Tests] → Connectivity

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 can be commanded for any of the following interfaces:

- Network
- DSX-1
- Port 1

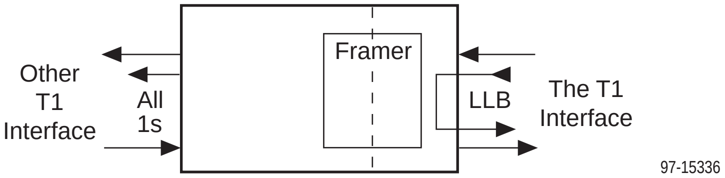
Physical tests require the participation of your network service provider.

CAUTION:

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

Line Loopback

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



CAUTION:

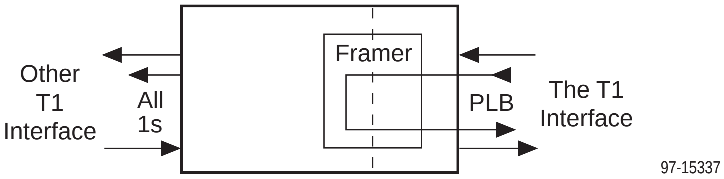
Line Loopback may affect the operation of the frame relay PVCs assigned to the selected port. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

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

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

Payload Loopback

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



CAUTION:

Payload Loopback may affect the operation of the 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.

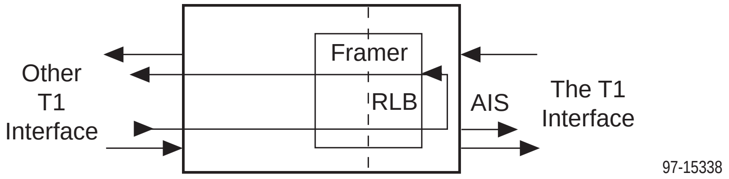
A PLB cannot be started when one of the following tests is active:

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

Repeater Loopback

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

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.

CAUTION:

Repeater Loopback may affect the operation of the 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 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) and assigned to 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.

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

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

▶ Procedure

To start and stop a Remote Line Loopback:

1. Follow this menu selection sequence:

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

2. Select the desired Network interface (shown in the screen title).
3. Select the code Up or Down in the Send Line Loopback field.
   - Up – Puts a remote device in loopback.
   - Down – Takes the remote device out of loopback.
4. Highlight Send and press Enter to start the test. The code is sent for 10 seconds.
5. View the length of time that the test has been running in the Result column.

Send and Monitor Pattern Tests

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

The following test patterns are available:

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

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

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

▶ Procedure

To send and monitor a Pattern Test:

1. Follow this menu selection sequence to display the Tests screen:

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

2. Select the desired pattern in the Send or Monitor field. If sending/monitoring a user-defined pattern, enter the the desired 2-byte hexadecimal value in the field next to Send or Monitor.

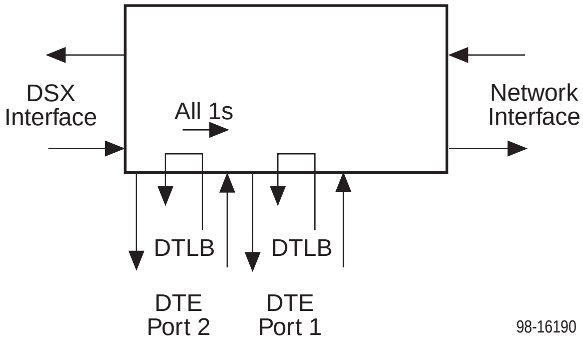
   When sending a pattern, the Inject ERR function key appears. Use Inject ERR if you want to inject a bit error in the transmitted bit pattern.

3. Highlight the Send command to send a pattern, or the Start command to monitor a pattern, and press Enter to start the test or start monitoring it.
4. View the length of time that the test has been running in the Results column. An error count is also displayed. When monitoring a pattern, the ResetMon virtual function key appears. ResetMon resets the error count to zero.
5. Highlight Stop and press Enter to stop the test.
6. View the length of time that the test has been running in the Result column.

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.

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



CAUTION:

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

IP Ping Test

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

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 on page 11-26 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 on page 11-26 to Ping the SNMP trap managers.

▶ Procedure 1

To Ping any far-end FrameSaver unit:

1. Select the IP Ping test.

   Main Menu → Test → IP Ping

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

   NOTE:

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

3. Verify the results of the IP Ping test.

   — While the test is running, **`In Progress...`** is displayed 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...`** is displayed 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.

If the Test Timeout configuration option is enabled and a Test Duration is set, the Lamp Test stops when the test duration expires.

See *Configuring General System Options* in Chapter 8, *Configuration Options*, to configure the unit to stop the test automatically.

If verifying LEDs remotely, Telnet into the unit's menu-driven user interface and view the Display LEDs and Control Leads screen.

Main Menu → Status → Display LEDs and Control Leads

▶ Procedure

To perform a Lamp Test from DCE Manager, take the folllowing path:

DCE Manager → Device Display → Diagnosis menu → Lamp Test Start

The LEDs on the unit start blinking. Once the device is located and the LEDs verified, select *Lamp Test Stop*. The unit LEDs return to normal operation.

▶ Procedure

To perform a Lamp Test from Performance Wizard:

1. Click on the Tests button from Navigation Wizard.
2. Highlight the unit to be tested.
3. Click on the Device Tests menu and select Start Lamp Test.
4. To stop the test, select Stop Lamp Test from the Device Tests menu.

LMI Packet Utility

A packet capture utility is provided to aid with problem isolation when LMI errors are detected. Using this utility, any enabled frame relay link that is having problems 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.

▶ Procedure

To use the utility:

1. Select an enabled frame relay link.
2. 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. If the utility is left to overrun the buffer, only the most current 8000 packets are retained.
3. To stop the utility, press Return. The field toggles back to Start.
4. Upload the data file holding the collected packets to a diskette so the information can be transferred to a Network General Sniffer for debugging/decoding.

   See *FTP File Transfers* in Chapter 10, *Operation and Maintenance*, to learn how to transfer a data file.

