OPENLANE™ DCE MANAGER

USER'S GUIDE

Document No. 7800-A2-GB26-80

May 1999

PARADYNE™

Notice

Warranty, Sales, Service, and Training Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Internet:** Visit the Paradyne World Wide Web site at **www.paradyne.com**. (Be sure to register your warranty 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

Printed on recycled paper

Contents

2 Using the DCE Manager

3 Administering Devices

4 Configuring Devices and Device Interfaces

5 Monitoring Devices

6 Performing Loopback Modes and Pattern Tests

A SNMP Management Connectivity

Glossary

Index

About This Guide

Document Purpose

The OpenLane™ Data Communications Equipment (DCE) Manager Release 4.3 is a collection of components that run as part of the Hewlett-Packard (HP) OpenView (herein referred to as OpenView) or NetView network management system. This guide describes how to install and use the OpenLane DCE Manager to administer, configure, monitor, and test the following devices:

- ACCULINK® 3100 and 3300 Series
- Hotwire™ 51xx , 52xx, and 54xx Remote Termination Units (RTUs)
- 71xx and 76xx Data Service Units (DSUs)
- Hotwire 7974, 7975, and 7976 Multirate Symmetric Digital Subscriber Line (M/SDSL) Standalone Units
- Hotwire 7984, 7985, and 7986 Multirate High-bit-rate Digital Subscriber Line (M/HDSL) Standalone Units
- Hotwire 8100 and 8200 Series (trap and icon support only)
- Hotwire 8310 and 8312 Multiple Virtual Lines (MVL™) Card
- Hotwire 8510, 8540, and 8546 Rate Adaptive Digital Subscriber Line (RADSL) Cards
- Hotwire 8600, 8610, 8800, and 8810 Digital Subscriber Line Access Multiplexers (DSLAM)
- Hotwire 8774, 8775, and 8776 Multirate Symmetric Digital Subscriber Line (M/SDSL) Cards
- Hotwire 8784 and 8786 Multirate High-bit-rate Digital Subscriber Line (M/HDSL) Standalone Units
- FrameSaver™ 9028 Frame Relay Compression Unit (FRCU)
- FrameSaver 9120 and 9620 Frame Relay Access Units (FRAU)
- FrameSaver Service Level Verifier (SLV) 9124, 9126, 9128, 9624, 9820, and 9820-C
- 9162, 9165, 9262, and 9265 T1 Access Multiplexer

- NextEDGE™ 9192 and 9195 Multiservices Access System
- FrameSaver SLV 9580 T3 ATM DSU
- ACCULINK Access Controller (AAC), Front Load and Full Expansion
- Digital Access and Cross-Connect System (DACS) Low-Speed Interface Unit (LSIU)

See Table 1-1, OpenLane DCE Manager Functions, for a complete list of supported devices.

Document Audience

The DCE Manager can be installed and used on Hewlett Packard (HP-UX), Sun (Solaris), and IBM (AIX) systems. This guide is intended for those persons who must administer, monitor, and perform tests on network devices and interfaces. It assumes that you are familiar with each of the following:

- Supported devices listed in Table 1-1, OpenLane DCE Manager Functions
- OpenView for HP-UX and Solaris systems or NetView for AIX systems
- System and network administration of your operating platform

Document Summary

Section	Description
Chapter 1	*Setting Up the DCE Manager.* Introduces the DCE Manager and provides you with the information you need to install the product software and integrate with OpenView or NetView.
Chapter 2	*Using the DCE Manager.* Describes how to access and display devices for use in DCE Manager operations.
Chapter 3	*Administering Devices.* Describes how to perform various administrative operations such as polling devices, managing and unmanaging devices, and resetting devices.
Chapter 4	*Configuring Devices and Device Interfaces*. Describes how to perform DCE Manager configuration operations, such as displaying and setting parameters and copying configuration images to another area in device memory or to a file.
Chapter 5	*Monitoring Devices*. Describes how to use the DCE Manager to evaluate the status of devices.

Section	Description
Chapter 6	*Performing Loopback Modes and Pattern Tests.* Describes how to set loopback modes and send pattern tests to check the integrity and performance of a device. Also describes how to use loopback modes and pattern tests to isolate a problem on a device or the line.
Appendix A	*SNMP Management Connectivity.* Gives examples of management connectivity, including device configuration.
Glossary	Defines acronyms and terms used in this document.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

Documentation Conventions

The DCE Manager can be installed on HP-UX, Solaris, or AIX systems, running either OpenView or NetView, depending on your operating platform. Chapter 1, *Setting Up the DCE Manager*, describes how to install the DCE Manager on each of these systems. Further chapters describe the use of the DCE Manager under HP OpenView only. Though the look and feel of the screens differ from running the DCE Manager with NetView for AIX, the functionality remains the same.

The following conventions are used in this document:

- An *italic typeface* separated by arrows (→) indicates a menu selection sequence, as in the following example:

  Administer→DCE Manager→Device Display

- A **`courier typeface`** indicates a file name, pathname, or command that you enter using the keyboard. It can also indicate a field name or value in a display.

- An italic typeface enclosed in bracket indicates variable information, such as <*model_number*>.

Product-Related Documents

Document Number	Document Title
582-510-100	*ACCULINK Access Controller Reference Guide*
3150-A2-GB21	*ACCULINK 315x CSU Operator's Guide*
3160-A2-GB21	*ACCULINK 3160, 3161, 3164, and 3165 DSU/CSU Operator's Guide*
3170-A2-GB20	*ACCULINK 3172 and 3174 DSU/CSU Operator's Guide*
3360-A2-GB20	*ACCULINK 3360, 3364, AND 3365 E1 NTU Operator's Guide*
5216-A2-GN10	*Hotwire 5216 Remote Termination Unit (RTU) Customer Premises Installation Instructions*
5246-A2-GN10	*Hotwire 5246 Remote Termination Unit (RTU) Customer Premises Installation Instructions*
5446-A2-GN10	*Hotwire 5446 Remote Termination Unit (RTU) Customer Premises Installation Instructions*
7110-A2-GB20	*Model 7110 T1 DSU/CSU User's Guide*
7112-A2-GB20	*Model 7112 T1 DSU/CSU, with Internal Ethernet LAN Adapter, User's Guide*
7610-A2-GB20	*Model 7610 SNMP DSU User's Guide*
7612-A2-GB20	*Model 7612 SNMP DSU, with Internal Ethernet LAN Adapter, User's Guide*
7974-A2-GB20	*Hotwire 7974 M/SDSL Standalone Termination Unit, with DSX-1 Interface, User's Guide*
7975-A2-GB20	*Hotwire 7975 M/SDSL Standalone Termination Unit User's Guide*
7976-A2-GB20	*Hotwire 7976 M/SDSL Standalone Termination Unit, with G.703 Interface, User's Guide*
7984-A2-GB20	*Hotwire 7984 M/HDSL Standalone Termination Unit, with DSX-1 Interface, User's Guide*
7985-A2-GB20	*Hotwire 7985 M/HDSL Standalone Termination Unit, with EIA-530A Interface, User's Guide*
7986-A2-GB20	*Hotwire 7986 M/HDSL Standalone Termination Unit, with G.703 Interface, User's Guide*
8000-A2-GB20	*Hotwire DSLAM for 8540 and 8546 DSL Cards User's Guide*
8000-A2-GB21	*Hotwire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide*
8000-A2-GB26	*Hotwire DSLAM for 8310/8312 MVL and 8510 RADSL Cards User's Guide*

Document Number	Document Title
8000-A2-GB27	*Hotwire DSLAM for 8310/8312 MVL and 8510 RADSL Cards Network Configuration Guide*
8000-A2-GB90	*Hotwire 8100/8200 Interworking Packet Concentrator (IPC) User's Guide* (Feature No. 8200-M2-901)
8000-A2-GN11	*Hotwire Management Communications Controller (MCC) Card Installation Instructions*
8600-A2-GN20	*Hotwire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8610-A2-GN10	*Hotwire 8610 DSLAM Installation Instructions*
8774-A2-GB20	*Hotwire 8774 M/SDSL Termination Unit, with DSX-1 Interface, User's Guide*
8775-A2-GB20	*Hotwire 8775 M/SDSL Termination Unit User's Guide*
8776-A2-GB20	*Hotwire 8776 M/SDSL Termination Unit, with G.703 Interface, User's Guide*
8784-A2-GB20	*Hotwire 8784 M/HDSL Termination Unit, with DSX-1 Interface, User's Guide*
8786-A2-GB20	*Hotwire 8786 M/HDSL Termination Unit, with G.703 Interface, User's Guide*
8800-A2-GN21	*Hotwire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8810-A2-GN11	*Hotwire 8810 DSLAM Installation Instructions*
9024-A2-GB20	*FrameSaver SLV 9x24 User's Guide*
9028-A2-GB20	*FrameSaver 9028 Compression Unit User's Guide*
9121-A2-GB20	*FrameSaver 9120 User's Guide*
9121-A2-GH30	*FrameSaver 9120 Technical Reference*
9124-A2-GB20	*FrameSaver SLV 9124 User's Guide*
9128-A2-GB20	*FrameSaver SLV 9126/9128 User's Guide*
9161-A2-GH30	*Model 916x/926x T1 Access Mux Technical Reference*
9191-A2-GB20	*NextEDGE Multiservices Access System User's Guide*
9580-A2-GB20	*FrameSaver SLV 9580 T3 ATM DSU User's Guide*
9621-A2-GB20	*FrameSaver 9620 User's Guide*
9621-A2-GH30	*FrameSaver 9620 Technical Reference*
9820-A2-GB20	*FrameSaver SLV 9820 User's Guide*

Contact your sales or service representative to order additional product documentation.

Most Paradyne documents are also available on the World Wide Web at:

http://www.paradyne.com

Select *Library* → *Technical Manuals*

See the following documents for more information about services, applications, and network deployment for your specific devices:

- *DSL Sourcebook*
- *Frame Relay Sourcebook*

Reference Documents

Black, Ulysses. *Network Management Standards. The OSI, SNMP and CMOL Protocols.* New York, NY: McGraw-Hill, 1992. (ISBN 0-07-005554-8)

Comer, Douglas. *Internetworking with TCP/IP: Principles, Protocols, and Architecture, Volume 1.* New York, NY: Prentice-Hall, 1991. (ISBN 0-13-468505-9)

IBM. *NetView for AIX Installation and Configuration, Version 4, Document Number: SC31-8163*: International Business Machines, 1992, 1995

McCloghrie, K., Rose, M.T., *Management Information Base for Network Management of TCP/IP-based Internets.* RFC 1156, March, 1991

Rose, M.T., *The Simple Book: An Introduction to Management of TCP/IP-based Internets.* Englewood Cliffs, NJ: Prentice-Hall, 1994 (ISBN 0-13-177254-6)

Rose, M.T., *The Simple Times: The Bi-monthly Newsletter of SNMP Technology*, **http://www.simple-times.org/pub/simple-times/issues**

World Wide Web Sites

The following sections list World Wide Web sites that may be of interest. At the time of this writing, the web sites are current.

HP OpenView Web Site

For the latest information on HP OpenView, visit the following web site:

`http://www.openview.hp.com/index.asp`

For information on installing and setting up OpenView, see the *Hewlett Packard (HP) Network Node Manager Products Installation Guide*.

NetView Web Site

For the latest information on Tivoli NetView, visit the following web site:

`http://www.tivoli.com/o_products/html/netview.html`

For information on installing and setting up NetView, see the *TME10 NetView Installation and Configuration Guide.*

OpenLane Performance Wizard Web Site

The OpenLane™ Performance Wizard™ application is used to collect and display both real time and historical data on various network devices. Using this data, you can monitor, analyze, troubleshoot, and networks that use Frame Relay, T1, and DSL network devices, and other network devices that support MIB-2 Frame Relay Transmission (RFC-1315), DS1 Transmission (RFC-1406), and Management Services (RFC-1604) variables.

For more information on the Performance Wizard, visit the following web site:

`http://www.paradyne.com/perfwizard/index.htm`

OpenLane DSLAM Configurator Web Site

The OpenLane DSLAM Configurator is used to quickly and efficiently configure a DSLAM chassis and its associated endpoints. Using the DSLAM Configurator, you can:

- Assign IP addresses for the Management Communication Controller (MCC) and Digital Subscriber Line (DSL) cards
- Specify Dynamic Host Configuration Protocol (DHCP) server information (if used)
- Create static routes to the Network Management System (NMS)
- Configure DSL ports and Service Providers, and manage additional card parameters
- Set Simple Network Management Protocol (SNMP) configuration information, such as community strings, trap destinations, and IP Security
- Perform Proxy Address Resolution Protocol (ARP) configurations

Management Information Base (MIBs) Web Site (Paradyne Only)

For the latest Paradyne MIB file information, visit the following web site:

`http://www.paradyne.com/tech_support/html/mibs.html`

Setting Up the DCE Manager

1

OpenLane DCE Manager Overview

The OpenLane™ DCE Manager provides an integrated set of components that you can use to administer, configure, monitor and diagnose Paradyne's Simple Network Management Protocol (SNMP) network access devices. It is available on HP-UX and Solaris systems running the HP OpenView Network Node Manager (herein referred to as OpenView), or AIX systems running NetView.

This chapter introduces the features of the DCE Manager, lists supported devices, and provides you with the information you need to install and run the DCE Manager on your operating platform.

Features of the DCE Manager

The DCE Manager offers several features that you can use to manage devices and device interfaces, including Data Link Connection Identifiers (DLCIs), Network Access Module (NAM) cards, Management Communication Controller (MCC) cards, Digital Subscriber Lines (DSL) cards and DSL endpoints. Use the DCE Manager to:

- Perform administrative tasks
  - — Open a graphical display of the front or rear of a device
  - — Synchronize devices
  - — Manage polling of devices for operational and administrative status
  - — Reset device firmware and cards
  - — Manage and unmanage device interfaces
  - — Navigate to other OpenView submaps
- Manage configurations
  - — Start a terminal session to perform tasks from a device's craft interface
  - — Display and modify configuration options
  - — Create and modify Injection Table configuration
  - — Back up and restore device configuration images
  - — Copy and store multiple configuration images
- Monitor and troubleshoot devices, device interfaces
  - — View status through the use of color-coded icons
  - — Obtain operational status and administrative status
  - — Identify the type of device or interface, and obtain other characteristics
  - — Turn a lamp test on or off
  - — Perform tests, including loopback, pattern, and connectivity tests
  - — Receive traps asynchronously from the device

You can also obtain context-sensitive help from within the DCE Manager components.

Devices Supported by the DCE Manager

Table 1-1 lists the supported devices and **major** functions of the DCE Manager. A check mark (✓) indicates that a function is supported. For a complete list and description of functions, see *Using the DCE Manager Components* in Chapter 2, *Using the DCE Manager*.

Table 1-1. OpenLane DCE Manager Functions

Supported Devices	Functions										
	ID	Status	Device Display	Device Config	Tests	Config Up/Down Load	Dev. Copy Config	Telnet	Trap Support	Device Reset	Lamp Test
3100s	✓	✓	✓	✓	✓		✓	✓	✓		
3300s	✓	✓	✓	✓	✓		✓	✓	✓		
5100s	✓	✓	✓	✓	✓			✓	✓		
5216, 5246	✓										
5446	✓	✓	✓	✓					✓	✓	
7110, 7112	✓	✓	✓	✓	✓		✓	✓	✓	✓	
7974, 7975, 7976, 7984, 7985, 7986	✓	✓	✓	✓	✓			✓	✓	✓	
8100, 8200								✓	✓		
7610, 7612	✓	✓	✓	✓	✓		✓	✓	✓	✓	
8310, 8312, 8510	✓	✓	✓	✓					✓	✓	
8540, 8546, 8600, 8610, 8800, 8810	✓	✓	✓	✓				✓	✓	✓	
8774, 8775, 8776, 8784, 8786	✓	✓	✓	✓	✓			✓	✓	✓	
9028	✓	✓	✓					✓	✓		
9120, 9124, 9126, 9128, 9192, 9195, 9580, 9620, 9624, 9820	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9162, 9165, 9262, 9265	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
AACs	✓	✓	✓	✓		✓		✓	✓		
DACS LSIU	✓	✓	✓	✓		✓		✓	✓		

Preparing to Install the DCE Manager

Before you install the OpenLane DCE Manager Release 4.3, check the contents of the distribution package and ensure that your system meets the requirements as outlined in the following sections.

In addition to the requirements listed, read the OpenView or NetView release notes, which provide the latest information on the use of each product.

- For HP-UX and Solaris systems:

  `/opt/OV/ReleaseNotes/attGEM/attGEMr1.rn`

- For AIX systems:

  `/usr/OV/ReleaseNotes/attGEM/attGEMr1.rn`

Verifying the Contents of the Distribution Package

The DCE Manager software and documentation are available on the World Wide Web. However, in certain instances, a distribution package is made available, which consists of the following:

- DCE Manager, distributed on CD-ROM (for either OpenView or NetView)
- *OpenLane DCE Manager User's Guide* (this manual), which provides details on installing and using the DCE Manager
- Software License Agreement, which specifies the product serial number
- Software License Key Request form, which you must fill out and fax to the specified location to obtain a license key

Retain the Software License Agreement and the Software License Key, as both are needed during installation or if you place a call for service.

Verifying Software Requirements

The DCE Manager software can be installed on the following operating platforms:

- Solaris 2.5 or higher for Sun systems
- HP-UX 10.10 or higher for HP systems
- AIX Release 4.1.4 or higher for IBM systems

Depending on the operating platform you are using, you must also have the following software available on your system:

- HP OpenView Network Node Manager, Release 5.01 or higher, with the highest consolidated patch (for Solaris and HP-UX systems only)
- NetView for AIX Release 4 or 5 (for AIX systems only)
- Tooltalk, which is a part of the Common Desktop Environment (CDE) toolset

Verifying Hardware Requirements

The following lists the minimum hardware requirements needed to install the DCE Manager on HP, Sun, or IBM platforms:

- 64 MB of RAM minimum
- 50 MB of free hard disk space
- 128 MB of swap space (for HP or SUN workstations only)
- 196 MB of swap space (for IBM workstations only)

Setting Kernel Parameters (HP-UX Only)

Table 1-2 shows the recommended HP-UX kernel parameter settings. These parameters can be set using the **sam** command.

Table 1-2. Recommended Kernel Parameter Values for HP Systems

Parameter	Recommended Value	Description
maxfiles	256	Soft file limit per process
maxfiles_lim	1024	Hard file limit per process
nfiles	2048	Maximum number of open files
nproc	512	Maximum number of processes
maxuproc	128	Maximum number of processes per user
ninode	2048	Maximum number of open inodes

Meeting Network and Device Requirements

You must ensure the correct configuration of devices, and all devices must be connected to the Network Management System (NMS) running OpenView or NetView through a TCP/IP network. The physical medium that connects the devices to NMS must be supported by the TCP/IP software package. If the platform can communicate with the device using the OpenView *SNMP MIB Browser,* then the DCE Manager software can manage the device.

OpenView and NetView establish a management link to devices using one of the following methods:

- Local Area Network (LAN), using a router or LAN adapter
- Leased line
- Dial-up connection

Discovery and management of devices is straightforward over a LAN and leased-line connections. Once the hardware and software are configured, OpenView discovers the devices and maintains a continual diagnostic link to them.

Dial-up connections are more problematic because you may need to manually configure the Point-to-Point Protocol (PPP) software with a large number of phone numbers, and dialing a large number of devices can take a long time. Also, if you dial a device on an as-needed basis only, the devices appear on the map in an unknown state (blue) when a connection does not exist.

See Appendix A, *SNMP Management Connectivity* for examples of network management connections.

Verifying OpenView Requirements (HP-UX and Solaris Only)

The following requirements must be met if you are using the OpenView environment on HP-UX or Solaris systems:

- The DCE Manager runs on OpenView management stations and X terminals connected to management stations only. Do not install or attempt to use the DCE Manager on OpenView distributed consoles.
- The OpenView on-demand submap feature cannot be enabled. Set Maps to **persistent** at all levels.
- The DCE Manager handles devices discovered by OpenView only. It does not manage devices discovered and managed by remote node managers (collection stations).
- The DCE Manager supports the default filter settings for OpenView only.

Installing the DCE Manager

The DCE Manager software is available on the World Wide Web (WWW) and on CD-ROM for HP-UX, Solaris, and AIX platforms. The following sections describe how to access and install the DCE Manager software.

Installing the DCE Manager on HP-UX or Solaris

This section describes how to download and install the DCE Manager software on HP-UX or Solaris operating platforms.

▶ Procedure

To install the DCE Manager on a HP-UX or Solaris system:

1. Log into the targeted system as root.
2. Enter the following command lines:

   ```
   PATH=/usr/bin:$PATH:/opt/OV/bin
   export PATH
   ```

3. Stop the Volume Manager (**vold**), if it is running (Solaris systems only).

   To see if the Volume Manager is active on your system, type the following:

   ```
   ps -ef | grep vold
   ```

   If the Volume Manager is running, note the process number for **vold** returned by the **ps** command, then enter the following to stop the process:

   kill -9 <*process number*>

4. Access the install program.

   — If you are downloading the software from the World Wide Web, go to the web site, which provides access to the DCE Manager:

   http://www.paradyne.com/products/ovr_management.html

   Download the file **SOLARIS_tar.Z** (for Sun systems) or **HPUX_tar.Z** (for HP systems) to your local system and uncompress the file as follows:

   uncompress <*tarfile*>

   In the previous example, <*tarfile*> is the name of the compressed tar file you downloaded.

   — If you are loading from CD-ROM for HP systems, mount the CD-ROM as follows:

   ```
   mkdir /tmp/cdrom
   /etc/mount -r /dev/dsk/<cdrom> /tmp/cdrom
   ```

   In this example, <*cdrom*> is the name of the CD-ROM device.

   — If you are loading from CD-ROM for Sun systems, mount the CD-ROM as follows:

   ```
   mkdir /tmp/cdrom
   /etc/mount -F hsfs -o ro,nomaplcase /dev/sr0
   /tmp/cdrom
   ```

5. Start the install program.

   — If you downloaded the software from the World Wide Web, change to the directory where you uncompressed the file and run the installation program:

   cd *<directory>*
   ./DCEinstall

   — If you mounted the CD-ROM for HP systems:

   cd /tmp/cdrom/DCE/HP-UX10
   ./DCEinstall

   — If you mounted the CD-ROM for Sun systems:

   cd /tmp/cdrom/DCE/SOLARIS2
   ./DCEinstall

6. Respond to the installation prompts. The prompts vary depending on whether or not the DCE Manager is currently installed on your system.

   — If the DCE Manager is currently installed on your system, the following prompt appears:

   Do you want to remove the existing product? (y/n)

   Enter **y** to remove the installed version of the DCE Manager. After removing the installed version, the installation process asks if you want to install the DCE Manager. You must enter **y** to continue.

   Enter **n** to stop the installation.

   — If the DCE Manager is not installed on your system, the following prompt appears:

   Do you want to install OpenLane™ DCE Manager? (y/n)

   Enter **y** to continue the installation.

   Enter **n** to stop the installation.

7. Enter the product serial number, which is printed on the Software License Agreement distributed with the product:

   Please enter the product serial number:

8. Enter the software license key. The prompts you receive vary depending on whether or not you have a current license key.

   — If you have a software license key, the following prompt appears:

   `Do you want to enter a new software key? (y/n)`

   Enter **`y`** to enter the software license key. A new prompt appears.

   Enter **`n`** if you want to enter the software license key at a later date. The installation process continues, but you cannot use the DCE Manager functions until the new software license key has been entered, unless you have time remaining on your current license key.

   — If you have never entered a software license key, the following prompt appears:

   `Please enter your software key:`

   The installation process specifies the number of days remaining before the software license key expires.

9. Check the log files for your platform if you receive error messages during the installation process.

   — For HP systems:

   `/var/adm/sw/swagent.log`
   `/var/adm/sw/swconfig.log`

   — For Sun systems:

   `/tmp/update.log`
   `/var/adm/sw/swagent.log`

10. Change to the root directory:

    `cd /`

11. Unmount the CD-ROM:

    `/etc/umount /tmp/cdrom`

12. Restart the volume manager, if it was stopped (Solaris only):

    `vold &`

13. Exit from root.

The DCE Manager is automatically integrated into the OpenView application. When you start the OpenView application, the DCE Manager can be accessed through the Configuration or Fault menus.

Installing the DCE Manager on AIX

This section describes how to install the DCE Manager software on the AIX operating platforms. For information on the system commands used in the following procedure, refer to the AIX documentation set.

▶ Procedure

To install the DCE Manager on an AIX system:

1. Log in as root.
2. Set your path variables as follows:

   ```
   PATH=/usr/bin:$PATH:/usr/OV/bin
   export PATH
   ```

3. Access the install program.

   — If you are downloading the software from the World Wide Web, go to the web site, which provides access to the DCE Manager:

   http://www.paradyne.com/products/ovr_management.html

   Download the **AIX_tar.Z** file and uncompress it as follows:

   uncompress AIX_tar.Z

   — If you are loading from CD-ROM, mount the CD-ROM as follows:

   ```
   mkdir /tmp/cdrom
   /etc/mount -r -v cdrfs /dev/cd0 /tmp/cdrom
   ```

4. Start the install program.

   — If you downloaded the software from the World Wide Web, change to the directory where you uncompressed the file and run the installation program:

   cd *<directory>*
   ./DCEinstall

   — If you mounted the CD-ROM, change to the directory where the CD-ROM is mounted and run the installation program:

   ```
   cd /tmp/cdrom/DCE/AIX4
   ./DCEinstall
   ```

5. Specify whether or not you want to continue with the installation. The prompts vary depending on whether or not the DCE Manager is currently installed on your system.

   — If the DCE Manager is currently installed on your system, the following prompt appears:

   `Do you want to remove the existing product? (y/n)`

   Enter **`y`** to remove the installed version of the DCE Manager. After removing the installed version, the installation process asks if you want to install the DCE Manager. You must enter **`y`** to continue.

   Enter **`n`** to stop the installation.

   — If the DCE Manager is not installed on your system, the following prompt appears:

   `Do you want to install OpenLane™ DCE Manager? (y/n)`

   Enter **`y`** to continue the installation.

   Enter **`n`** to stop the installation.

6. Enter the product serial number:

   `Please enter the product serial number:`

7. Enter the software license key. The prompts you receive vary depending on whether or not you have a current license key.

   — If you have a software license key, the following prompt appears:

   `Do you want to enter a new software key? (y/n)`

   Enter **`y`** to enter the software license key. You are then prompted as follows:

   `Please enter your new software key:`

   Enter **`n`** if you want to enter the software license key at a later date. The installation process continues, but you cannot use the DCE Manager functions until the new software license key has been entered, unless you have time remaining on your current key.

   — If you have never entered a software license key, the following prompt appears:

   `Please enter your software key:`

   The installation process specifies the number of days remaining the software license key expires.

8. Check the **`smit.log`** file for your platform, which specifies any errors encountered during the installation.

9. Change to the root directory:

   `cd /`

10. Unmount the CD-ROM:

    /etc/umount /tmp/cdrom

11. Exit from root.

12. Reboot your machine.

The DCE Manager is automatically integrated into the NetView application. When you start the NetView application, the DCE Manager is available from the Configuration or Fault menus.

Verifying the Installation

The following sections provide you with the information you need to verify the installation of the DCE Manager software and the version of the DCE Manager software installed.

Checking Installed Software

To ensure that the DCE Manager has been installed on your system properly, enter the command line applicable to your system:

- For HP-UX and Solaris systems:

  /opt/OV/bin/ovstatus

- For AIX systems:

  /usr/OV/bin/ovstatus

If the DCE Manager is installed properly, the following processes are listed:

```
object manager name: attGEMlistener
 state:               RUNNING
 PID:                 1425
 last message:        Initialization complete.
 exit status:         –

object manager name: attGEMgtp
 state:               RUNNING
 PID:                 1432
 last message:        Initialization complete.
 exit status:         –

object manager name: attGEMparser
 state:               RUNNING
 PID:                 1433
 last message:        Initialization complete.
 exit status:         –
```

Determining the Version of the DCE Manager

If you need to determine the version of the DCE Manager that is installed on your system, type the following at the system prompt:

- For HP-UX and Solaris systems:
  `/opt/OV/bin/attGEMRel`
- For AIX systems:
  `/usr/OV/bin/attGEMRel`

Viewing Management Information Base (MIBs) Files

The DCE Manager uses internal copies of MIB files to manage devices and device interfaces.

▶ **Procedure**

To browse the MIB files using either OpenView or NetView:

1. Click on the Options menu and select Load/Unload MIBs SNMP. This opens a dialog box that you can use to manage the MIBs.
2. Click on the Misc menu and select SNMP MIB Browser. This opens a dialog box that you can use to view the MIB files.

Performing an Upgrade

Occasionally, you may have to upgrade the DCE Manager software. While information is not typically lost or corrupted during an upgrade, it is recommended that you back up your system before performing the upgrade process.

To perform the upgrade, you must have the product serial number and the software license key used to install your system.

Removing the DCE Manager

This section describes how to remove the DCE Manager from HP-UX, Solaris, or AIX operating platforms.

▶ Procedure

To remove the DCE Manager:

1. Log in as root on the system where the DCE Manager is installed.
2. Set the PATH variable and export the path using the commands for your operating platform:
   - For HP and Sun systems:

     ```
     PATH=$PATH:/opt/OV/bin:/sbin:/usr/sbin
     export PATH
     ```

   - For AIX systems:

     ```
     PATH=$PATH:/usr/OV/bin:/etc:/usr/etc
     export PATH
     ```

3. Stop the OpenView or NetView process:

   ```
   ovstop
   ```

4. Remove the DCE Manager:

   ```
   attGEMremove
   ```

5. Restart the OpenView or NetView process (if you stopped the process in Step 3):

   ```
   ovstart
   ```

Retaining Event Configuration

When the DCE Manager is installed or removed, the **`trapd.conf`** database is purged of all entries placed there by the DCE Manager. If you specified additional additional actions for traps associated with a Paradyne device using OpenView, these actions are deleted also when the DCE Manager is installed or removed.

To keep these actions, you must reenter the data using OpenView or the **`trapd.conf`** database must be modified after installing or removing the DCE Manager. The following table lists the location of the database for each operating platform.

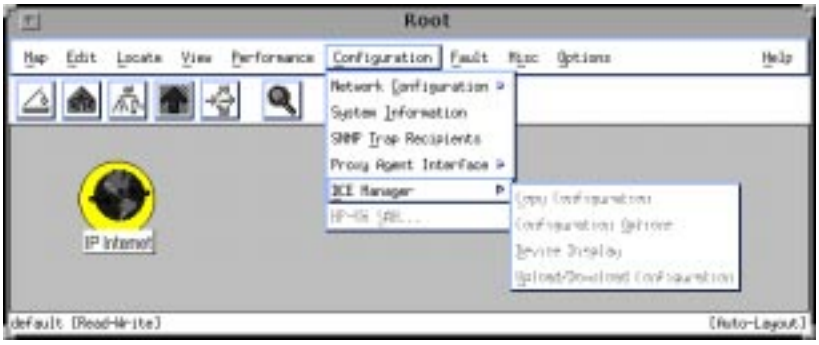
Platform	Database Location
Solaris	**`/etc/opt/OV/share/conf/C/#trapd.conf.bak`**
HP-UX Version 10	**`/etc/opt/OV/share/conf/C/#trapd.conf.bak`**
AIX	**`/usr/OV/conf/C/#trapd.conf.bak`**

NMS System Setup for the DCE Manager

In most instances, an NMS workstation is connected to a router. With this setup, the NMS can easily access devices on other subnets. However, if the NMS is not attached to a router (such as a hub), you must create explicit routes to the other subnets. To do this, use the **`route`** command from the command line to manipulate the NMS routing table manually. See the **`route`** manpage for command line arguments.

Starting the DCE Manager

The DCE Manager is integrated with OpenView or NetView during the installation process and is available as a menu item on the Configuration and Fault menus. Selecting the DCE Manager menu item opens a submenu of its functions.



The remaining chapters in this manual describe how to use the DCE Manager with the OpenView user interface. Although the OpenView and NetView interface differ somewhat, the function of the DCE Manager is the same.