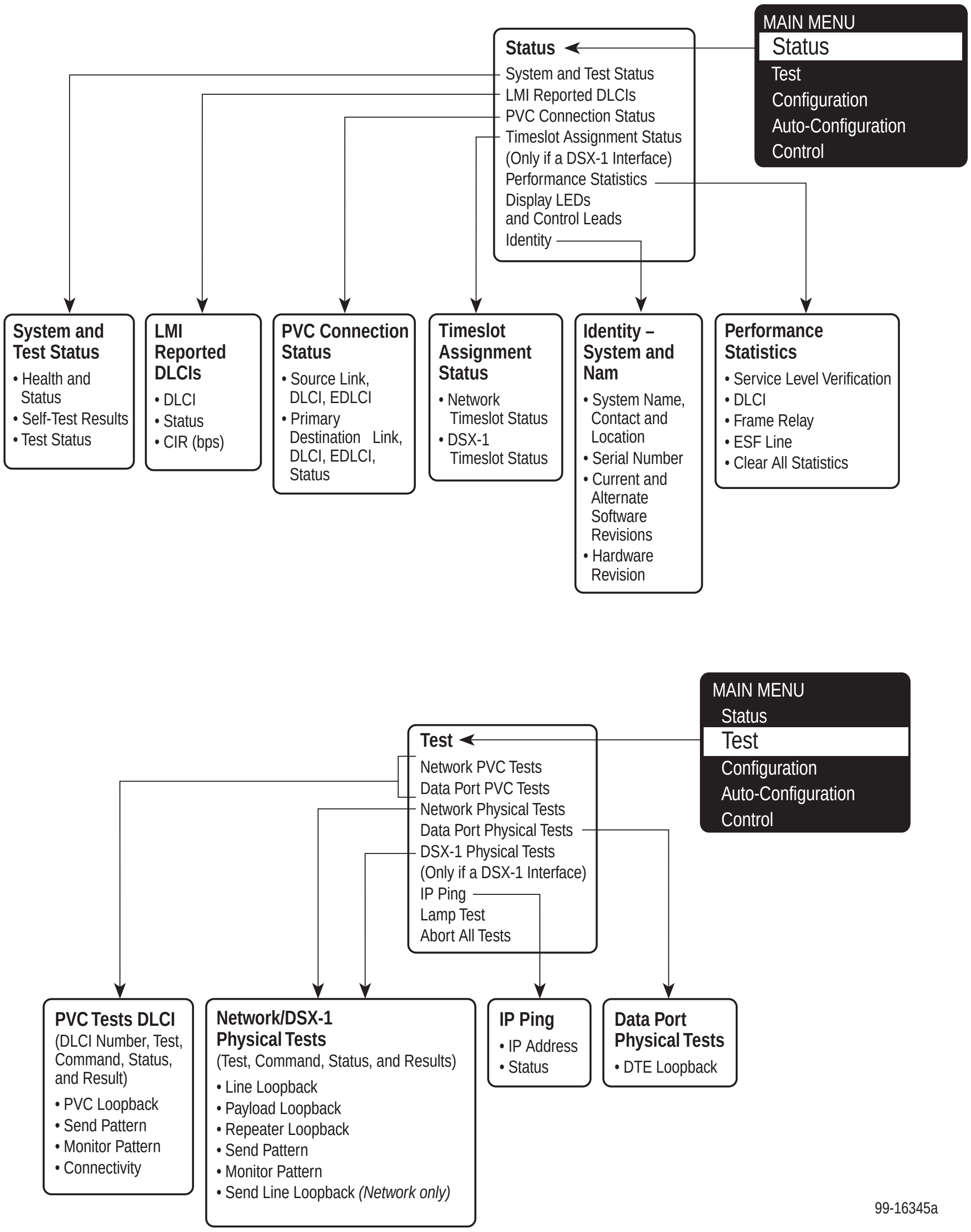
Menu Hierarchy

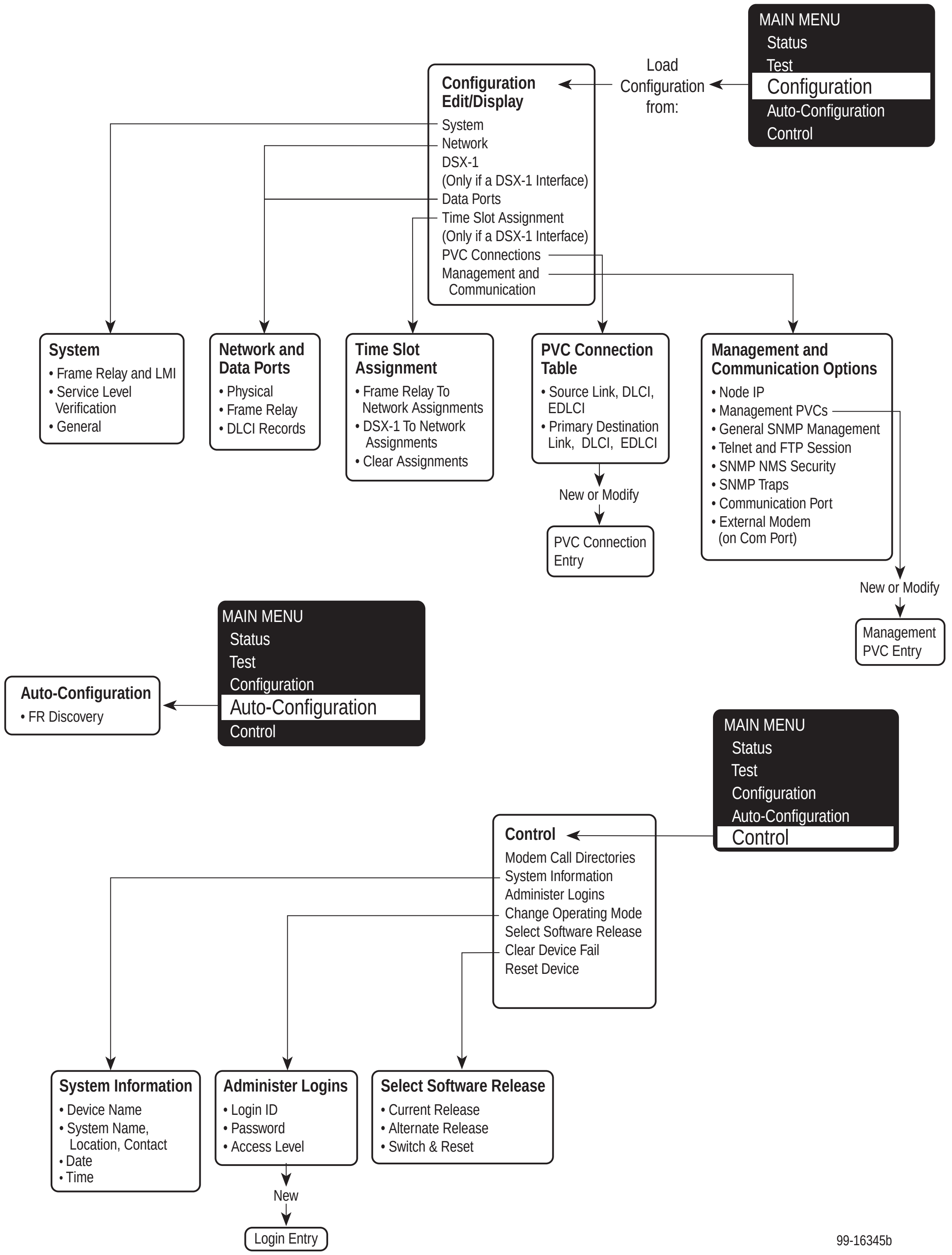
A

Menus

The following is a graphical representation of the 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
(Only if a DSX-1 Interface)
Data Ports
Time Slot Assignment
(Only if a DSX-1 Interface)
PVC Connections
Management and Communication
System
• Frame Relay and LMI
• Service Level Verification
• General
Network and Data Ports
• Physical
• Frame Relay
• DLCI Records
Time Slot Assignment
• Frame Relay To Network Assignments
• DSX-1 To Network Assignments
• Clear Assignments
PVC Connection Table
• Source Link, DLCI, EDLCI
• Primary 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
• External Modem (on Com Port)
New or Modify
Management PVC Entry
MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Auto-Configuration
• FR Discovery
MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Control
Modem Call Directories
System Information
Administer Logins
Change Operating Mode
Select Software Release
Clear Device Fail
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
99-16345b

IP Addressing

B

Selecting an IP Addressing Scheme

You can select from many IP addressing schemes to provide SNMP NMS connectivity. When selecting a scheme, keep the following in mind:

- Because connection to remote devices is through PVCs, if desired, you can assign IP addresses and subnet masks to each PVC individually.
- Assign IP addresses on a per-interface or FrameSaver unit basis.
- Although routing information is automatically passed between interconnected FrameSaver units from the network side, make sure to set a route to the subnet(s) in the NMS's or local router's routing table.

  The gateway to subnet(s) is through the FrameSaver unit connected to:

  — A router's, terminal server's, or NMS's direct PPP (point-to-point protocol) or SLIP's (link-layer protocol for IP traffic) serial connection, or

  — The router's DTE port using a local PVC, or

  — The LAN (using a LAN adapter).
- Be aware that each FrameSaver unit's routing table supports a maximum of 300 routes, even though a single route is all that is needed to reach every device on a subnet.
- Have a default route set only for devices directly connected to the NMS's COM port.
- Allow any legal host address for a given subnet; the address choice within the subnet is not important to the unit, but it should be selected in conjunction with all IP addressing for the subnet.

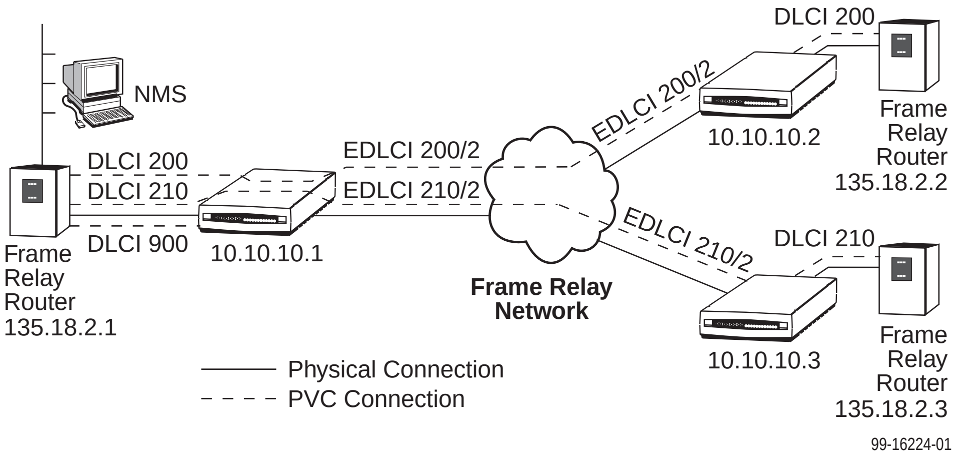
NOTE:

When dealing with IP addressing, your Information Systems (IS) department needs to be involved since they typically dictate the IP addressing scheme used in an organization.

Mixing Private and Public Addressing on the Same Network

When customers are connected to the internet, IP addresses are limited to the number of IP addresses they own. Using FrameSaver units, private addressing can be used for your network without taking away from the customer's pool of IP addresses.

The illustration below shows this scheme of public and private IP addressing, which is like having two networks in one.