Using the DCE Manager

2

Overview

The OpenLane DCE Manager is integrated with OpenView during the installation process. Thus, any device that is discovered by OpenView can be managed using the components of the DCE Manager.

A subset of DCE Manager functions are available from the OpenView menus. However, to use all of the features of the DCE Manager, or to perform an action on a device interface, you must open a Device Display. A Device Display shows a front or rear view of a selected device and its associated interfaces.

This chapter provides you with the information you need to access and use the components of the DCE Manager from within OpenView or a Device Display.

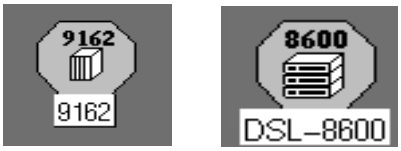
Discovering Devices

OpenView offers several features used by the DCE Manager, which includes the discovery of devices and creation of submaps. OpenView discovers devices by polling the network for device information.

Once a device is discovered, it is added to a submap, which presents a view of your network. You can have many submaps depending on the configuration of your network.

Each device in a submap is presented as a **device icon**. Device icons display the model number, device type, and the device selection name as shown in the following table.

The color of each device icon presented in a submap represents the status of that device as described in Chapter 5, *Monitoring Devices*.

Icon	Device
	Standalone DCE device
	IP-addressable carrier card device
	Multi-slot device

Discovering Endpoints

The Hotwire 5446 RTU, which interoperates with the 8546 RADSL card, does not appear on the OpenView submaps by default. However, it is discovered by the DCE Manager and placed on a separate submap behind the icon that represents the DSLAM chassis. You can launch a Device Display for the 5446 RTU from the Device Display of a DSLAM chassis or from the submap. Using the Device Display for the 5446 RTU, you can perform a variety of DCE Manager functions.

The Hotwire 79*xx* M/HSDL and M/SDSL endpoints interoperate with 87*xx* M/HSDL and M/SDSL cards. You can launch a Device Display for the 79*xx* endpoints from the Device Display of a DSLAM chassis or from a submap.

All other endpoints are discovered by the DCE Manager and proxied on each DSL card. While you cannot launch a Device Display for these endpoints, you can obtain the identity of the endpoint from the Device Display for the DSLAM card.

See *Managing Devices Behind the DSLAM Chassis* on page 2-14 and *Obtaining the Identity of Devices and Interfaces* in Chapter 5, *Monitoring Devices*, for more information.

Discovering FrameSaver Remote Site Units

A FrameSaver remote site unit is not automatically discovered because it is not colocated and resides outside of the local domain of the FrameSaver unit and the NMS. To force discovery, add map or subinterface statements 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.

Accessing the DCE Manager

You can access the DCE Manager and a subset of its functions from the OpenView menus. The DCE Manager functions that are available from within OpenView can be applied to a device itself, but not to an individual device interface (port).

To use the complete features of the DCE Manager, including performing an operation on a device interface, you must use the Device Display. The Device Display presents a front or rear view of a device and its interfaces and offers menus that you can use to perform all of the DCE Manager functions.

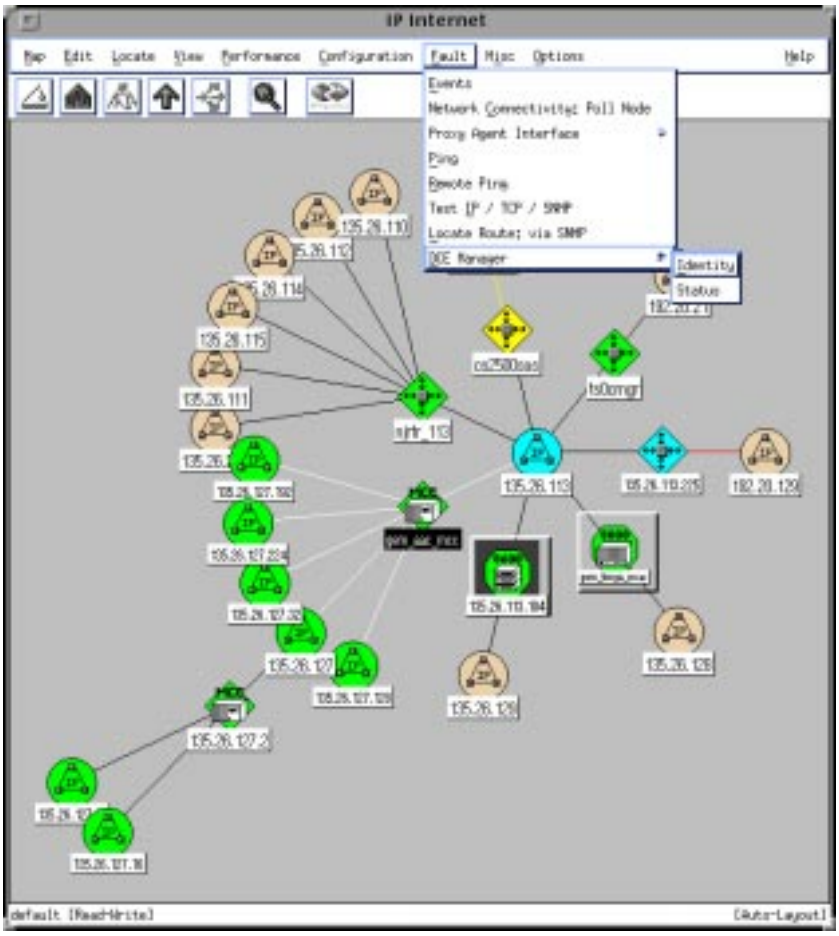
The following sections discuss how to access the DCE Manager components within OpenView, including the Device Display.

Accessing the DCE Manager Submenus from OpenView

The DCE Manager appears as a menu item on the OpenView Configuration and Fault menus. Selecting the DCE Manager menu item opens a cascading submenu of DCE Manager functions.

The following example shows the DCE Manager submenu cascade that is available from the OpenView Configuration menu.

The following example shows the DCE Manager submenu cascade that is available from the OpenView Fault menu.



See *Components Available from the OpenView DCE Manager Submenus* on page 2-6, which lists and describes the use of each of the previously listed functions.

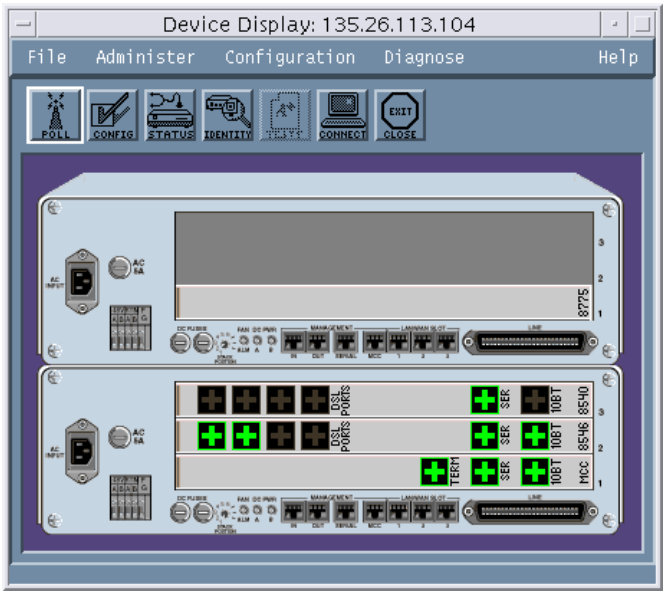
Accessing the Device Display from OpenView

The DCE Manager Device Display is used to perform operations on devices and device interfaces. It provides a front or rear presentation of a device and its interfaces and enables you to use all of the components of the DCE Manager.

To access the Device Display, use any of the following methods:

- Double-click on a submap device icon.
- Select DCE Manager from the Configuration menu, then click on Device Display.
- Position the mouse over a submap device icon, click on the right mouse button, and select Open Symbol from the pop-up menu.

The following figure is an example of a DCE Manager Device Display window. Using the menus or toolbar within the Display Device, you can perform various operations on a device or device interface.



Using the DCE Manager Components

You can access the DCE Manager components from both the OpenView and Device Display menus. The OpenView menus offer those DCE Manager components that can be performed on a device only. The Device Display offers the complete set of DCE Manager functions, including a toolbar and pop-up menus, which you can use to access the most commonly used functions quickly.

The following sections discuss:

- DCE Manager submenus within OpenView
- Device Display menus
- Device Display pop-up menus
- Device Display toolbar

Components Available from the DCE Manager Submenus

The DCE Manager is available from the OpenView Configuration and Fault menus as a menu item. Selecting the DCE Manager from either menu provides a submenu of DCE Manager functions. Table 2-1 and 2-2 list and describe these components.

Table 2-1. OpenView Configuration DCE Manager Submenu Items

DCE Manager Submenu Item	Description
Copy Configuration	Creates duplicate or modified images of a device configuration and stores it within the configuration area of the device itself.
Configuration Options	Lists device parameters and is used to set parameters for a device.
Device Display	Opens a Device Display window, which presents a front or rear view of the selected device.
Upload/Download Configuration	Saves and restores device configuration images.

Table 2-2. OpenView Fault DCE Manager Submenu Items

DCE Manager Submenu Item	Description
Identity	Opens a dialog and displays information about the selected device, such as device type, model, release number, version number, device uptime, and so forth.
Status	Opens a dialog and displays operational and administrative status on a device. Some of the fields can be modified.

Components Available from the Device Display Menus

The DCE Manager Device Display menus contain options which you can use to perform various operations on devices and device interfaces. Likewise, the Device Display toolbar and pop-up menus (as described in the following sections) provide a shortcut to some of these menu items. Depending on the device or interface you are viewing, some options are not available. Table 2-3 lists and describes the Device Display menus.

Table 2-3. Device Display Menus (1 of 2)

Menu	Menu Item	Description
File	Exit	Closes the Device Display window.
Administer	Demand Poll	Causes a device to be polled for operational and administrative status, regardless of the polling interval.
	Device Sync	Updates configuration information for a device.
	Manage	Specifies that a device interface is in a state where it can be polled, updated, and so forth.
	Unmanage	Specifies that a device interface cannot be polled or updated.
	Show Submap	Opens the OpenView submap associated with the device from within the Device Display.
	Reset Device	Performs a warm start of a device remotely.
	Reset Card	Performs a warm start of a card remotely.
	Set Polling Interval	Specifies how frequently the DCE Manager queries a device for status information.
Configuration	Options	Displays parameters associated with a device and can be used to modify certain parameters for a device.
	Connect	Opens a terminal window, which you can use to gain direct access to a device's craft interface.
	Copy	Creates duplicate or modified images of a device configuration and stores it within the configuration area of the device itself.
	Upload/Download	Saves and restores device configuration images.
	DLCI Options	Displays parameters associated with DLCIs.
	VP/VC Options	Displays parameters associated with the virtual paths and channels aligned with DLCIs on an ATM interface.
	Remote Device Display	Opens a Device Display for 5446 RTUs configured behind 8546 DSL interfaces and 79*xx* endpoints configured behind 87*xx* M/HDSL and M/SDSL interfaces.
	Remote Device Identity	Displays information about the endpoints configured on each DSL interface.

Table 2-3. Device Display Menus (2 of 2)

Menu	Menu Item	Description
Diagnose	Identity	Displays information about the selected device, such as device type, model, release number, version number, device uptime, etc.
	Status	Displays operational and administrative status on a device. Some of the fields can be modified.
	DLCI Status	Displays details about DLCIs, such as the operational and administrative status, tests results, and Frames Dropped by Outbound Enforcement.
	SLV Status	Displays details about DLCIs, such as Frames and Octets Dropped by the network, Latency Width, Latency Period, etc.
	VP/VC Status	Displays details about the status of DLCIs associated with a virtual path and channel.
	VP/VC SLV Status	Displays details about Latency Width, Latency Status, Average Latency, Packet Size, etc.
	Tests	Starts loopback and pattern tests for the interface you selected.
	PVC Tests	Starts loopback and pattern tests for the specified DLCI.
	Lamp Test Start	Causes the lights to blink on the front panel of a supported device. This option is useful when you are attempting to locate a single device with a setup of many devices.
	Lamp Test Stop	Causes the lights on the front panel of a supported device not to blink.
Help	On Context	Opens a window and displays context-sensitive help.

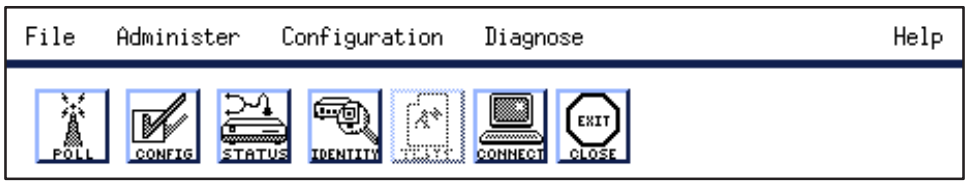
Device Display Pop-up Menus

Within a Device Display, pop-up menus provide shortcuts to certain operations that can be performed on a device interface. Any item contained in a pop-up menu is available from the Device Display menus also.

See *Performing an Operation on a Device Interface* on page 2-12, which describes how to access the pop-up menus.

Components Available from the Device Display Toolbar

The Device Display toolbar appears below the menus and offers a shortcut to the most commonly used menu selections.



The following options are available from the toolbar:

- Polls a device to obtain the operational and administrative status of its ports (equivalent to menu selection *Administer* →*Demand Poll*)

- Provides the configuration settings of a device or port and enables you to change some of these settings (equivalent to menu selection *Configuration* →*Options*)

- Provides identity information about a device or DSLAM card (equivalent to menu selection *Diagnose* →*Identity*)

- Provides status information about a device or port (equivalent to menu selection *Diagnose* →*Status*)

- Provides **Telnet** connection to a device's native interface (equivalent to menu selection *Configuration* →*Connect*)

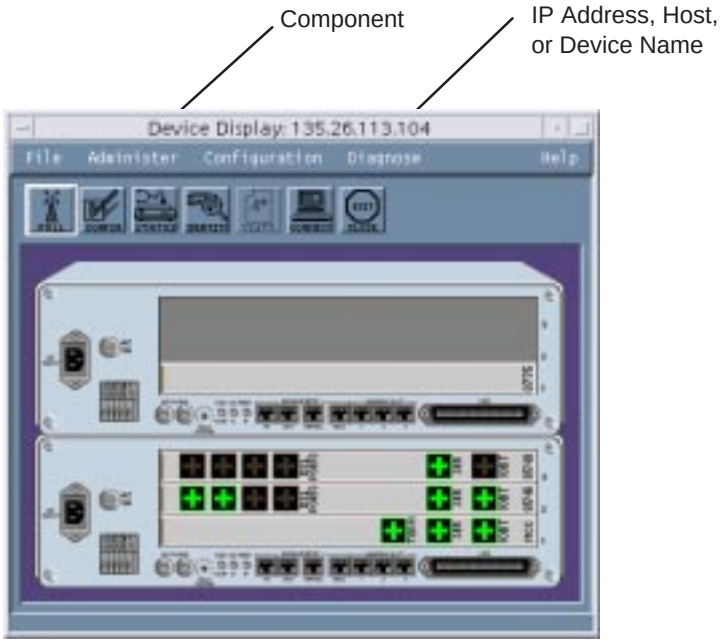
- Opens a dialog, which you can use to select loopback modes and pattern tests (equivalent to menu selection *Diagnose* →*Tests*)

- Closes the device display (equivalent to menu selection *File* →*Exit*)

- Additionally, there is a Display Front/Back button that switches between front and back views of full expansion AAC devices

Using the Device Display

The DCE Manager Device Display window offers a front or rear view of a device. Each Device Display window specifies the DCE Manager component name, IP address, Hostname, or Device name.



Within the Device Display windows, device interfaces are represented by icons. Operations within the Device Display can be performed on the device itself or a device interface. However, to perform an operation on a device interface, you must first select it.

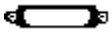
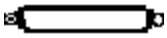
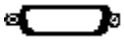
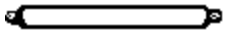
The DCE Manager functions are available from the Device Display menus and the toolbar provides access to frequently used features. Pop-up menus are used to provide quick access to components for device interfaces.

The following sections discuss:

- Understanding the icons used in a Device Display
- Performing an operation on a device from the Device Display
- Performing an operation on a device interface from the Device Display
- Accessing a Device Display for interfaces behind the DSLAM chassis

Understanding the Device Display Interface Icons

Icons are used to represent each of the device interfaces in the Device Display. The following table displays each icon used and specifies the interface it represents.

Icon	Interface
	RJ11 connector
	RJ48 connector
	DB9
	DB15
	DB25
	DB26
	DB50
	V.35
	Generic connector representing logical data interfaces.

Within the Device Display, color is used to indicate the operational and administrative state of an interface. See Chapter 5, *Monitoring Devices*, for an explanation of the colors used.

Performing an Operation on a Device

To perform an operation from the Device Display on the device itself, use either of the following methods:

- Click on any menu and then select the operation from the available menu items.
- Click on the option in the toolbar menu.

If a menu item or toolbar option is dimmed, it is unavailable for the device you selected.

Performing an Operation on a Device Interface

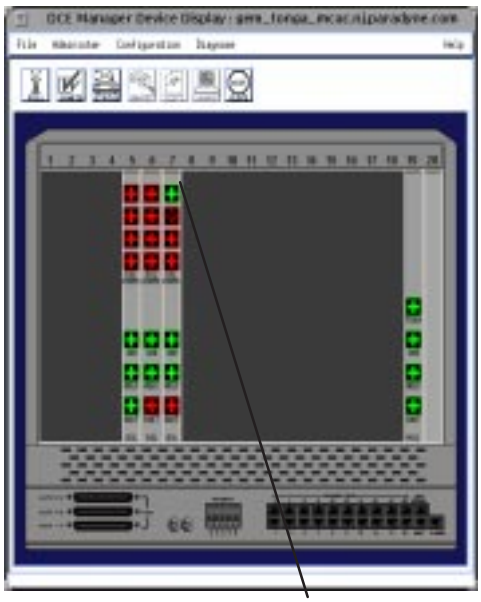
You can perform an operation on a device interface using the Device Display menus, toolbar, or pop-up menus. The following procedures describe how to select a device and perform an operation using any of these options.

If a menu item or toolbar option is dimmed, it is unavailable for the device interface you selected.

▶ Procedure

To select a device interface and perform an operation from the menus or toolbar:

1. Click on the interface to select it for an operation.
2. Choose the operation you want to perform from the Administer, Configuration, or Diagnose menu, or click on a toolbar option.



▶ Procedure

To select a device interface and access the pop-up menu:

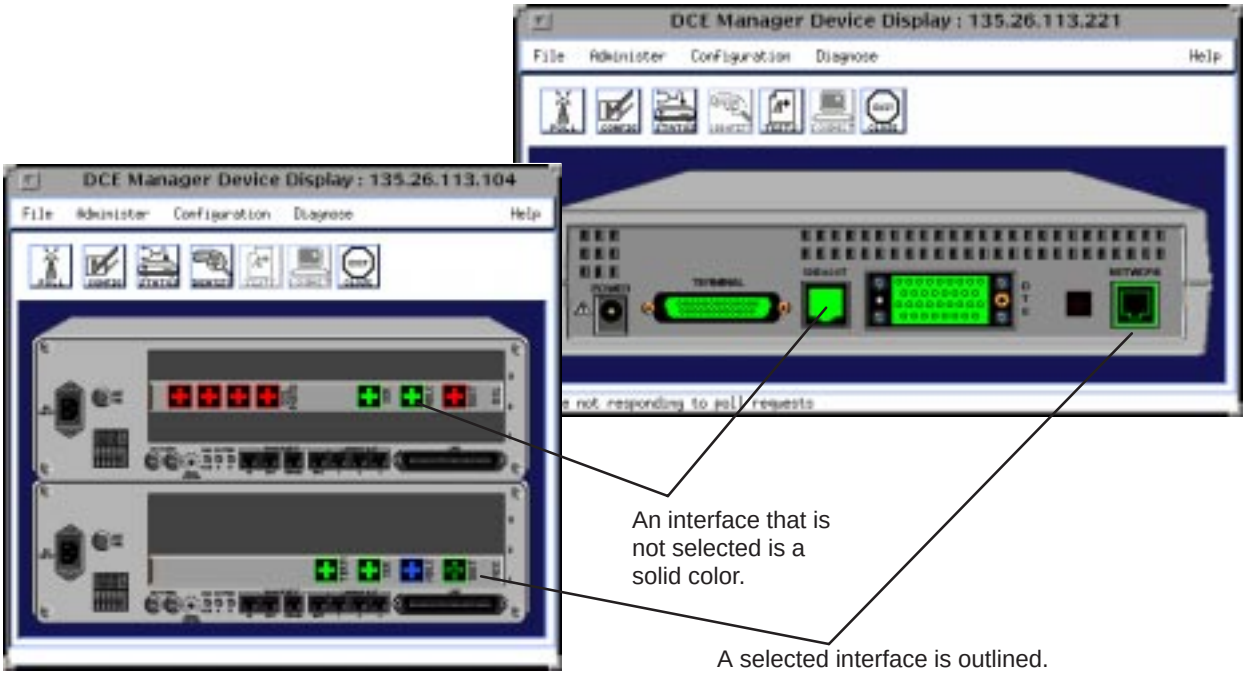
1. Position the cursor over an interface and press the right mouse button. A pop-up menu appears.
2. Select the operation you want to perform from the pop-up menu.

   The options available to you depend on the device interface you select.

   The menu items are described in Table 2-3, Device Display Menus.

Position the cursor over a device interface icon and press the right mouse button to display the pop-up menu items.

When you select a device interface within the Device Display, it is outlined. If a device interface is not selected, it remains a solid color as shown in the following example.



Managing Devices Behind the DSLAM Chassis

A Device Display for the various DSLAM chassis displays the cards configured for each chassis. The Device Display for a DSLAM chassis varies depending on the type of chassis selected. There are three types of DSLAM chassis:

- The 8600 DSLAM chassis is an independent, standalone system that consists of three slots, with one slot reserved for the MCC card and the remaining slots used to house the DSL cards. However, this chassis provides a stackable design that allows up to six systems to share management access through a single MCC card, which in turn, frees an additional slot for a DSL card in the remaining stacked systems.

  In a stacked configuration, the base chassis must contain the MCC card in Slot 1, while the other two slots can house up to two DSL cards. Each additional chassis in the stack can house up to three DSL cards.

- The 8800 DSLAM chassis is a 20-slot system designed to house 18 DSL cards and one MCC card. The remaining slot is reserved for future use.

- The 8810 DSLAM chassis is designed for high-density cards. It is a 20-slot system with integral power, alarm, cooling, and interface subsystems that is designed to house up to 18 DSL cards and one MCC card. The remaining slot is reserved for future use.

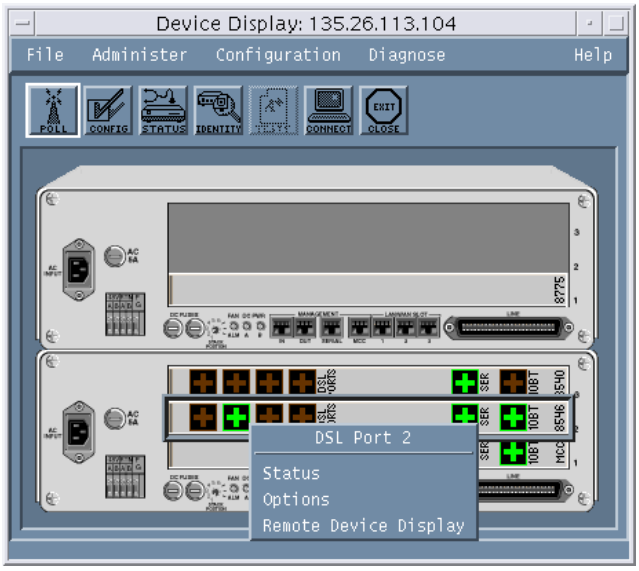
Each DSL card in a chassis can have up to four interfaces and a single endpoint can be connected to each interface. The 5446 and 79*xx* endpoints have an SNMP agent which can be managed directly by the DCE Manager. The remaining endpoints are proxied on the DSL cards.

You can launch a Device Display for the 5446 and 79*xx* endpoints from a Device Display of a DSLAM chassis that contains a corresponding 8546 DSL or 87*xx* card or an OpenView device submap as described in the following procedures.

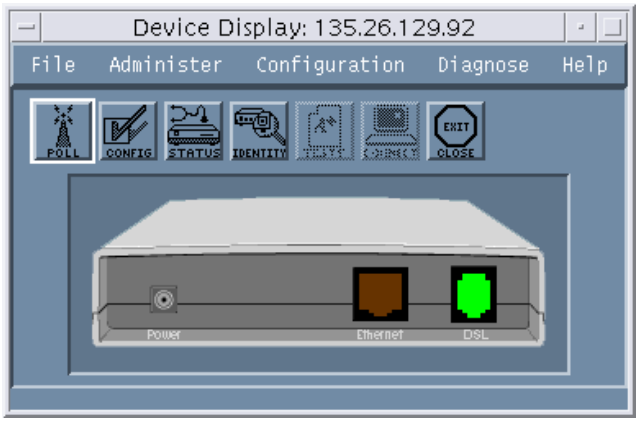
▶ Procedure

To launch a Device Display of a 5446 or 79*xx* endpoint from the Device Display for a DSLAM chassis:

1. Open the Device Display for a DSLAM chassis:
2. Position the mouse over the DSL card interface and click on the right mouse button. A pop-up menu appears.



3. Select Remote Device Display from the pop-up menu. The Device Display for an endpoint appears.

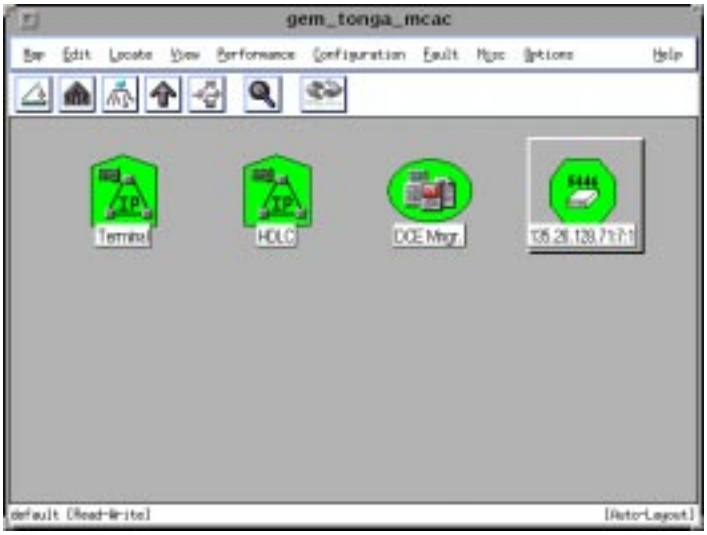


If an endpoint is not connected to the interface, this option is dimmed on the pop-up menu.

▶ Procedure

To launch a Device Display of an endpoint from an OpenView submap:

1. Open the Device Display for the DSLAM chassis.
2. Click on the Administer menu and select Show Submap. An OpenView submap that lists the available endpoints appears.



3. Double-click on endpoint icon to open the Device Display.

A Device Display is available for the 5446 and 79*xx* endpoints only. For other endpoints, you can obtain information about the endpoints using the identity option.

Managing the IP Conservative DSLAM

When a DSLAM is configured in IP Conservative mode, the chassis, cards, and endpoints all appear to have the same IP address. The cards and endpoints are addressed through a distinct community string.

NMS can manage the cards and endpoints when the community string does not contain either of the following special characters: ~ and @

Any community string in the network must also refrain from using these special characters.

Administering Devices

3

Overview

Using the DCE Manager, you can perform various administrative operations, which include:

- Updating device information
- Setting polling intervals
- Managing and unmanaging devices
- Displaying other submaps
- Resetting device firmware and cards

Updating Device Information

The DCE Manager maintains a device database, which provides configuration information for each device known to the DCE Manager. If a new device is added to the network, the DCE Manager is notified by OpenView. Once the DCE Manager is notified, it queries the device for configuration information and adds this to its internal database.

Occasionally, the configuration of a device is modified. To ensure that the DCE Manager device database contains the correct configuration for a device, you can perform a synchronization of the device with the device database as described in the following procedure.

▶ Procedure

To update the DCE Manager's device database:

1. Open a Device Display window.
2. Click on the Administer menu in the Device Display window and select Device Sync.

On receipt of a Change Configuration Notification (CCN) trap, device synchronization occurs automatically.

Polling Devices

By default, devices are queried periodically for operational and administrative status, while the Device Display component is present. You can specify how frequently a device is polled for status, as well as perform a demand poll to obtain immediate status. The following sections discuss these options.

See *Managing and Unmanaging Device Interfaces* on page 3-3, which describes how to turn polling on or off for device interfaces.

Setting a Polling Interval

▶ Procedure

To specify how frequently the DCE Manager queries a device for status information:

1. Open a Device Display window.
2. Click on the Administer menu and select Set Polling Interval. A Set Poll Rate dialog appears.
3. Use the sliding bar to set an interval. (The default is 1 minute.)
4. Click on the Apply button.

You can change the default poll rate for all devices by changing the value of the **attGEMdd*pollRate** parameter in the **/opt/OV/att/attGEM/GEMDD.res** file (or the **/usr/OV/att/attGEM/GEMDD.res** file for AIX systems). The value of the parameter represents the poll rate in minutes. The default is 1 minute.

To suspend polling, set the polling interval to zero (0).

Using Demand Poll

To obtain immediate operational or administrative status on a device from the Device Display window, do one of the following:

- Click on the Administer menu and select Demand Poll.
- Click on the Poll button available from the toolbar.

A status message indicates whether or not a device is currently being polled. A Demand Poll can occur while the Device Display is open only.

Managing and Unmanaging Device Interfaces

You can set the management state of a device interface as managed or unmanaged. When an interface is managed, it is polled for its administrative and operational state. The device or device interface icon on the OpenView submap changes color to reflect its current state.

An interface that is unmanaged is not polled and any trap that is generated by this interface is not used to determine the color of the OpenView map icon. By default, all device interfaces are marked as managed.

The following procedures describe how to place a device in a managed or unmanaged state.

▶ Procedure

To place a device interface in a managed state:

1. Open a Device Display window.
2. Click on a device interface.
3. Click on the Administer menu and select Managed.

▶ Procedure

To place a device interface in an unmanaged state:

1. Open a Device Display window.
2. Click on a device interface.
3. Click on the Administer menu and select Unmanaged.

Opening a Submap

An OpenView submap presents a view of your network. You can open the submap that is associated with the device you are viewing.

▶ Procedure

To display the submap associated with a device:

1. Open a Device Display window.
2. Click on the Administer menu and select Show Submap.

Resetting Devices and Cards

Resetting a device or card performs a warm start of that device or card remotely. The following procedures describe how to reset a device or card.

▶ Procedure

To reset a device:

1. Open a Device Display window.
2. Click on the Administer menu and select Reset Device.

A message dialog is opened and you must specify whether or not you want to continue the operation as service to the device is interrupted during a reset.

▶ Procedure

To reset a MCC or DSL card:

1. Open a Device Display for a DSLAM chassis.
2. Click on a MCC or DSL card within the Device Display.
3. Click on the Administer menu and select Reset Card.

   This option is also available from the pop-up menu. To access the pop-up menu, position the mouse over a card and press the right mouse button.

A message dialog is opened and you must specify whether or not you want to continue the operation as service to the card is interrupted during a reset.

Configuring Devices and Device Interfaces

4

Overview

By using the DCE Manager, you can perform various configuration operations, which include:

- Starting a Telnet session
- Displaying and setting select device parameters
- Storing multiple configuration images within a device's memory
- Adding, deleting, or modifying the Injection table (for 5446 devices only)
- Saving and restoring a configuration to and from a file

Before you set or change the configuration values of a known device or device interface, ensure that the Read/Write settings of the Community Names of the physical devices matches that of the Community Names configured in OpenView.

This chapter describes how to set Community Names and complete other configuration operations.

Setting Community Names

The Community Names of the physical device is set from the Front Panel of the device itself, or by issuing commands in a Telnet session.