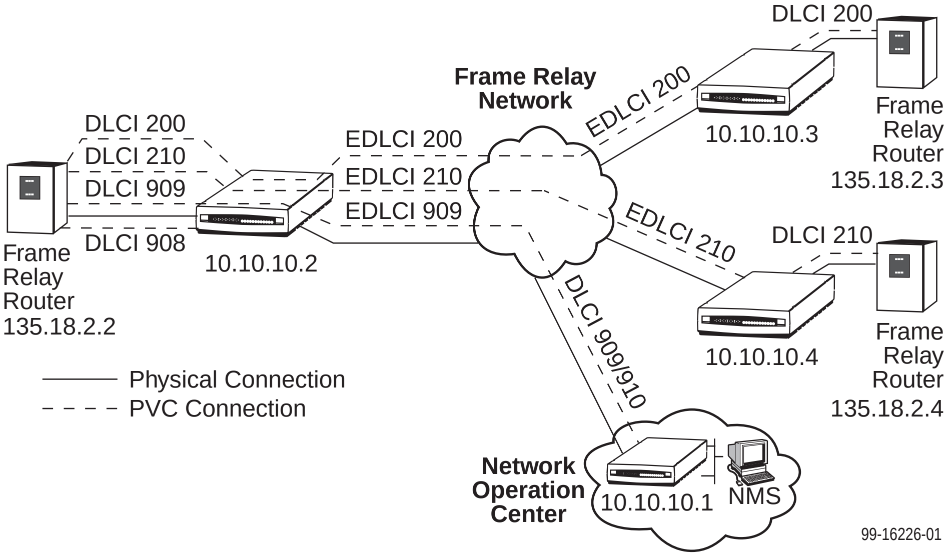
Both networks share the near-to-far end customer-ordered DLCIs (200 and 210) so that user data and management data use EDLCIs (multiplexed DLCIs, e.g., 200/2). Management of the far-end devices is performed via EDLCIs. FrameSaver EDLCIs enhance standard DLCIs, creating a communication path within a communication path.

Using the NextEDGE/FrameSaver RIP feature, far end NextEDGE/FrameSaver devices can be identified automatically and reported to the management station via DLCI 900. DLCI 900 is not propagated to the network by the router. The DLCI terminates in the NextEDGE system and is only used for management.

Preferred Method

Instead of having one PVC for the router (DLCI 909) and another for the FrameSaver unit (DLCI 910), management of the network can be accomplished using only the router PVC when the NOC uses a FrameSaver unit, which has its own IP address, as seen in the illustration below.

Simply create a PVC between the NOC and the router, then let the FrameSaver unit automatically discover the DLCI and convert it to an EDLCI via its Auto-Configuration feature (DLCI 909/2). This solution eliminates the need for two DLCIs per central-site FrameSaver unit-router set. The management PVC would be shared by both the FrameSaver unit and the router.



Whether automatically discovering or manually configuring DLCIs, a local management PVC must be created between each FrameSaver unit and its router if management through a back door is desired. Using private addresses, the router will not pass the DLCI to the network so the PVC is reserved for management only.

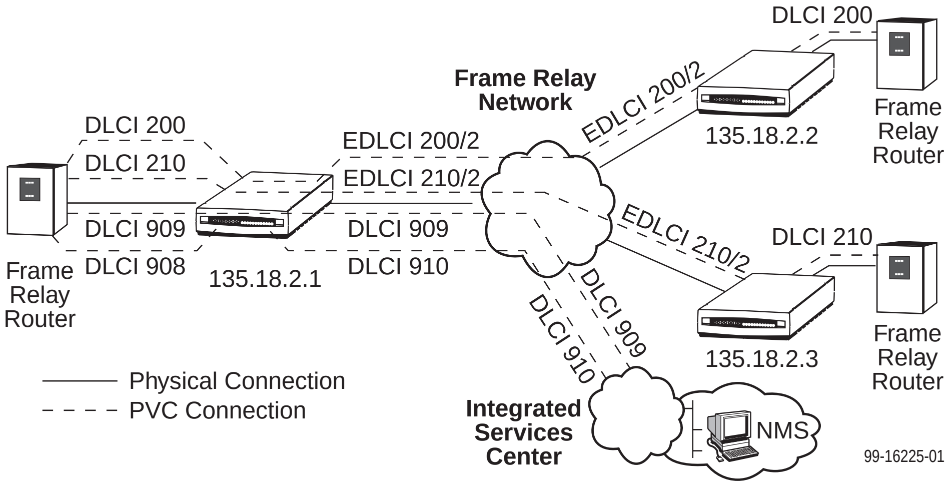
Management through a back door can be accomplished via a dial line to the router. Should the network fail, communication with both the router and the FrameSaver unit would be maintained.

In this case, one PVC is used for both unit and router management.

- DLCI 909 is used to manage the router.
- DLCI/EDLCI 909/2 is used to manage the unit.
- DLCI 908 is a static route from the router for back door managment of the unit.

Service Provider Example

Total management can be performed by service providers using both private and public IP addressing. A standard CSU/DSU can be used by the network operation center (NOC) NMS. This requires two dedicated DLCIs.



In this illustration, two dedicated PVCs are required.

- DLCI 909 is used to manage the router.
- DLCI 910 is used to manage the unit.

Using private addresses ensures that the router will not pass DLCI traffic to the network, so the PVC is reserved for management traffic only. Notice that the DLCI for the FrameSaver unit (910) terminates in the unit and is not passed to the router.

The only other requirement is that there is a separate DLCI for each remote FrameSaver unit.

IP Addressing Scheme Examples

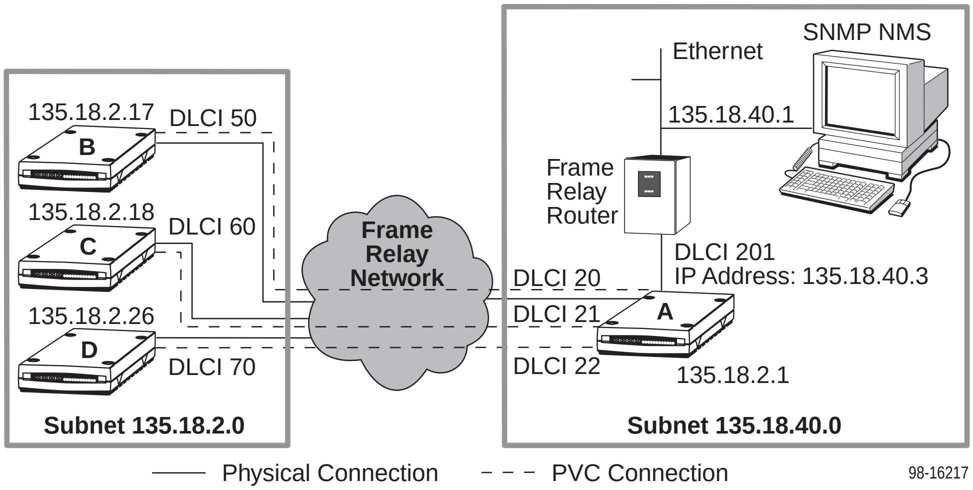
The following examples describe some typical network scenarios; they are not the only scenarios that can be used. The subnet mask shown for each FrameSaver unit is 255.255.255.0.

Direct PVCs to Remote FrameSaver Units

In this example, FrameSaver unit A is connected to:

- The NMS at the central site
- Each remote FrameSaver unit through a management PVC

The illustration below shows three separate management PVCs, one for each remote FrameSaver unit.

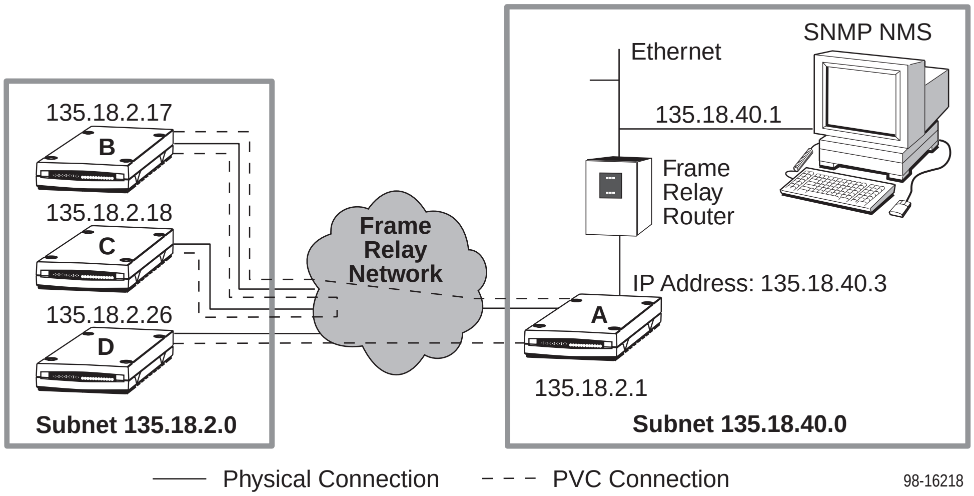


Routing to Remote FrameSaver Units on the Same Subnet

In this example, FrameSaver unit A is connected to:

- The NMS at the central site
- Remote FrameSaver units through management PVCs

The illustration below shows two management PVCs at the central site, with FrameSaver units B and C connected through one management PVC.