To set the Read/Write Community Names of the device as configured in OpenView, you must use the SNMP Configuration dialog as described in the following procedure.

▶ Procedure

1. Click on the OpenView Options menu and select SNMP Configuration. The SNMP Configuration dialog appears.

2. Enter the Read Community Name and the Write Community Name in the Community and Set Community text input fields, respectively.
3. Click on OK to apply the changes and close the dialog.

For 8600, 8800, and 8810 devices, each DSL and MCC card contains its own SNMP agent; hence, the Community Names for each card must be set by using the instructions in this section.

For 5446 RTUs, the default Set Community Name is **private**, not public as it is with most devices.

Starting a Telnet Session

A Telnet session opens a separate terminal window, which you can use to access a devices' craft interface. From the craft interface, you can perform various operations on a device as documented in the user documentation for that device.

A Telnet session is started from a Device Display window or the OpenView submap. The following procedures describe how to start a Telnet session from either a Device Display or OpenView.

▶ Procedure

To start a Telnet session from the Device Display, use one of the following methods:

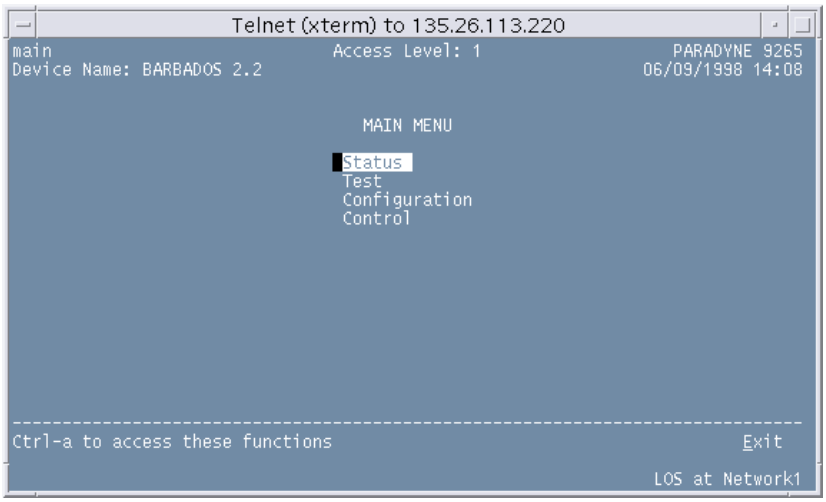
- Click on the Connect button located on the toolbar.
- Click on the Configuration menu and select Connect.

By default, a Telnet session that is started through the Device Display opens a **`dtterm`** terminal interface, which is included with the Common Desktop Environment (CDE). To change this default to an **`xterm`** terminal interface, edit the **`/opt/OV/att/attGEM/GEMDD.res`** file (or **`/usr/OV/att/attGEM/GEMDD.res`** file on AIX) and change the command parameter **`attGEMdd*dtterm`** to **`attGEMdd*xterm.`**

▶ Procedure

To initiate a Telnet session from an OpenView submap:

1. Select a device icon within an OpenView submap.
2. Click on the Misc menu and select Terminal Connection. A submenu is displayed.
3. Select Telnet from the submenu. The craft interface for the device you selected is displayed. For example, the following Telnet window is for a 9265 device.



Setting or Changing Configuration Options

You can display configuration options for most devices, device interfaces, and DLCIs. With the exception of DLCIs, you can also set certain configuration options. The following sections discuss how to:

- Display and set configuration options on a device
- Display and set configuration options a device interface
- Display configuration options for FrameSaver devices

Displaying and Setting Configuration Options on a Device

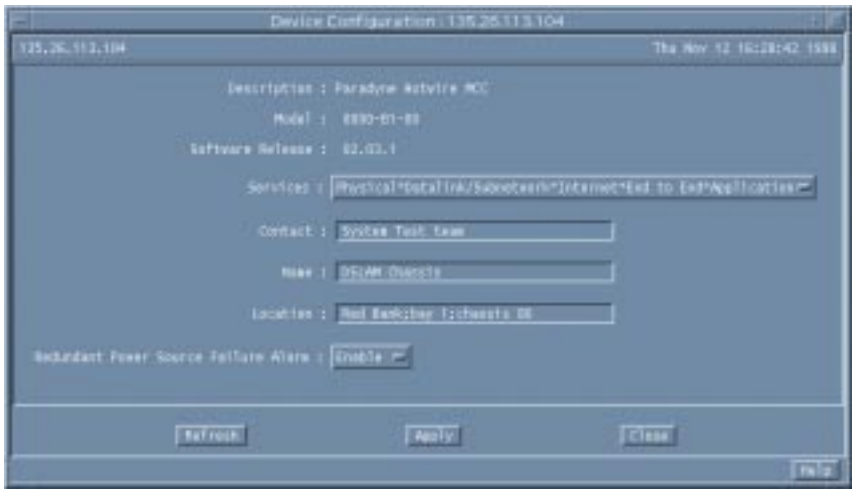
Configuration options provide a description of a device and the options displayed depends on the device. At a minimum, however, you can change the following:

- Contact person for the device
- Logical name attached to the device
- Physical location of the device

▶ Procedure

To set parameters for a device:

1. Open a Device Display.
2. Click on the Device Display Configuration menu and select Options. A Device Configuration dialog similar to the following appears.



3. Fill in fields as appropriate.
4. Click on the Redundant Power Source Failure Alarm button to enable (default) or disable this feature.
5. Click on Apply to set the parameters and close the dialog.

Setting or Changing Configuration Parameters on a Device Interface

To display and set configuration parameters for a device interface, use the Device Configuration dialog. Minimally, this dialog provides a description of the device interface, interface type, and speed of the interface in bits per second.

Depending on the type of device interface you are viewing, many other fields may be displayed such as bandwidth, datagram size, clock source, connect present, port type, and so on. You can modify some of these fields.

▶ Procedure

To set parameters for a device interface:

1. Open a Device Display.
2. Select a device interface from the Device Display.
3. Click on the Device Display Configuration menu and select Options. A Device Configuration dialog similar to the following appears.

4. Enter or select parameters as appropriate.
5. Click on Apply to set the parameters and close the dialog.

Displaying and Modifying DLCI Options on FrameSaver Devices

To display the current settings for DLCIs on FrameSaver devices, use the DLCI Configuration dialog.

▶ Procedure

To display or modify DLCI options:

1. Open the Device Display for a 912x or 962x.
2. Position the mouse over the Network DDS Frame Relay Server interface. A pop-up menu appears.
3. Select DLCI Options from the menu. A DLCI Configuration dialog similar to the following appears.

4. Modify the fields as appropriate.
5. Click on the Apply button.

NOTE:

Release 1 of the 9620 devices does not provide support for DLCIs through SNMP. If you have Release 1 of a 9620 device, while the DLCI Options menu item is selectable, the results rendered are not predictable.

Creating Injection Table Configurations for 5446 RTUs

The injection table specifies the address, mask, type and status of the service provider or host routes configured for 5446 RTUs as described in the following table.

Table 4-1. Parameter Descriptions

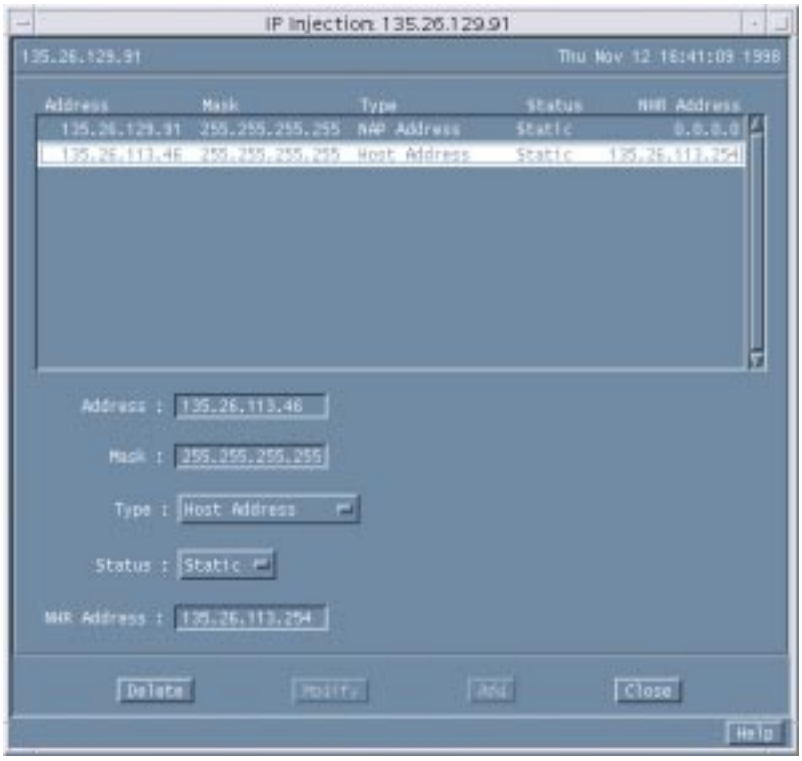
Parameter	Description
Address	Specifies the address of the Network Address Provider (NAP), Service Provider, Host Address, or Default Gateway for 5446 RTUs. The address format is Z.x.x.x where: ■ Z ≠ 0 and Z ≠ 127 ■ Z has to be < 224 if the address is a service provider address or < 240 if it is a Host Address.
Mask	Defines the subnet mask that corresponds to the address entry. The netmask has to be a left justified contiguous bitmask. The netmask cannot be 0.0.0.0.
Type	Specifies the category of the Address you selected, where categories include: Network Access Provider (NAP), Service Provider, Host Address, and Default Gateway.
Status	Indicates the state of the provider or host: ■ Static ■ Dynamic ■ Invalid Invalid means the Address is marked for deletion and the entry eventually disappears from the table.
Next Hop Router	Specifies the IP Address of the gateway. This field is available when the Type is set to Host Address only.

By using the IP Injection dialog, you can add, delete, or modify entries in the injection table for 5446 RTUs. However, by default, the injection table contains a single Network Access Provider (NAP) entry which cannot be removed or modified. All other entries must be added.

CAUTION:

When a NAP address on a 5446 RTU is changed by a push from 8600/8800 devices, all the injection table entries are deleted.

For 5446 RTUs, the default Community Name is **private**, not public as it is with most devices. Ensure that you have set the Community Name as described in the *Setting Community Names* on page 4-2, before adding or modifying the injection table.



Adding Entries to the Injection Table

The injection table can contain up to four service provider entries and up to 27 host routes for each 5446 RTU.

▶ Procedure

To add an entry:

1. Open a Device Display for a 5446 RTU.
2. Position the cursor over a DSL interface and press the right mouse button. A pop-up menu appears.
3. Select Injection Table from the pop-up menu. The IP Injection dialog appears.
4. Enter the Address and Mask in the appropriate text input fields in the dialog and select the Type and Status.
5. Click on the Add button.

Modifying the Injection Table

You can modify the address, mask, type, or status of an injection table entry.

▶ Procedure

To modify an injection table entry:

1. Open a Device Display for a 5446 RTU.
2. Position the cursor over a DSL interface and press the right mouse button. A pop-up menu appears.
3. Select Injection Table from the pop-up menu. The IP Injection dialog appears.
4. Click on the entry you want to modify.
5. Change the parameters as appropriate.
6. Click on the Modify button.

Deleting an Injection Table Entry

If an entry in the injection table is no longer valid, you can remove it from the table.

▶ Procedure

To delete an injection table entry:

1. Open a Device Display for a 5446 RTU.
2. Position the cursor over a DSL interface and press the right mouse button. A pop-up menu appears.
3. Select Injection Table from the pop-up menu. The IP Injection dialog appears.
4. Click on the entry you want to remove.
5. Click on the Delete button.

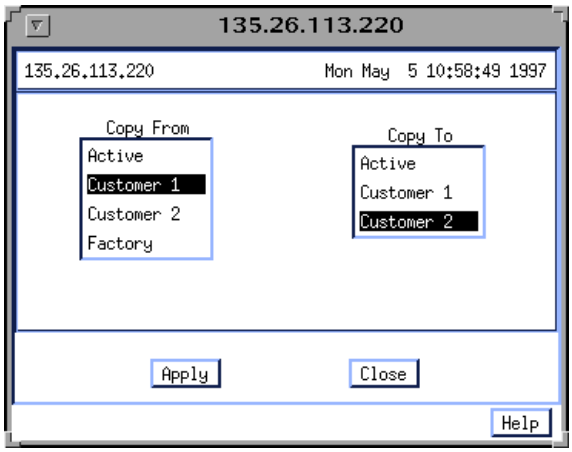
Copy Configuration

You can create a duplicate or modified image of a device configuration and store it within the configuration area of the device itself. This is useful if you want to restore an image or if you want to have multiple configurations available.

▶ Procedure

To create a copy of a configuration image:

1. Select a device of which you want multiple configuration images.
2. Click on the OpenView Configuration menu and select DCE Manager. The DCE Manager submenu appears.
3. Select Copy Configuration from the submenu. A Copy Device Configuration dialog similar to the following appears.



4. Select the configuration you want to duplicate from the Copy From display area.

   You have the option of copying the Active image, the Factory default image, or customized images stored in Customer 1 or Customer 2.

5. Select a destination for the image from the Copy To display area.

   If you copy an image to the Active image, you can cause the IP address within the device to be set to NULL. If this occurs, the address of the device must be reset from the front panel of the physical device.

6. Click on the Apply button.

Saving and Restoring Device Configuration Images

Device configurations set through the craft interface or the DCE Manager are stored in a configuration image on the device. Some devices support the transfer of a binary configuration image from a device to a UNIX file. This is referred to as **uploading**.

Conversely, a configuration image stored in a UNIX file can be transferred from the UNIX file back to the device of origin only. This is called **downloading**. Uploading and downloading provides a means of saving and recovering the configuration image should the image on a device become corrupt.

- For AAC devices only, you can transfer configuration images by using the DCE Manager Upload/Download dialog.
- For FrameSaver 9000 Series devices, the DCE Manager opens a FTP interface, which you can use to transfer the configuration image.

The following sections discuss how to use the DCE Manager to upload and download configuration images for AAC devices only. For information on uploading and downloading configuration images for the FrameSaver 9000 series devices, refer to the user documentation for those devices.

Uploading Configuration Images on AAC Devices

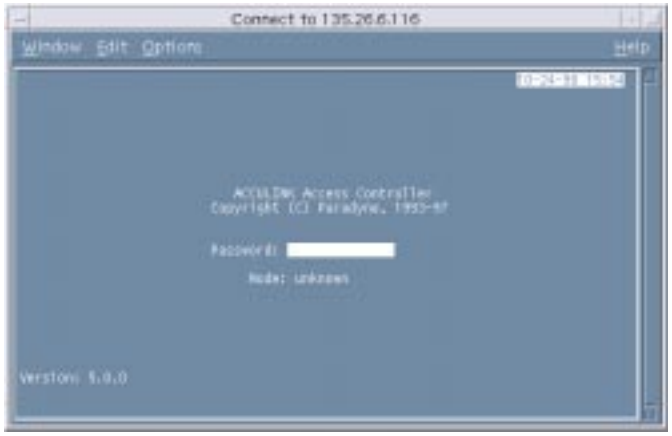
To upload a configuration image for an AAC device only, the DCE Manager opens a Telnet dialog and the Upload/Download dialog. By using these interfaces, you can save the configuration image of an AAC device to a UNIX file.

▶ Procedure

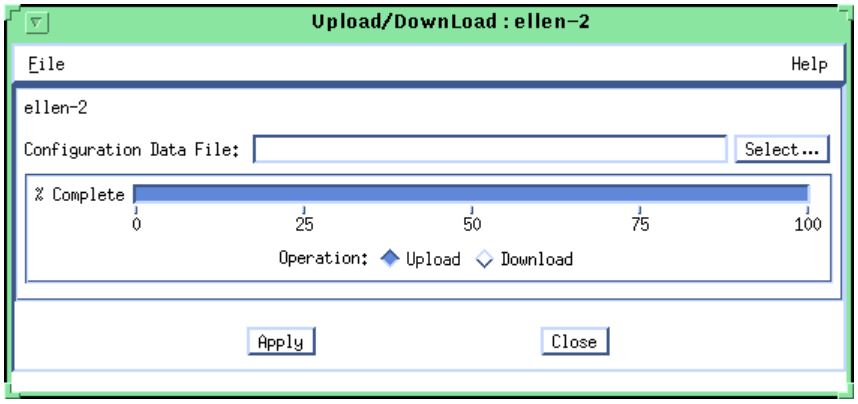
To upload a configuration image:

1. Select an AAC device in an OpenView submap.
2. Click on the OpenView Configuration menu and select DCE Manager. The DCE Manager submenu appears.
3. Select Upload/Download from the submenu. A Telnet dialog and an Upload/Download dialog appear.