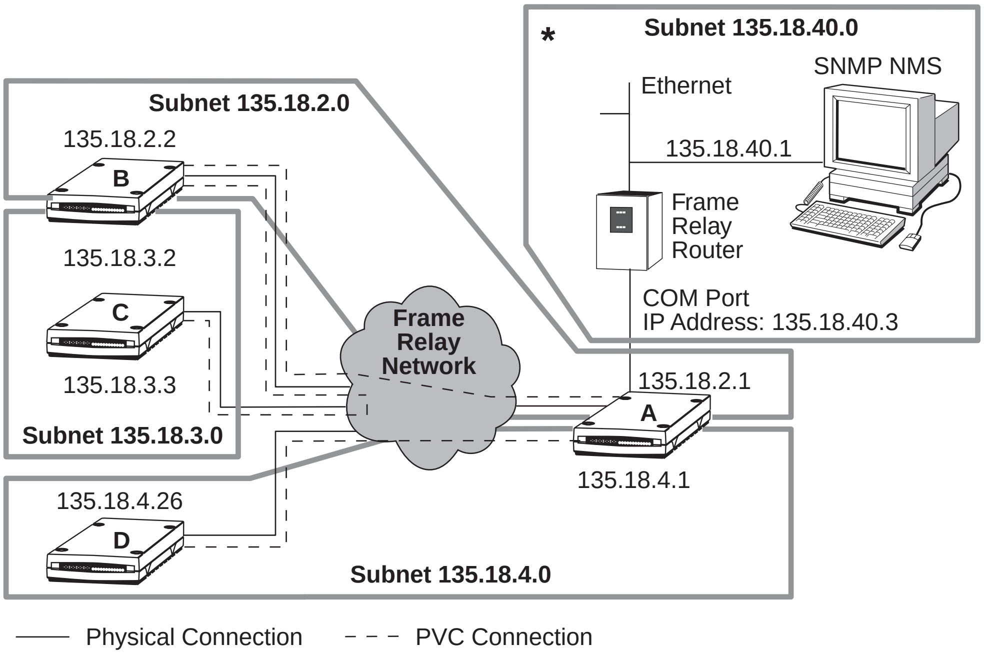
Routing to Remote FrameSaver Units Using Different Subnets

In this example, FrameSaver unit A is connected to:

- The NMS at the central site
- Two remote FrameSaver units through management PVCs

The illustration below shows two management PVCs, with FrameSaver units B and C connected through one management PVC. By configuring a different IP address and subnet for each management PVC:

- FrameSaver units B and C share a subnet: 135.18.3.0
- FrameSaver units A and B share a different subnet: 135.18.2.0
- FrameSaver units A and D share yet another subnet: 135.18.4.0



* This subnet connection can be to any of the following:
- Frame relay RFC 1490 IP router via the DTE Port
- Frame relay non-RFC router via AUX port-to-COM port
- SNMP NMS via the COM Port
- Terminal server via the COM Port
- LAN adapter via the COM Port

98-16219

Routing to Remote FrameSaver Units Using Routers

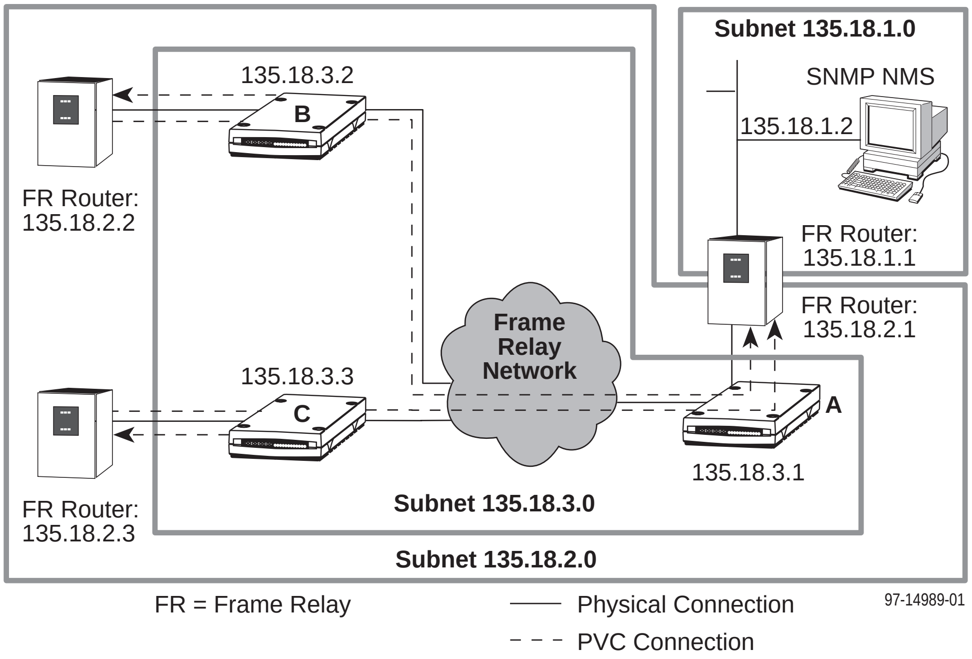
In the following examples, the FrameSaver unit at the central site is connected to:

- A router (instead of a LAN connection)
- The router is connected to the NMS
- The router's additional serial or AUX port connection is not used for management
- No additional network PVCs are required

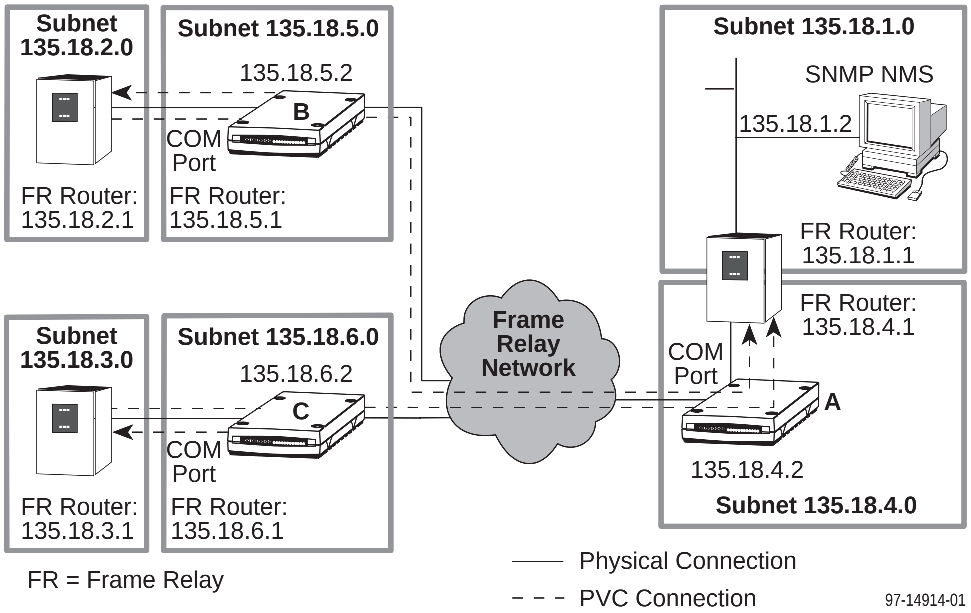
In the following examples, data is not routed by the FrameSaver units, and management PVCs are not configured between them. Instead, management data for the remote FrameSaver units is routed through the routers, with management PVCs configured between the routers and FrameSaver units. Connection is via the existing DTE cable, between the router's DTE interface and the T1 access unit.

In the following examples, data is not routed by the FrameSaver units, and management PVCs are not configured between them. Instead, management data for the remote FrameSaver units is routed through the routers, with management PVCs configured between the routers and FrameSaver units. Connection is via the existing DTE cable, between the router's DTE interface and the access unit.

The illustration below shows all FrameSaver units on the same subnet, and all routers on the same subnet.



The following illustration is a more complex example in which each FrameSaver unit is on its own subnet, having a subnet mask of FF.FF.FF.00 (255.255.255.0). This subnet is independent of the subnet on the LAN supported by the local router.



Assigning IP Addresses and Subnet Masks

Once you select an IP scheme, assign an address (or addresses) to the access unit.

- If one IP address is wanted for the FrameSaver unit, set node IP address and subnet mask.
- If an IP address is wanted for each interface, assign a separate IP address and subnet mask to each interface.