4. Log into the Telnet dialog as either Superuser or Manager. You are then prompted to enter your password in a Telnet dialog similar to the following.



5. Enter the name of file in the Configuration Data File text input file in the Upload/Download dialog where the image is to be stored.



6. Select Upload from the Upload/Download dialog.
7. Click on the Apply button in the Upload/Download dialog.

   The gauge in the Upload/Download dialog displays the progress of the transfer as a percentage of the job that is complete. A message appears when the transfer is complete.

   The amount of time required to upload a configuration image from a device to a file varies depending on your network configuration and transmission speed.
8. Click on Close to exit the Upload/Download dialog.
9. Click on the Telnet dialog. If the transfer was successful, the following message appears:

   `Transfer is successful. Press any key to continue.`
10. Press Return and type **`l`** to exit the Telnet session.

Downloading Configuration Images

A configuration image from an AAC device that has been uploaded and stored in a UNIX file can be restored by performing a download operation.

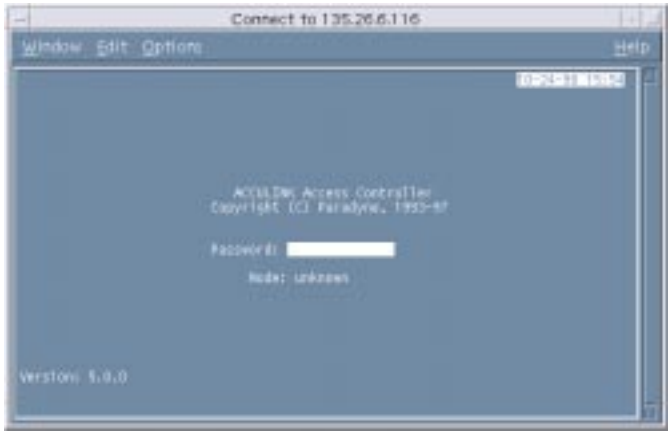
CAUTION:

A configuration image retains the IP address of the device from which it is uploaded. If you choose to download a configuration image to a device other than the one you uploaded from originally, you must change the IP address.

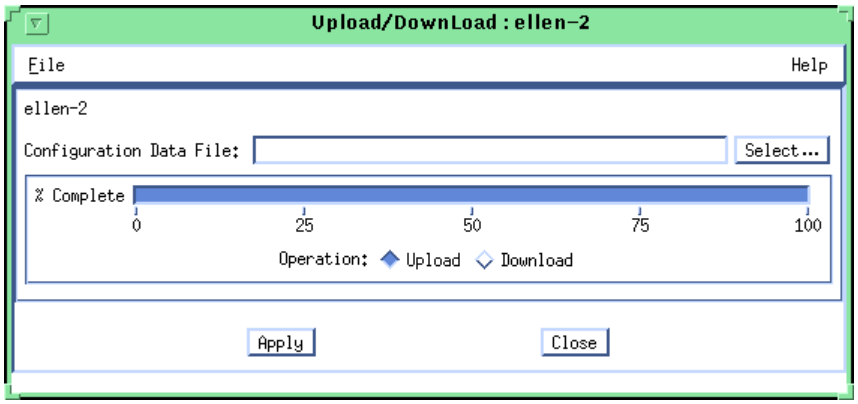
▶ Procedure

To restore a configuration image:

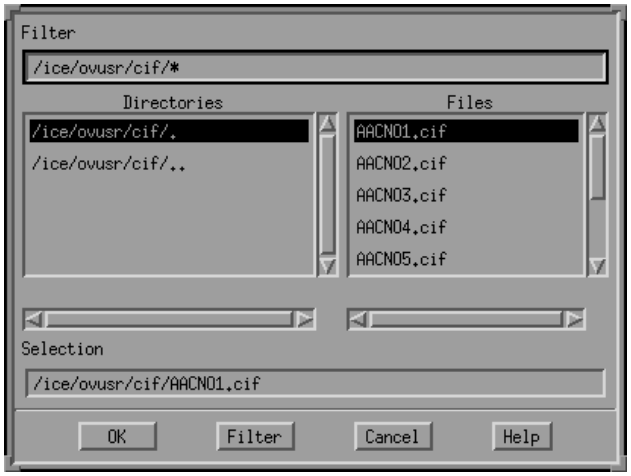
1. Select an AAC device in an OpenView submap.
2. Click on the OpenView Configuration menu and select DCE Manager. The DCE submenu appears.
3. Select Upload/Download from the DCE Manager submenu. A Telnet dialog and an Upload/Download dialog appear.
4. Enter the password for the device in a Telnet dialog similar to the following:



5. Click on the Select button in the Upload/Download dialog to search for a configuration image to download.



6. Select a file from the File Selector dialog, then click on OK.



NOTE:

You must not select a configuration image file that was uploaded from another device. Each configuration image contains information and options specific to the particular device from which the configuration image was transferred.

7. Click on Download in the Upload/Download dialog.
8. Click on the Apply button in the Upload/Download dialog.

   The gauge in the Upload/Download dialog displays the progress of the transfer as a percentage of the job that is complete. A message appears when the transfer is complete.

   The amount of time required to upload a configuration image from a device to a file varies depending on your network configuration and transmission speed.

9. Click on Close to close the Upload/Download dialog.
10. Click on the Telnet dialog. If the transfer was successful, the following message appears:

    ```
    Transfer is successful. Press any key to continue.
    ```

11. Press Return. You are prompted to reboot the system as follows:

    ```
    A reboot is required to activate the new
    configuration.
    OK to reboot the system (y/n)?
    ```

    Enter **y** to download the configuration image and reset the device.

Monitoring Devices

5

Overview

You can both identify and obtain status of devices and device interfaces using features of the DCE Manager. Specifically, you can:

- Monitor devices and device interfaces through the use of color-coded icons
- Use the OpenView event log to view categories of events
- Obtain a description of a device or device interface
- Display detailed status on a device or device interface

This chapter discusses these options in more detail.

Using Color to Obtain Status

Both the device icons displayed in an OpenView map and the device interface icons within a Device Display use color to indicate the state of the device or device interface. The following sections discuss this in more detail.

Obtaining Device Status through Color

Within the OpenView submaps, the color used for DCE Manager device icons is derived from the standard OpenView colors, which indicate the alarm state of a device. The following table lists the colors used and defines the associated alarm state. You can change these colors as described in the OpenView user documentation.

Table 5-1. DCE Manager Device Icon Status Colors

Color	State
Salmon	In test.
Red	**Critical Alarm:** The device is not operating or performance is severely degraded.
Orange	**Major Alarm:** A serious problem exists, and performance is likely to be degraded.
Yellow	**Minor Alarm:** A problem exists; however, performance should not be degraded.
Cyan	**Warning/Informational Alarm:** A problem exists that could cause a problem in the future.
Green	**Normal:** The device, its cards, and interfaces are functioning properly.
Blue	**Unknown.** The status of the device is not known currently.

The color of a device icon within the OpenView maps reflects its last known state (for example, the highest severity alarm). To ensure that you are viewing the highest severity alarm state for the within an OpenView map, use the following procedure.

▶ Procedure

To propagate the alarm state, perform these steps from within the OpenView application:

1. Click on the Map menu and select Maps. The Maps submenu appears.
2. Select Describe/Modify from the submenu. The Map Description dialog appears.
3. Select Propagate Most Critical from the Compound Status list.
4. Select IP Map from the Configurable Applications list.
5. Press the Configure for this Map... button. The IP Map Configuration dialog appears.
6. Set Should status of nodes be IP/IPX only? to False.
7. Click OK to apply the changes and close the dialogs for Map Description and IP Map Configuration.

To complete alarm synchronization, reset the device as described in *Resetting Devices and Cards* in Chapter 3, *Administering Devices*.

Obtaining Device Interface Status through Color

The DCE Manager Device Display dialog presents a visual view of the rear of a device. The color of each interface on the device shows the last known operational and administrative state of each interface. Table 5-2 lists and describes the use of each color.

Table 5-2. DCE Manager Device Interface Status Colors

Color	State
Off-white	**Unmanaged:** The user has put the interface in an unmanaged state (using the Device Display menu selection *Administer→Unmanage*). Interfaces will also be in the unmanaged state if the user has placed the entire device in an unmanaged state (using the OpenView *Map→Unmanage Objects* menu item). Unmanaged takes precedence over all other states.
Blue	**Unknown:** The status of the interface is unknown. Unknown takes precedence over Administratively Down, In Test, Down, and Up states.
Dark Brown	**Administratively Down:** The interface is in the administratively down state. Administratively Down takes precedence over In Test, Down, and Up states. (The color used for this state may make an interface appear black on some workstations.)
Salmon	**In Test:** The interface is in test mode. In Test takes precedence over Down and Up.
Red	**Down:** The interface is not operating or performance is severely degraded. Down takes precedence over Up.
Green	**Up:** The interface is functioning properly.

You can change these colors as described in the *HP OpenView User's Guide* or by modifying the colors listed in the **`/opt/OV/att/attGEM/GEMDD.res`** file (or the **`/opt/OV/att/attGEM/GEMDD.res`** file on AIX systems).

The DCE Manager checks the state of an interface every one (1) minute by default. You can change this interval as described in *Polling Devices* in Chapter 3, *Administering Devices*.

Monitoring Devices Using the OpenView Event Log

When OpenView is started, an Event Categories dialog appears. The Event Categories dialog reads the OpenView Event Log and organizes all alarms/events into six groups. By selecting one of the Event Categories, you can open an Event Browser dialog for that group.

The following sections discuss:

- Using the OpenView Event Browser Dialog
- Mapping DCE Manager Alarm/Events within OpenView
- Understanding Paradyne Event/Alarm Log Formats
- Handling Proxy Address Resolution Protocol (ARP)

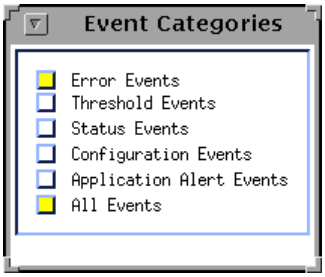
Using the OpenView Event Browser Dialog

When an alarm or event is received from a device, the OpenView Event Log is updated. You can access the Event Log by selecting a group from the OpenView Event Categories dialog using the following procedure.

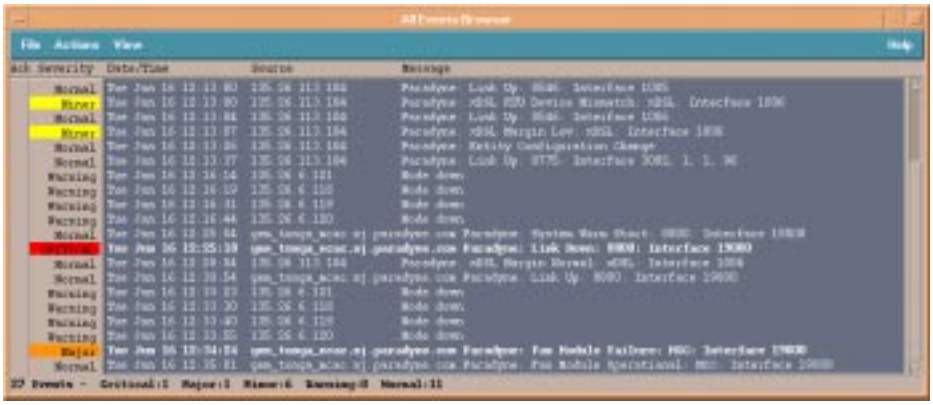
▶ Procedure

To open an Event Browser dialog from the OpenView Event Categories dialog:

1. Determine the category of alarms/events you want to view.
2. Position the mouse over the category and press the right mouse button. The Event Browser dialog for that category appears.



For example, if All Events is selected from the Events Categories dialog, an Event Browser dialog similar to the following appears:



Each entry within the Event Browser dialog presents the following information:

- Severity of the alarm or event, where color indicates severity level:

  Normal – Green

  Warning – Cyan

  Minor – Yellow

  Major – Orange

  Critical – Red

- Date and time of the alarm or event
- Name of the network element where the alarm or event originated
- Description of the alarm or event

Because devices have alarms and events that differ from those of OpenView, the DCE Manager provides its own mapping for alarm and events. See *Mapping DCE Manager Alarms and Events within OpenView* on page 5-6 and *Understanding Paradyne Formats Used in the Event Browser Dialog* on page 5-7 for more information.

When an alarm is received from a device, the status color of a device icon in the OpenView submap is also updated as described in *Obtaining Device Status through Color* on page 5-2.

NOTE:

Problem: Occasionally, a rare condition is encountered within the DCE Manager when a new device or card is added to the network. This occurs when a device or card that has been configured properly is not discovered by the DCE Manager and a SNMP trap event is issued that generates an Event Log entry. The entry that is generated may not reflect the true severity level (color) for the device or card on the IP Status Map. Propagation of the correct status color to the submap device icons is also affected.

Workaround: If the device is discovered by the DCE Manager software and it is displayed on the IP Status Map, the severity status color can be synchronized by resetting the device or card as described in *Resetting Devices and DSL Cards* in Chapter 3, *Administering Devices*.

Mapping DCE Manager Alarms and Events within OpenView

Devices have alarm and event categories that differ from those used by OpenView. Thus, the DCE Manager provides its own mapping as described in Table 5-3 for some of the most common alarm and events.

Table 5-3. Some Common Device Alarm/Event Categories

Device Alarm/Event Category	OpenView Alarm/Event Category
Cold Start	Warning
Warm Start	Normal
Link Down*	Critical
Link Up*	Normal
Authentication Failure	Warning
Clock Failure	Critical
Self-Test Failure	Critical
Device Failure	Critical
Configuration Change Notification	Normal
Test Start* (appears as salmon on the interface)	Warning
Test Clear*	Normal
*Designates an alarm.	

▶ Procedure

To change the default mapping of states to the colors (used in the OpenView Event Browser), use the following general steps:

1. Start OpenView.
2. Click on the Options menu and select Event Configuration.
3. Set the options as described in the OpenView user documentation.
4. Exit and restart OpenView to have the new options take effect.

The DCE Manager Device Display *Help →On Legend* menu lists the meaning of the various status colors.

NOTE:

Alarms change the color of a device symbol, while events do not. The alarms and events specified in the previous table may not correspond to older Paradyne Model 3xxx and AAC device families.

Understanding Paradyne Formats Used in the Event Browser Dialog

The Message column of the OpenView (or NetView) Event Browser dialog displays a consistent format for SNMP traps for all Paradyne devices, with one exception (described later). The Message column displays from 2 to 4 fields of information separated by a colon (:).

The format is as follows:

Paradyne: *Event Type*
Paradyne: *Event Type: Device Type*
Paradyne*: Event Type: Device Type: Device-Specific Information*

Using the above formats, a series of events could appear as follows:

```
Paradyne: Entity Configuration Change
Paradyne: Authentication Failure: 9124
Paradyne: Test Start: 9124: Interface 10, 1, 3, 32, 1
```

The fields are defined as follows:

- *Paradyne* indicates that the trap originates from a Paradyne device.
- *Event Type* specifies the kind of trap that the device generated.
- *Device Type* indicates the model of the Paradyne device that generated the trap. If the model has a value of MCC, this refers to the 8000 Management Control Card (MCC) of a DSLAM Model 8600, 8800, or 8810.
- *Device-Specific Information* provides-additional information on the parameters associated with the trap. Typically, the first parameter displays the interface index, which is a decimal number of the form SSIII, where SS represents the slot number in a chassis (if applicable) and III represents the affected interface.

  See the SNMP trap section of the devices' User Manual for more information on parameters.