If using . . .	**Then . . .**
COM port as a management interface	Assign the node IP address and subnet mask or the COM port IP address and subnet mask. Menu selection sequence: *Main Menu→ Configuration→ Management and Communication→ Communication Protocol*
COM port connected to an external modem	Configure an IP address and subnet mask to dial out traps using the alarm directory. Menu selection sequence: *Main Menu→ Configuration→ Alarm* Or, configure the IP address and subnet mask. Menu selection sequence: *Main Menu→ Configuration→ Management and Communication→ Communication Protocol*
Management PVC as a management interface	Assign IP addresses and subnet masks to each PVC, or to the node IP address if only one IP address per unit is desired. Menu selection sequence: *Main Menu→ Configuration→ Management and Communication→ Management PVCs*

SNMP MIBs and Traps, and RMON Alarm Defaults

C

This appendix includes the following sections:

MIB Support

The NextEDGE 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.

Standards Compliance for SNMP Traps

NextEDGE units, with their special operational trap features, comply with SNMP format standards.

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 NextEDGE unit supports the following traps:

- warmStart on page C-3.
- authenticationFailure on page C-4.
- linkUp and linkDown on page C-4.
- enterprise-Specific on page C-7.
- RMON-Specific on page C-13.

These traps are listed in alphabetical order within each table.

Trap: warmStart

This trap indicates that the NextEDGE unit has been reset as a result of a reset command or a power disruption.

Table C-1. warmStart Trap

Trap	What It Indicates	Possible Cause
warmStart	NextEDGE unit has just reinitialized and stabilized itself.	■ Reset command sent. ■ Power disruption. *String:* ‘Unit reset.’
	Variable-Bindings	
	devLastTrapString (devHealthAndStatus. mib)	

Trap: authenticationFailure

Table C-2. authenticationFailure Trap

<table>
<tr><th>Trap</th><th>What It Indicates</th><th>Possible Cause</th></tr>
<tr><td rowspan="3">authenticationFailure</td><td>Access to the NextEDGE unit was attempted and failed.</td><td rowspan="3">■ 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.
<i>String:</i>
‘Unauthorized access attempted.’</td></tr>
<tr><td><b>Variable-Bindings</b></td></tr>
<tr><td>devLastTrapString (devHealthAndStatus. mib)</td></tr>
</table>

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 C-3. 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 C-4. linkUp and linkDown Variable-Bindings (1 of 2)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer – Represented by the entry in the MIB II Interfaces Table.		
Network, DSX-1 (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 C-4. linkUp and linkDown Variable-Bindings (2 of 2)

Interface	Variable-Bindings	Possible Cause
Logical Link Sublayer – Represented by the entry in the MIB II Interfaces Table.		
Synchronous Data Port Service Side of the Frame Relay UNI (Supported by the media-specific Frame Relay Services MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured,[3] or Frame Relay link is disabled. '$ifString LMI down.' No alarms exist on the link. (E.g., 'Frame Relay link "Chicago" on T1 Network LMI down.') '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$ifString up.'
Network DTE Side of the Frame Relay UNI (Supported by the media-specific Frame Relay DTE's MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured,[3] or Frame Relay link is disabled. *Strings:* '$ifString LMI down.' '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$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 C-5. enterprise-Specific Traps (1 of 2)

Trap	What It Indicates	Possible Cause
enterpriseCIR-Change(115)	CIR has changed due to the LMI report.	LMI Protocol is set to Standard and the network's CIR changed.
enterpriseConfig-Change(6)	Configuration has been changed via the async user interface or an SNMP Manager after 60 seconds has elapsed without another change.	Configuration has been changed via the async user interface or an SNMP Manager from devLastTrapString (devHealthAndStatus.mib).
enterpriseDevice-Fail(3)	An internal device failure. The variable binding for this trap is devHealthandStatus.	Operating software has detected an internal device failure.
enterpriseDLCI-Down(11)	The DLCI for an interface supporting one side of the UNI is down.	DLCI is down.
enterpriseDLCIUp(12)	The DLCI for an interface supporting one side of the UNI is up.	DLCI is up again.
enterprisePrimary-ClockFail(1)	A failure of the device's currently configured primary clock source.	Operating software has detected that the primary clock source has failed.
enterprisePrimary-ClockFailClear(101)	The failure of the device's currently configured primary clock source has cleared.	Operating software has detected that the primary clock source is now operational again.
enterpriseRMON-ResetToDefault(13)	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.
enterpriseSecondary-ClockFail(4)	A failure of the device's currently configured secondary clock source.	Operating software has detected that the secondary clock source has failed.
enterpriseSecondary-ClockFailClear(104)	The failure of the device's currently configured secondary clock source has cleared.	Operating software has detected that the secondary clock source is operational again.

Table C-5. enterprise-Specific Traps (2 of 2)

Trap	What It Indicates	Possible Cause
enterpriseSelfTest-Fail(2)	A hardware failure.	Unit has completed (re)initialization and a hardware failure was detected.
enterpriseTest-Start(5)	A test is running.	At least one test has been started on an interface or virtual circuit.
enterpriseTest-Stop(105)	All tests have been halted.	All tests have been halted on an interface or virtual circuit.

The following variable-bindings support the enterprise-Specific traps and conditions for each interface.

Table C-6. enterprise-Specific Variable-Bindings (1 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseCIR-Change(115)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciCIR (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib)	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 async user interface or an SNMP Manager from devLastTrapString (devHealthAndStatus.mib). *String:* 'Device configuration change.'
enterpriseDevice-Fail(3)	■ devLastTrapString (devHealthAndStatus.-mib is the internal failure number.)	An internal device failure was detected. *String:* 'Device fail with error code *xxxxxxxx*.'

Table C-6. enterprise-Specific Variable-Bindings (2 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseDLCIDown(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.
enterprisePrimaryClockFail(1)	■ devLastTrapString (devHealthAndStatus.mib)	Operating software has detected that the primary clock source has failed. *String:* ‘Primary clock failed.’
enterprisePrimaryClockFailClear(101)		Operating software has detected that the primary clock source is now operational again. *String:* ‘Primary clock restored.’
enterpriseRMONResetToDefault(13)	■ devLastTrapString (devHealthAndStatus.mib)	Default Factory Configuration settings have been reloaded, returning RMON-related options to their original settings. *String:* ‘RMON database reset to defaults.’
enterpriseSecondaryClockFail(4)	■ devLastTrapString (devHealthAndStatus.mib)	Operating software has detected that the secondary clock source has failed. *String:* ‘Secondary clock failed.’
enterpriseSecondaryClockFailClear(104)		Operating software has detected that the secondary clock source is operational again. *String:* ‘Secondary clock restored.’

Table C-6. enterprise-Specific Variable-Bindings (3 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseSelfTest-Fail(2)	■ devLastTrapString (devHealthAndStatus.-mib)	Unit has completed (re)initialization and a hardware failure was detected. *String:* ‘Selftest failed: $*s*.’ ($*s* is the contents of devSelfTestResult.)
enterpriseTest-Start(5)	For physical interfaces and frame relay links: ■ ifIndex (RFC 1573) ■ .0.0 (placeholder) ■ devLastTrapString (devHealthAndStatus.-mib For virtual circuits (DLCIs): ■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib	At least one test has been started on an interface or virtual circuit. *String:* ‘$testString test started on$ifString.’ (E.g., ‘DTE External Loopback test started on Sync Data Port S01P1.’)
enterpriseTest-Stop(105)		All tests have been halted on an interface or virtual circuit. *String:* ‘$testString test started on$ifString.’ (E.g., ‘DTE External Loopback test stopped on Sync Data Port S01P1.’)

Variable-Bindings: enterpriseTestStart/Stop

Tests that affect the enterpriseTestStart and enterpriseTestStop traps and variable-bindings are different for each interface.

Interface	Variable-Bindings	Possible Cause
Physical Sublayer		
T1 Network	■ ifLink (RFC 1513) ■ .0.0 (placeholder) ■ devLastTrapString (devHealthAndStatus.-mib	■ enterpriseTest Start – The following tests are active on the interface: – DSU Loopback – CSU Loopback – Send 511 pattern – Monitor 511 pattern ■ enterpriseTest Stop – No longer any tests running on the interface. ■ linkDown – One or more alarm conditions are active on the port.
Virtual Circuits (DLCIs)		
Synchronous Data Port Service Side of the Frame Relay Link	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib	■ enterpriseTest Start – A test is active on the interface. *String:* '$testString test $started on $ifString.' ■ enterpriseTest Stop – No longer any tests running on the interface. *String:* '$testString test $stopped on $ifString.'
Network DTE Side of the Frame Relay Link		

Interface	Variable-Bindings	Possible Cause
Synchronous Data Port Service Side of the Frame Relay Link	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ frPVCEndptDLCIIndex (RFC 1604) ■ frPVCEndptRcvdSig Status (RFC 1604)	■ enterpriseDLCIDown trap is issued when DLCI Status is set to Inactive. ■ enterpriseDLCIUp trap is issued when DLCI Status is set to active.
T1 Network DTE Side of the Frame Relay Link	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ frCircuitDlci (RFC 2115) ■ frCircuitState (RFC 2115) ■ frPVCEndptDLCIIndex (RFC 1604) ■ frPVCEndptRcvdSig Status (RFC 1604)	■ enterpriseDLCIDown trap is issued when DLCI Status is set to Inactive. ■ enterpriseDLCIUp trap is issued when DLCI Status is set to active.