  To keep the Message column readable, the number of parameters displayed is limited. If the number of parameters is less than the limit, the following information, which is informational only, is returned in the *Device-Specific Information* field.

  — For HP OpenView:

  ```
  (UNAVAILABLE EVENT PARAMETER $6)
  ```

  — For NetView:

  ```
  FMT ERROR: accessing element #6, only 5 available
  ```

If an incorrect entity MIB trap OID is detected, the Message column can contain an additional field as stated earlier. This is indicated by the following entry:

```
Paradyne: Incorrect Entity MIB Trap OID: Device–Specific
Information
```

Handling Proxy Address Resolution Protocol (ARP) for DSL Cards

When configuring a Hotwire DSLAM system, the user can choose to have the DSL cards Proxy ARP for the remote 5446 Remote Termination Units (RTUs). This configuration is attractive in large networks because it simplifies the configuration needed on the router. In certain network configurations however, the use of Proxy ARP on the DSL cards causes OpenView to log a major event. This occurs when OpenView or NetView receives the same IP address from two different MAC addresses.

By default, the OpenView system logs and displays all events. However, the user can filter out certain events. This is desirable, because it prevents the Event Browser dialog from becoming bogged with extraneous error messages.

To filter out these events, see the subject *Filtering Events* in the OpenView or Netview user documentation.

Obtaining the Identity of Devices and Interfaces

When you request an identity for a device or device interface, a description is displayed, which include information such as the model number, device or interface up time, physical location of the device, and so forth.

The procedures that follow describe how to:

- Obtain the identity of a device from OpenView
- Obtain the identity of a device from the Device Display
- Obtain the identity of MCC, DSL, and NAM cards from the Device Display
- Obtain the identity of endpoints connected to a DSL interface from the Device Display

▶ Procedure

To obtain the identity of a device from within OpenView:

1. Display an OpenView submap.
2. Click on the device you want to identify.
3. Click on the Fault menu and select DCE Manager. The DCE Manager submenu opens.
4. Select Identity from the DCE Manager submenu. A Device Identity dialog appears.

   The information displayed in the dialog varies depending on the device type you selected. The following examples shows the identity of a FrameSaver SLV 9124 device.

▶ Procedure

To obtain identity of a device from within a Device Display:

1. Open a Device Display.
2. Click on the Diagnose menu and select Identity. The Device Identity dialog for the selected device appears.

   As in the previous example, the information that is displayed is specific to the device you selected.

▶ Procedure

To obtain the identity of a card:

1. Open a Device Display.

   The Device Display representation of the 916x and 926x devices display a NAM card, which supports the Identity component. Likewise, the Device Display for a DSLAM chassis displays the MCC card and DSL cards, which support the Identity component also.

2. Position the mouse over the card you want to examine and press the right mouse button. A pop-up menu appears.

3. Select Identity from the pop-up menu. A Device Identity dialog appears.

   The following example displays the identity for an MCC card.

▶ Procedure

To obtain the identity of an endpoint connected to the DSL interface:

1. Open a Device Display for the DSLAM Chassis.

2. Position the mouse over a DSL interface and click on the right mouse button. A pop-up menu is displayed.

3. Select Remote Device Identity from the pop-up menu. A dialog similar to the following appears.

Obtaining the Status of Devices and Interfaces

When you request status on a device or device interface, operational status is displayed always and, depending on the type of device you selected, administrative status can also be displayed. A status request at the DSL or NAM card level provides the operational status of each port on a card.

You can obtain status information on a device from within OpenView or a Device Display. To obtain status information on a device interface or card, you must use a Device Display.

The following procedures describe how to:

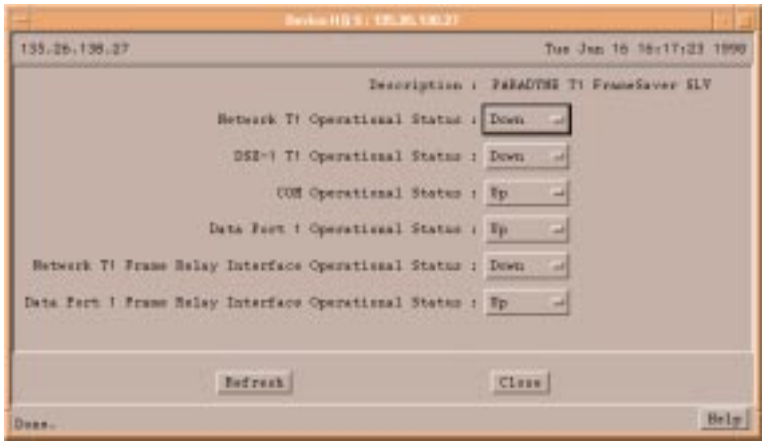
- Obtain administrative and operational status on a device from OpenView
- Obtain administrative and operation status on a device interface
- Obtain operational status at the DSL or NAM card level

▶ Procedure

To obtain the state of a device from within OpenView:

1. Display an OpenView submap.
2. Click on the device you want to examine.
3. Click on the Fault menu and select DCE Manager. The DCE Manager submenu appears.
4. Select Status from the DCE Manager submenu. The Device H & S dialog appears, where H & S represents Health and Status.

   The information in the dialog varies depending on the device type you selected.



▶ Procedure

To obtain status on a device from within a Device Display:

1. Open a Device Display.
2. Click on the Diagnose menu and select Status, or press the Status button on the toolbar.

   A Device H & S dialog is displayed, where H & S represents Health and Status.

▶ Procedure

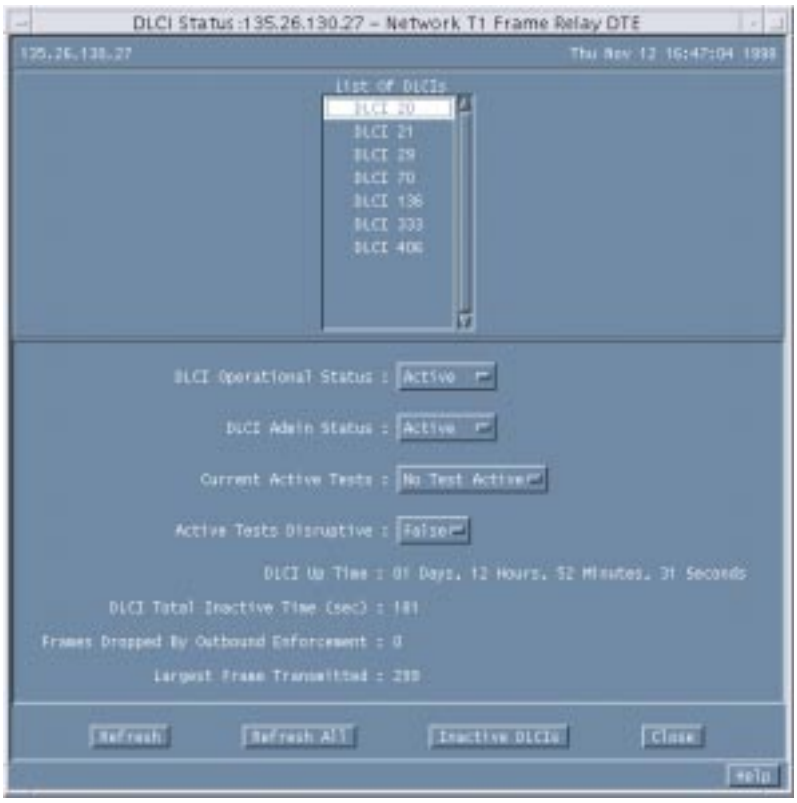
To obtain status on a device interface:

1. Open a Device Display.
2. Position the mouse over the device interface you want to examine and press the right mouse button. A pop-up menu appears.
3. Select Status from the pop-up menu. A Status dialog appears.

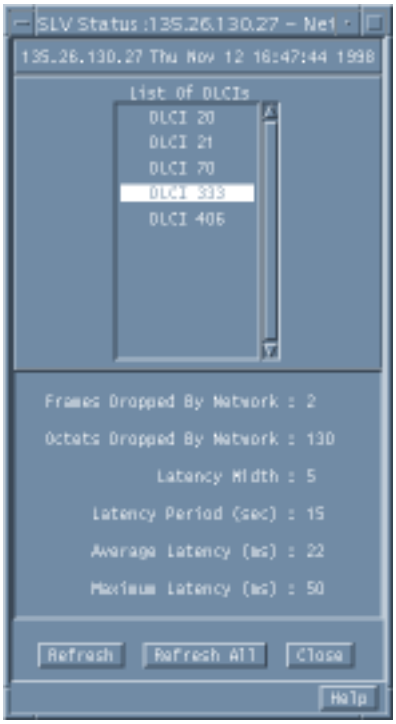
   This option is available from both the Diagnose menu and toolbar also. The Diagnose menu and pop-up menus may offer *DLCI Status, SLV Status, VP/VC Status,* and *VP/VC SLV Status*, depending on the type of FrameSaver device you selected.

   See *Components Available from the Device Display Menus* in Chapter 2, *Using the DCE Manager*, for more information.

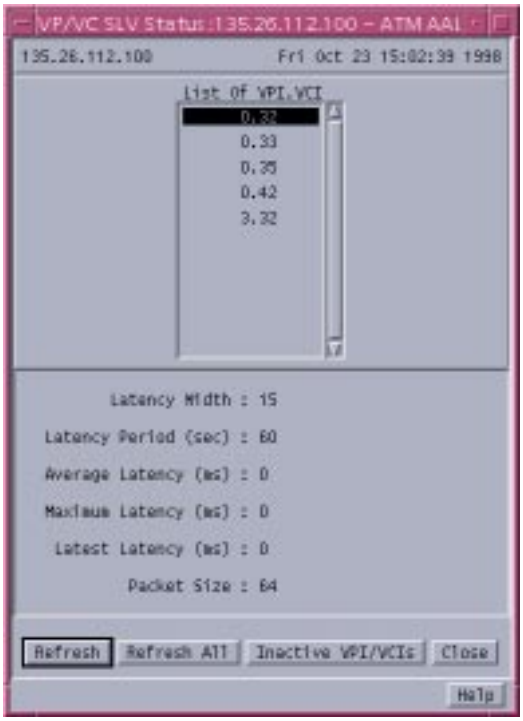
   The following is an example of a DLCI Status dialog:



The following is an example of an SLV Status dialog:



The following is an example of a VP/VC SLV Status dialog:



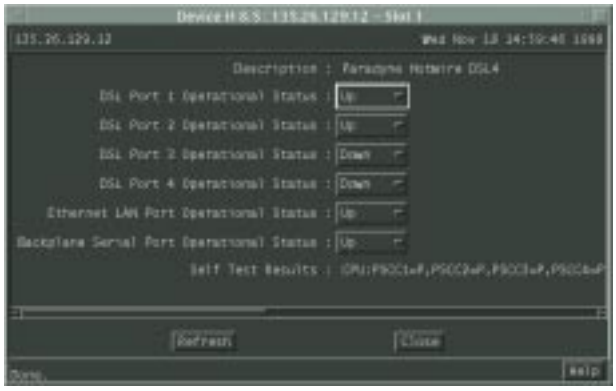
▶ Procedure

To obtain status on the MCC, DSL, or NAM card:

1. Open a Device Display that contains the MCC, DSL, or NAM card.
2. Press the right mouse button over the MCC, DSL, or NAM card. A pop-up menu appears.

   You can select this option from both the Diagnose menu and toolbar also.
3. Select Status from the pop-up menu. A Status dialog appears.

   The following example shows Health and Status for DSL card.



Using the Lamp Test

A Lamp Test causes the front panel lights on a device to blink on and off. This enables a service person to easily locate the device in a rack full of equipment. This option is available for all devices that support Lamp Test operations under SNMP control.

The following procedures describe how to enable and disable a Lamp Test.

▶ Procedure

To enable a Lamp Test:

1. Open a Device Display.
2. Click on the Diagnose menu and select Lamp Test Start.

▶ Procedure

To disable a Lamp Test:

1. Open a Device Display.
2. Click on the Diagnose menu and select Lamp Test Stop.

Some devices have a timer that terminates a Lamp Test automatically. For more information, see the Device User Manual.

Monitoring Interface Status on AAC Devices

A size limit has been implemented on the number of SNMP requests that can be sent to an ACC device. This size limit varies depending on the firmware revision and the network connectivity of the AAC device. The DCE Manager Device Display has a default limit set on the number of interface status requests that can be sent to an ACC device in a single SNMP request. The default limit is 5.

You can change this default by modifying the **`attGEMdd*pduSize`** parameter in the **`/opt/OV/att/attGEM/GEMDD.res`** configuration file (or the **`/usr/OV/att/attGEM/GEMDD.res`** configuration file on AIX systems). Setting the value too low causes a high number of SNMP requests to be sent to the device. Setting the value too high can cause the AAC device not to respond to status polls. If the interfaces on the AAC device display remain in the blue “unknown” state the user should reduce the value of the **`attGEMdd*pduSize`** parameter, or unmanage one or more of the interfaces that are in an “unknown” state.

Performing Loopback Modes and Pattern Tests

6

Overview

Loopback modes and pattern tests check the integrity and performance of network devices and, to some extent, the network itself. This chapter describes how to:

- Isolate device problems
- Use loopback modes
- Use pattern tests
- Run tests

Isolating Device Problems

There are several ways that you are notified of problems with a device, and several methods you can use to resolve it. The following sections offer information that you can use to both diagnose and manage problems that you encounter.

Determining the Type of Problems

The following table highlights some of the more common problems you can encounter when working with devices.

Table 6-1. Device Troubleshooting Table

Notification	Problem	Go To . . .
OpenView submap displays a device symbol in blue (unknown).	Connection between management system and device has been lost.	*Diagnosing Problems with the Management Link* on page 6-3
OpenView submap displays a device symbol in red.	One of the device interfaces is in an alarm state.	*Diagnosing Problems with the Device or Line* on page 6-3
The OpenView Event Categories display reports that a trap has been received. If the trap is **linkDown**, indicating that one of the interfaces is not functioning: ■ The Device Display shows the interface symbol in red, and ■ The OpenView submap displays the device symbol in red.	Device has sent a trap to the DCE Manager.	Device manual for a description of the alarm
The status fields of a health and status dialog report an interface as **down**. ■ The Device Display shows the interface symbol in red, and ■ The OpenView submap displays the device symbol in red.	Interface is not operational.	*Diagnosing Problems with the Device or Line* on page 6-3
The Line Status field of the 3100 or 3300 status dialogs reports a problem. Or, the DDS Status field of the 9621 status dialog reports a problem. ■ The Device Display shows the interface symbol in red, and ■ The OpenView submap displays the device symbol in red.	Interface has experienced degradation of performance.	*Diagnosing Problems with the Device or Line* on page 6-3
DCE Manager Test dialog reports the test result **`No Sync`** or **`In Sync with Bit Errors`**.	Test run on an interface has failed.	*Diagnosing Problems with the Device or Line* on page 6-3

Diagnosing Problems with the Management Link

You can manage a device from OpenView through an Ethernet, leased-line, or dial-up connection. If the management connection is lost to a functional (green) device, the device symbol that is displayed on the OpenView submap turns blue and the line connected to it turns red. The colors of the interface symbols on the Device Display correspond to their last known states. An unknown (blue) state may be the norm if you are managing a device only periodically over a dial-up connection.

Without a management connection to the device, diagnosis using the DCE Manager is impossible. Therefore, you should perform an on-site test of the device to determine whether the problem is in the device or in the line. The individual device manuals provide a troubleshooting section that describes how to diagnose problems. The device manuals also describe how to run the device self-test.

It may be possible to test the device using the device's terminal interface, which is accessible through a Telnet connection. Refer to the individual device manuals.

See *Diagnosing Problems with Device or Line* below.

Diagnosing Problems with the Device or Line

When the DCE Manager detects that one of the device interfaces is in a **down** (or alarm) state, the following symbols turn red:

- Interface symbol on the Device Display
- Device symbol that is displayed on the OpenView submap

This state is reflected in the Operational Status field of the appropriate Health and Status dialog. Using the DCE Manager, you can place these interfaces in loopback mode and run pattern tests to help you isolate the problem.