Traps: RMON-Specific

Two traps are defined to support the Alarm and Events Groups of RMON, which are shown below with their variable-bindings.

See *RMON Alarm Defaults* on page C-14 for the default values that will generate RMON-specific traps.

Variable-Bindings: risingAlarm and fallingAlarm

Table C-7. 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 NextEDGE 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 NextEDGE 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 NextEDGE unit, shows the alarm and event types, the interval used when generating alarms, and thresholds.

- *Physical Interface Alarm Defaults* on page C-15.
- *Static Frame Relay Interface Alarm Defaults* on page C-16.
- *Dynamic Frame Relay Interface Alarm Defaults* on page C-18.
- *DLCI Alarm Defaults – Paradyne Area* on page C-19.
- *Static DLCI Alarm Defaults – NetScout Area* on page C-20.
- *Dynamic DLCI Alarm Defaults – NetScout Area* on page C-21.

See *Standards Compliance for SNMP Traps* on page C-3 for information about how traps work, and *Traps: RMON-Specific* on page C-13 for traps specific to remote monitoring.

Rising Event Operation

If a rising threshold is crossed during the interval shown in a table (e.g., frames dropped by the network), the event is armed and an alarm is generated at the end of the interval. Only one alarm per event per interval is generated. The alarm condition persists until the event has been disarmed (reset).

The event is disarmed when a falling threshold has been crossed and the rising threshold has not been crossed during an interval, allowing the event to return to its original disarmed state.

Physical Interface Alarm Defaults

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

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 NextEDGE unit's frame relay interfaces. They are created during RMON initialization.

Table D-2. 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:* devfrext.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:* devfrext.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:* devfrext.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:* devfrext.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:* devfrext.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:* devfrext.mib (E) *Tag:* devFrExtLinkTotRxErrs *OID:* .1.3.6.1.4.1.1795.2.24.2. 6.9. 4.7.1.20.**I**	900 secs (15 mins)	Rising	1	1
Tx Total Errors	D	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkTotTxErrs *OID:* .1.3.6.1.4.1.1795.2.24.2. 6.9. 4.7.1.19.**I**	900 secs (15 mins)	Rising	1	1

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

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

Table D-2. 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
Rx Overruns	D	*MIB:* devfrext.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:* devfrext.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 Nonoctet Aligns	D	*MIB:* devfrext.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:* devfrext.mib (E) *Tag:* devFrExtLinkRxCrcErrs *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:* devfrext.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 NextEDGE unit's frame relay interfaces. They are created during RMON initialization, and will change if the interface's line speed changes.

Table D-3. 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 D-4. 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:* devfrext.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:* devfrext.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:* FT DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs *OID:* .1.3.6.1.2.1.10.32.2.1.5.**I.D**	60 secs (1 min)	Rising	1	1
Rx BECNs	D	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs *OID:* .1.3.6.1.2.1.10.32.2.1.4.**I.D**	60 secs (1 min)	Rising	1	1
Congested Seconds	D	*MIB:* devfrext.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:* devfrext.mib (E) *Tag:* frFrExtDlciNetDropFr *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.20.**I.D**	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.

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 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.

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. See *Editing Alarms* in Chapter 6, *Using NetScout Manager Plus*.

Table D-5. Static DLCI Alarm Defaults – NetScout Area

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Current Latency	A	*MIB:* devfrext.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)	Rising	Must be configured.	0
Average Latency	A	*MIB:* devfrext.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)	Rising	Must be configured.	0
Frames Received	D	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames *OID:* .1.3.6.1.2.1.10.32.2.1.8.**I.D**	60 secs (1 min)	Rising	Must be configured.	0
Frames Sent	D	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames *OID:* .1.3.6.1.2.1.10.32.2.1.6.**I.D**	60 secs (1 min)	Rising	Must be configured.	0
Tx Frames Exceeding CIR	D	*MIB:* devfrext.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)	Rising	Must be configured.	0
Tx CIR Utilization	D	*MIB:* FT 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	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 D-6. 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:* FT 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:* FT 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 (OID) Cross-Reference (Numeric Order)

The NextEDGE 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.

NetScout Manager Plus identifies these items by their OIDs in some of their reports, like User History. This cross-reference is to aid you in determining the condition being graphed.

Table C-7. Object ID Cross-Reference (1 of 3)

Object ID (OID)	Item	MIB/Tag
.1.1.3.6.1.4.1.1795.2.24.2.6.6.5.1.1.2.**I**	Unavailable Seconds	*MIB:* devSyncPortStats.mib (RFC 1406) *Tag:* devSyncPortStatsUASs
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.18.**I**	Invalid Frames	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkRxIlFrames
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.6.**I**	Short Frames	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkRxShort
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.7.**I**	Long Frames	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkRxLong
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.15.**I**	Rx Discards	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkRxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.14.**I**	Tx Discards	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkTxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.20.**I**	Rx Total Errors	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.19.**I**	Tx Total Errors	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.28.**I**	Rx Overruns	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkRxOverruns
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.29.**I**	Tx Underruns	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkTxUnderruns

Table C-7. Object ID Cross-Reference (2 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.16.**I**	Rx Nonoctet Aligns	*MIB:* devfrext.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:* devfrext.mib (E) *Tag:* devFrExtLinkRxCrcErrs
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.7.1.32.**I**	Total LMI Errors	*MIB:* devfrext.mib (E) *Tag:* devFrExtLinkTotalLMIErrs
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.2.1.2.**I** .**D**	DLCI Inactive Seconds	*MIB:* devfrext.mib (E) *Tag:* devFrExtDlciStsInactiveSecs
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.23.**I** .**D**	Missing Latency Responses	*MIB:* devfrext.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:* devfrext.mib (E) *Tag:* devFrExtDlciStsCongestedSecs
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.20.**I** .**D**	Frames Dropped by Network	*MIB:* devfrext.mib (E) *Tag:* frFrExtDlciNetDropFr
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.3.1.7.**I** .**D**	Current Latency	*MIB:* devfrext.mib (E) *Tag:* devFrExtLatencyLatest
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.3.1.5.**I** .**D**	Average Latency	*MIB:* devfrext.mib (E) *Tag:* devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9. 4.1.1.17.**I** .**D**	Tx Frames Exceeding CIR	*MIB:* devfrext.mib (E) *Tag:* devFrExtDlciTxFrOutCIR
.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
.1.3.6.1.2.1.10.32.2.1.8.**I** .**D**	Frames Received	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames

Table C-7. Object ID Cross-Reference (3 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.2.1.10.32.2.1.6.**I** .**D**	Frames Sent	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.7.**I** .**D**	Tx CIR Utilization	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.9.**I** .**D**	Rx DLCI Link Utilization	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets
.1.3.6.1.2.1.10.32.2.1.7.**I** .**D**	Tx DLCI Link Utilization	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.5.**I** .**D**	Rx FECNs	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.4.**I** .**D**	Rx BECNs	*MIB:* FT DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs

Cables, Connectors, and Pin Assignments

D

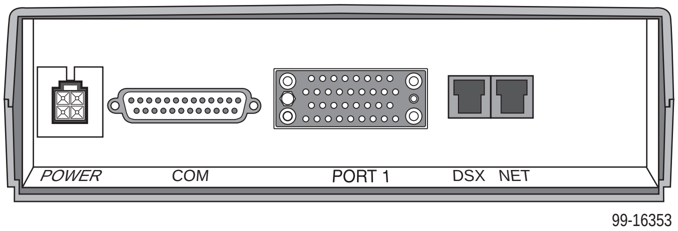
This appendix shows the FrameSaver unit rear panels, and pin assignments for the connectors/interfaces and cables. Native interfaces are used on the unit, so most cables do not have to be specially ordered; they can be purchased anywhere.

NOTE:

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

Rear Panels

The following illustration shows the FrameSaver 9124 rear panel.



The sections that follow provide pin assignments for each interface.

COM Port Connector

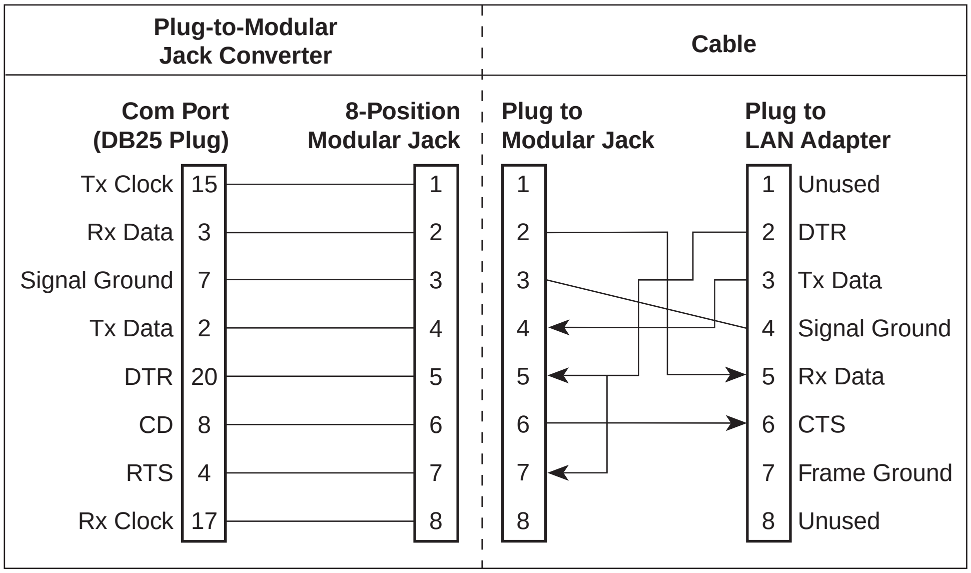
The following table provides the pin assignments for the FrameSaver 9124 unit's 25-position EIA-232C communication port connector.

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

LAN Adapter Converter and Cable

The following shows the pin assignments for the:

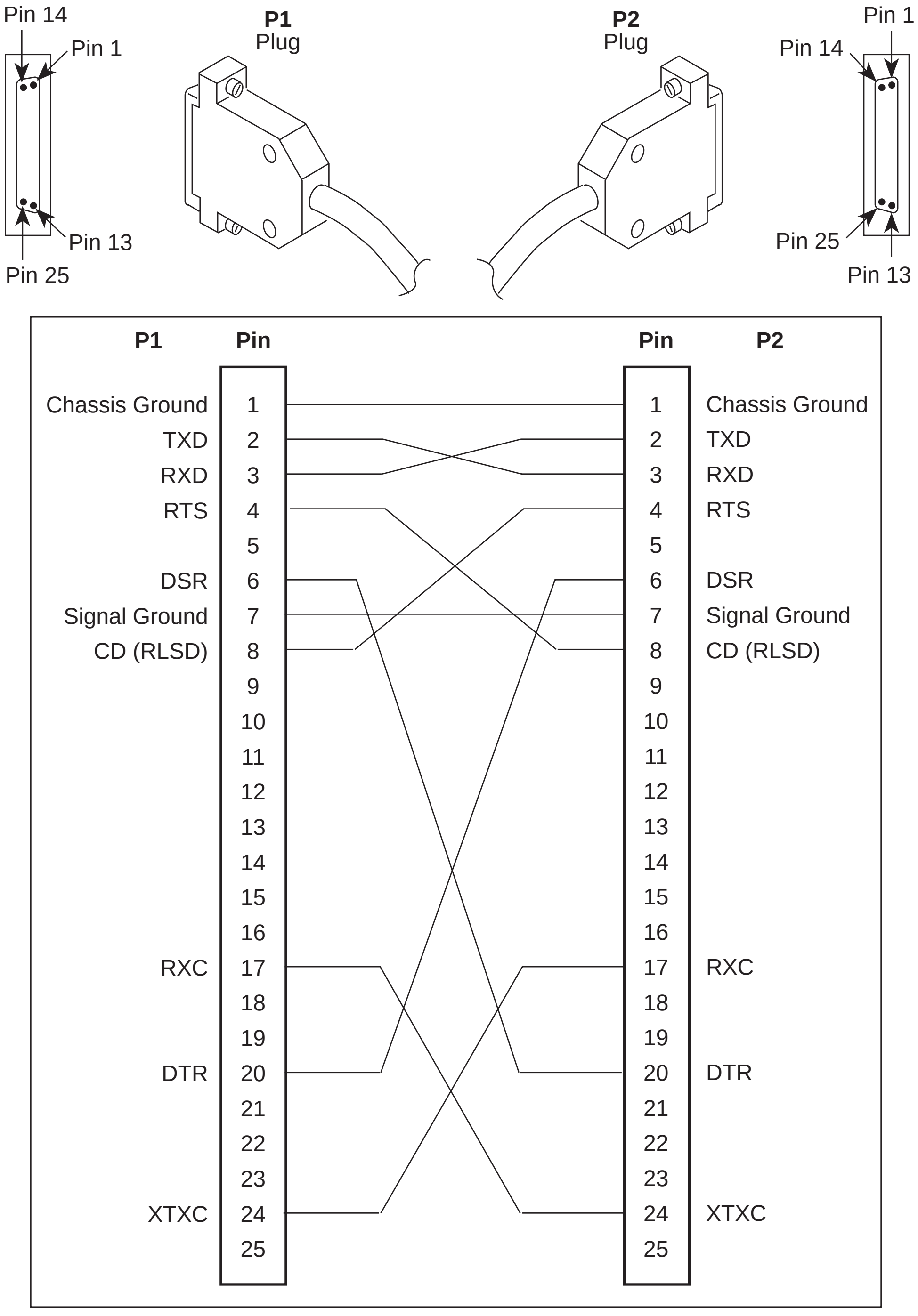
- DB25 plug-to-modular jack converter between the COM port and the 8-conductor LAN Adapter cable and
- Custom 8-conductor cable (with modular plugs on both ends) between the converter and the LAN Adapter (3100-F2-910).



98-16214

Standard EIA-232-D Crossover Cable

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



▶ Procedure

To configure an external modem:

1. Disconnect the asynchronous terminal from the standard cable. See page D-4 for an illustration of the COM Port connection.
2. Reconnect the crossover cable to the external modem.
3. Enable auto-answer on your modem, and configure it to use the following LSD, DSR, CTS, RTS, and DTR control leads.

   See the table below for AT D0 command strings. Use the following command string:

   ```
   AT &C0 &D2 &S0 &R1 \D0 S0=1
   ```

AT Command String	To configure the modem to . . .
&C0	Force LSD on.
&D2	Drop the connection when the unit drops DTR.
&S0	Force DSR on.
&R1	Ignore RTS.
\D0	Force CTS on.
S0=1	Automatically answer incoming calls.

Port 1 Connector

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

Signal	ITU CT#	Direction	34-Pin Socket
Shield	101	—	A
Signal Ground/Common	102	—	B
Request to Send (RTS)	105	To DSU (In)	C
Clear to Send (CTS)	106	From DSU (Out)	D
Data Set Ready (DSR)	107	From DSU (Out)	E
Receive Line Signal Detector (RLSD or LSD)	109	From DSU (Out)	F
Data Terminal Ready (DTR)	108/1, /2	To DSU (In)	H
Local Loopback (LL)	141	To DSU (In)	L
Transmit Data (TXD)	103	To DSU (In)	P (A) S (B)
Receive Data (RXD)	104	From DSU (Out)	R (A) T (B)
Transmit Signal Element Timing – DTE Source (XTXC or TT)	113	To DSU (In)	U (A) W (B)
Receive Signal Element Timing – DCE Source (RXC)	115	From DSU (Out)	V (A) X (B)
Transmit Signal Element Timing – DCE Source (TXC)	114	From DSU (Out)	Y (A) AA (B)
Test Mode Indicator (TM)	142	From DSU (Out)	NN

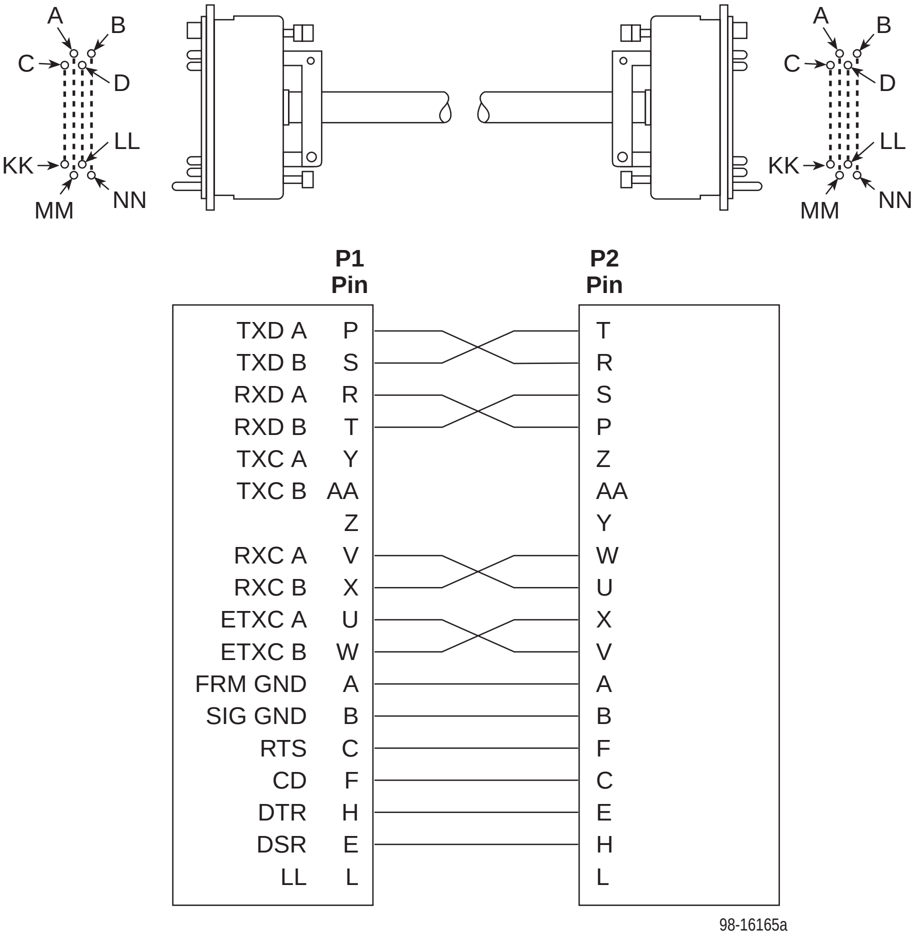
Standard V.35 Straight-through Cable

A standard V.35 straight-through cable can be used to connect a DTE port to a DTE, where a 34-pin plug-type connector is needed for the data port and a 34-position socket-type connector is needed for the DTE. No special-order cables are required.

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

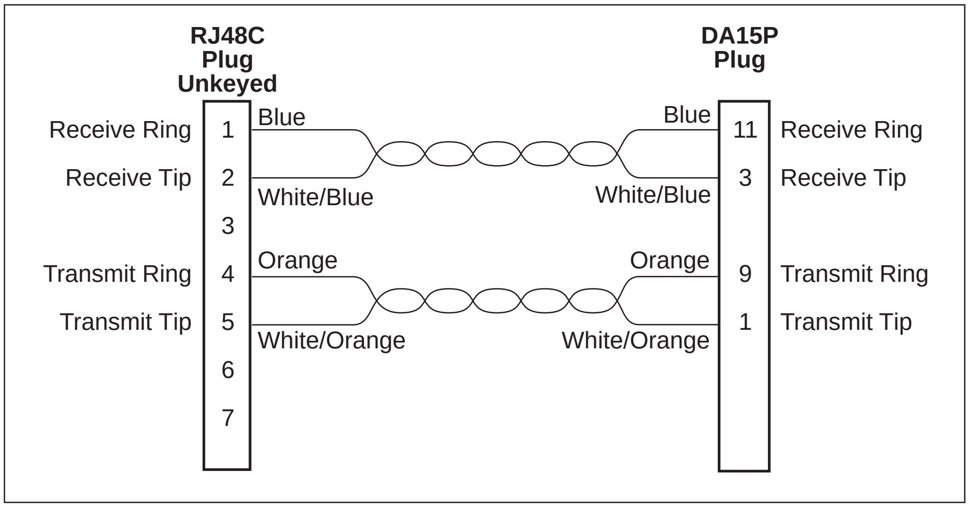
T1 Network Cable (3100-F1-500)

Network access is via a 20-foot cable with an RJ48C unkeyed plug-type connector on each end. The following table shows pin assignments and the purpose of each.

Function	Circuit	Direction	Pin Number
Receive Ring	R1	From Network	1
Receive Tip	T1	From Network	2
Transmit Ring	R	To Network	4
Transmit Tip	T	To Network	5

Canadian T1 Line Interface Cable (3100-F1-510)

The T1 line interface cable is used in Canada as an interface between the FrameSaver unit's network connector and the T1 network interface. The following shows pin assignments and the purpose of each.



98-16215

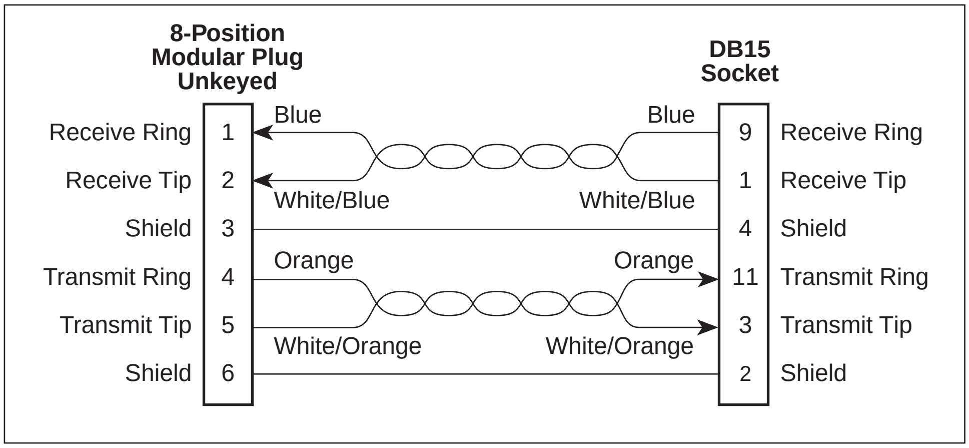
DSX-1 Connector

If your model includes a DSX-1 interface, the following table shows the signals and pin assignments for the 8-position modular DSX-1 interface. The DSX-1 Adapter is required for this interface (see page D-9).

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 (9008-F1-560)

The DSX-1 adapter cable is used as an interface between the unit's DSX-1 connector and the DTE's DB15 interface. The following shows pin assignments and the purpose of each.



99-16216a

Technical Specifications

E

Table E-1. 1-Slot FrameSaver Unit 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 85% (noncondensing)
Shock and vibration	Withstands normal shipping and handling
Physical Dimensions	
Height	2.9 inches (7.4 cm)
Width	8.5 inches (21.6 cm)
Depth	12.5 inches (31.8 cm)
Weight	2.59 lbs. (1.18 kg)
Power Consumption and Dissipation	7.9 watts, 60 Hz ± 3, 0.135 A at 120 Vac ± 123 Result: 27 Btu per hour

Table E-1. 1-Slot FrameSaver Unit Technical Specifications (2 of 2)

Specification	Criteria
COM Port	25-position (DB25) connector
Standard	EIA-232/ITU, V.24 (ISO 2110)
Data rates	9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 kbps
T1 Network Interface	8-position 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
DSX-1 Interface (if applicable)	
Physical interface	8-position modular connector with optional 8-position modular-to-DB15 adapter: D-Sub 15 socket
Framing format	D4, ESF
Coding format	AMI, B8ZS
DTE line equalization	5 selectable ranges from 0 to 655 feet (0 – 196.5 meters)
Send AIS	Selectable
Data Port	34-position V.35 connector
Standard	V.35/ITU (ISO 2593)
Data rates	Variations for T1 rates; automatically set to the network rate.

Equipment List

F

Equipment

See page F-2 for cables you can order.

Description	Model/Feature Number
FrameSaver SLV Units	
FrameSaver SLV 9124 T1 Remote Site with 64 PVCs (Includes 1-Slot Housing, 120 Vac Power Supply, Network Cable, and Documentation)	9124-A2-201
FrameSaver SLV 9124 T1 Central Site with 120 PVCs (Includes 1-Slot Housing, 120 Vac Power Supply, Network Cable, and Documentation)	9124-A2-204
Power Supplies	
100 – 240 Vac for 1-Slot Housing	9001-F1-040
120 Vac for 1-Slot Housing	9001-F1-020
NMS Products	
FrameSaver Management Package for Windows *Includes OpenLane DCE Manager 4.2, OpenLane Performance Wizard 4.2, and NetScout Manager Plus 5.5 for Windows.*	7700-P1-001
FrameSaver Management Package for Unix *Includes OpenLane DCE Manager 4.3, OpenLane Performance Wizard 4.3, and NetScout Manager Plus 5.5 for Unix.*	7800-P1-001
NetScout Server	
For Unix or Windows NT	9190
NetScout WebCast	
For Unix	9145
For Windows NT	9150

Description	Model/Feature Number
Optional Features	
Wall Mounting Kit for 1-Slot Housing	9001-F1-891
User Manual	
FrameSaver SLV 9124 User’s Guide (Paper Manual)	9124-M1-001

Cables

This table lists cables you can order.

Description	Part Number	Feature Number
RJ48C T1 Network Cable, RJ48C-to-RJ48C/RJ49C – 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
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
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
DSX-1 Adapter Cable, RJ48C-to-DB15 – 1 foot/0.3048 meters	035-0386-0031	9008-F1-560
Standard EIA-232-D Crossover Cable (connects COM Port to external device) DB25-to-RJ48 – 14 feet/4.3 meters	035-0336-1431	—

Index