When you are notified of a problem with a particular interface, try to determine whether or not the failure resulted from a problem with any of the following:

- The device itself
- Line
- Remote device

The sections that follow describe how you can use the loopback modes in combination with the pattern tests to do this. If you isolate a failure to a device, you may want to run the device self-test, as described in the troubleshooting section of some device manuals. If you isolate a failure to the network or to a device not supported by the DCE Manager, contact the network administrator or refer to the device manual.

Using Loopback Modes

The following sections discuss the various type of loopback modes available and describes how to use each. Although only DCE Manager supported devices are used in the following examples, the loopback modes and pattern tests are defined in MIBs.

Line Loopback

The Line Loopback (LLB) mode loops the information received on the Network T1 interface back to the network as close to the network interface as possible. When used with a pattern test, this loopback mode is useful for determining whether the problem is with the sending device or the T1 facility. The figure below illustrates how you can use the LLB in conjunction with a pattern test (see *Using Pattern Tests* on page 6-11) to isolate a problem.

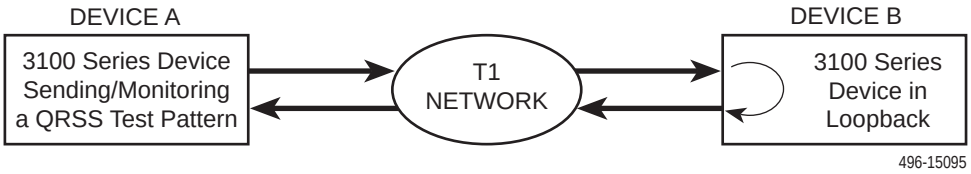
Note that while an interface is in loopback mode, the other interfaces send all 1's.

In the following figure, Device A is sending a known QRSS pattern out the Network T1 interface. (Device A sends a QRSS pattern when you select Send QRSS Pattern.)

Device B is in LLB mode returning the pattern. (Device B is put in LLB mode locally or by sending it an LLB Up Code from Device A.)

Device A monitors the returned information for errors. (Device A is put in monitor mode by selecting Monitor QRSS Pattern.) If Device A detects an error, it reports the error in the DCE Manager test dialog as **In Sync With Bit Errors** (device is marginal) or **Not in Sync** (device is down).

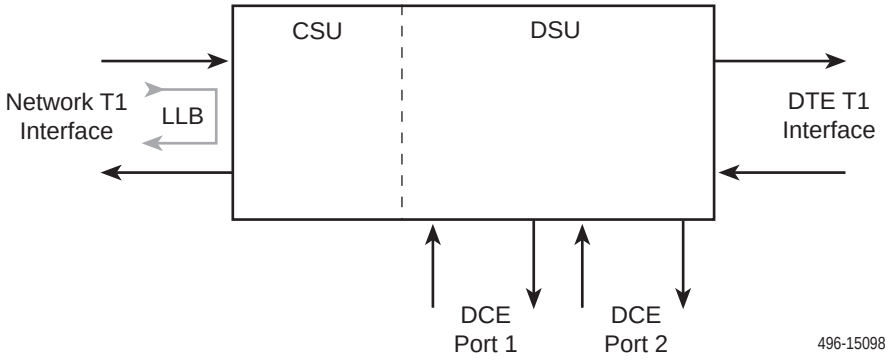
If Device A detects an error, the likelihood is that the problem is in the T1 facility and not within any internal circuitry of Device A because it was able to send and monitor the pattern data. If there are no errors reported, you can run the Payload Loopback test described in *Payload Loopback*, on page 6-5, to determine whether the problem is caused by the CSU circuitry of the remote device (Device B in our example).



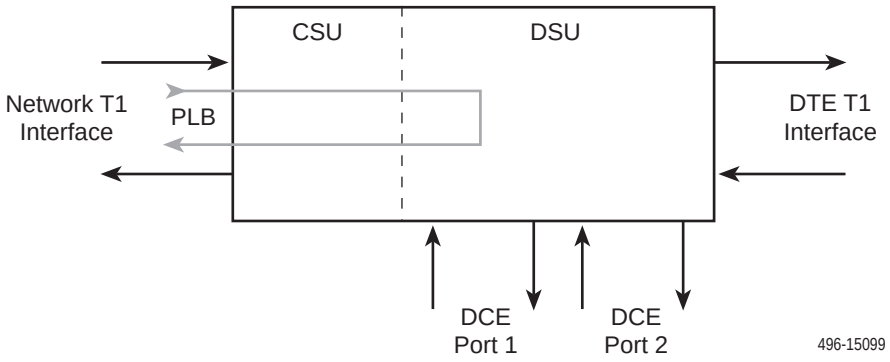
Loopback Mode (LLB) Combined with a Pattern Test

Payload Loopback

The Payload Loopback (PLB) mode loops the information received on the Network T1 interface back to the network after it has passed through the receive and transmit framing section (i.e., the CSU) of the DSU/CSU. This loopback is useful for determining whether the problem is with the T1 facility or in the circuitry of the remote device. Building on the previous example used in *Line Loopback*, if Device A does not detect an error as a result of a LLB test, but does detect an error as a result of a PLB test, the likelihood is that the error is in Device B. Compare Line Loopback (LLB) with Payload Loopback (PLB).



Line Loopback (LLB)



Payload Loopback (PLB)

Connectivity Tests (PVCs Only)

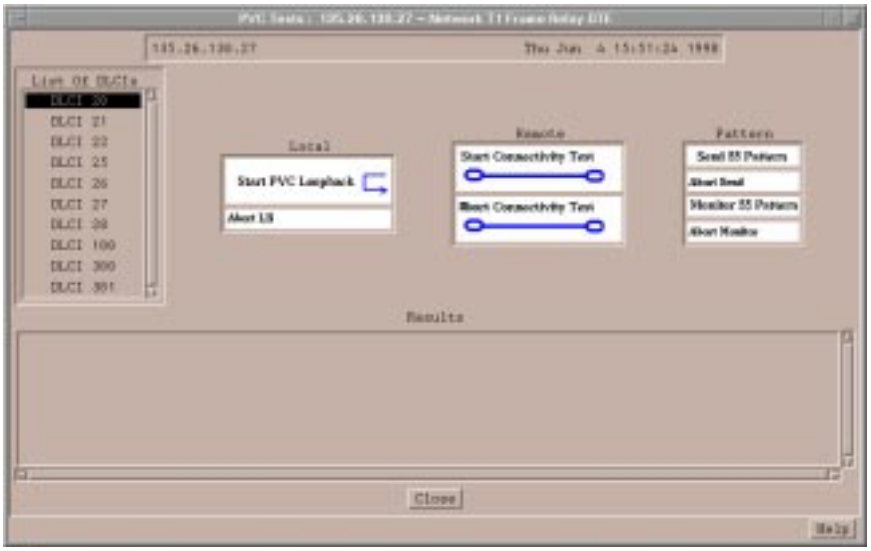
The Connectivity Test is a PVC loopback test, which is unique to 962x and 912x devices only. Other available tests devices are described throughout the chapter.

▶ Procedure

To open the dialog for PVC loopback tests on 962x and 912x devices:

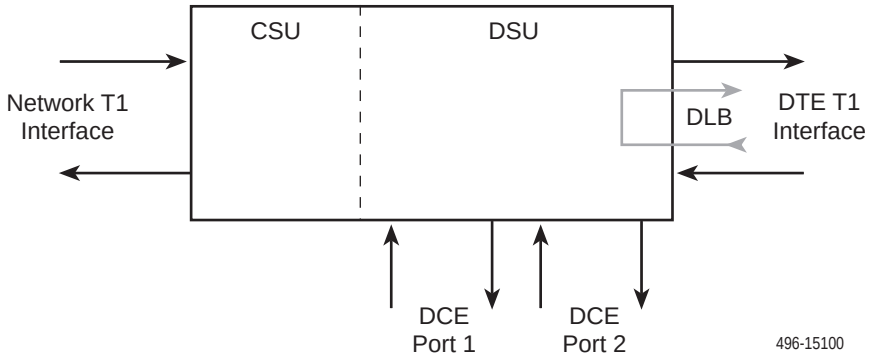
1. Open a Device Display for a 962x or 912x device.
2. Position the cursor over an active interface and press the right mouse button. A pop-up menu appears.
3. Select PVC Tests from the pop-up menu. The PVC Tests dialog appears.

   You can select a DLCI from the scroll list, followed by a test type. Test results are posted in the Results message box.



DTE Loopback

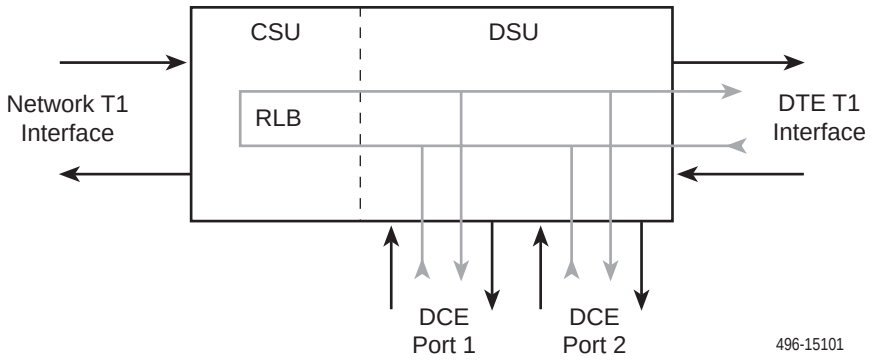
The DTE Loopback (DLB) performs an equivalent function on the DTE T1 interface that the LLB does on the Network T1 interface (see the figure below). It is useful for isolating problems on the DTE T1 line. For the DLB, a DTE device or test equipment must generate data to be looped back.



DTE Loopback (DLB)

Repeater Loopback

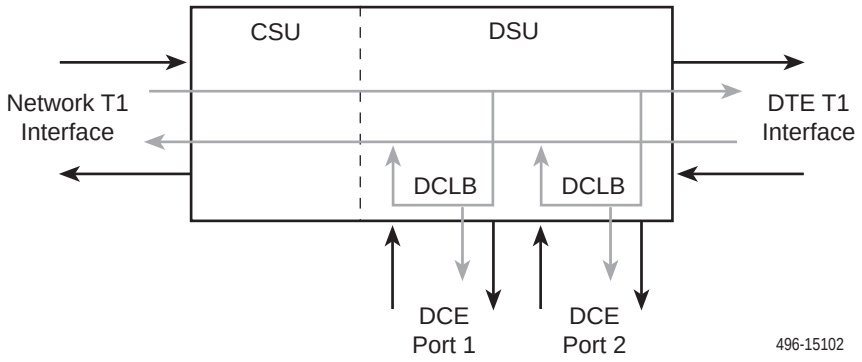
The Repeater Loopback (RLB) performs an equivalent function to the PLB on the Network T1 interface (see the figure below). The exception is that the RLB loops the entire T1 data stream, which includes the data on the DTE T1 interface as well as the synchronous data ports. The RLB is useful for ensuring that all of the customer's information is correct up to the point it is sent out the Network T1 interface (which helps indicate that the DSU/CSU is operational). For the RLB, a DTE device or test equipment must generate data to be looped back.



Repeater Loopback (RLB)

Data Channel Loopback

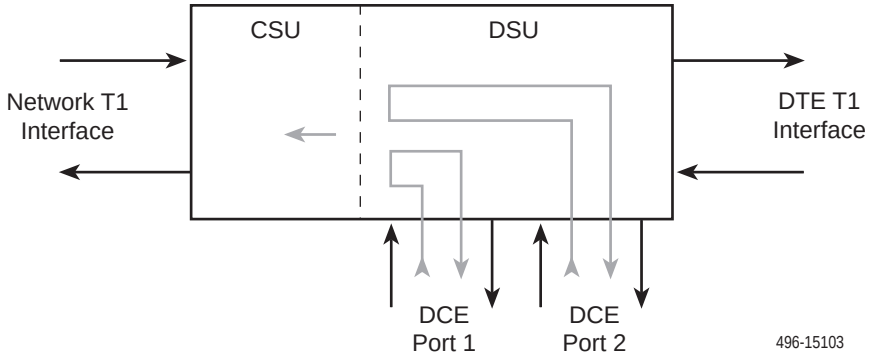
The Data Channel Loopback (DCLB) loops the data for a particular synchronous data port back to the network interface after the information has passed all the way through the DSU/CSU (i.e., just before it is sent to the customer's equipment, either through the Network T1 interface or the DTE T1 interface, see the figure below). It is useful for verifying the end-to-end integrity of a circuit for a particular interface.



Data Channel Loopback (DCLB) – V.54, Loop 2

Data Terminal Loopback

The Data Terminal Loopback (DTLB) loops the data for a particular synchronous data port back to the interface just before it is combined with the rest of the T1 data stream (see the figure below). It is useful for both isolating errors to the DTE equipment connected to the DSU/CSU and ensuring that the data for the interface is being received/transmitted correctly by the DSU/CSU.



Data Terminal Loopback (DTLB) – V.54, Loop 3

As described in *Using Loopback Modes* on page 6-4 and *Using Pattern Tests* on page 6-11, the remote loopback Send V.54 Up Code and Send FT1 Up Code put a remote device in loopback mode, while Send V.54 Down Code and Send FT1 Down Code take a remote device out of loopback mode. You can use these codes in troubleshooting, as described in *Using Pattern Tests* on page 6-11.

Use of the Loopback Up Codes and Down Codes

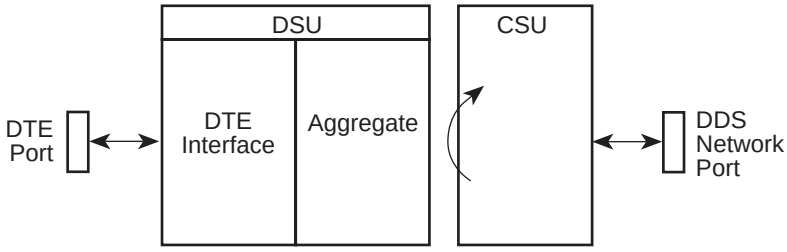
The remote loopback up codes (which put a remote device in loopback mode) and down codes (which take a remote device out of loopback mode) are in-band codes that allow remote control of a device. The loopback modes, as well as the pattern tests, are defined in MIBs, and so any device that supports the appropriate MIBs is able to go into loopback mode and send/monitor pattern tests. The LLB up code invokes an LLB in the remote unit while the LLB down code terminates the remote LLB. The Send V.54 Up/Down and FT1 Up/Down perform a similar function, but are only sent on the DS0s associated with a particular data port and will control the remote operation of the DCLB Loopback.

The up and down codes are useful for performing tests from one end of a circuit. The following example illustrates the use of the codes. You would:

1. Send an LLB up code from the local device to a remote DSU/CSU. The remote DSU/CSU goes into line loopback.
2. Send a QRSS pattern test from the local device. The remote DSU/CSU will return the QRSS pattern (because it is in loopback mode).
3. Start a monitor QRSS pattern test in the local 3100 Series device and monitor the result to determine whether the circuit is operational (**In Sync**), marginal (**In Sync With Bit Errors**), or completely down (**Not in Sync**). (The test dialog described in *Running Tests* on page 6-12 reports the results of the pattern test.)
4. Terminate sending and monitoring the QRSS pattern tests.
5. Send LLB down code from the local device to the remote DSU/CSU. Remote DSU/CSU terminates the line loopback.

CSU or External Network Loopback

CSU loopback is an external loopback that is located as close as possible to the network interface (see figure below).

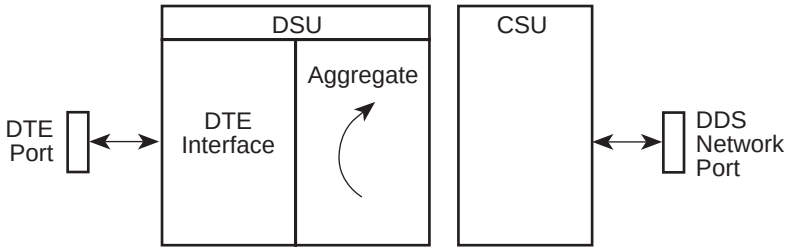


DDS Leased-Line Access Unit

496-14929

DSU or Internal Network Loopback

DSU loopback is an Internal loopback that is located as close as possible to the customer interface serving the DTE (see figure below).

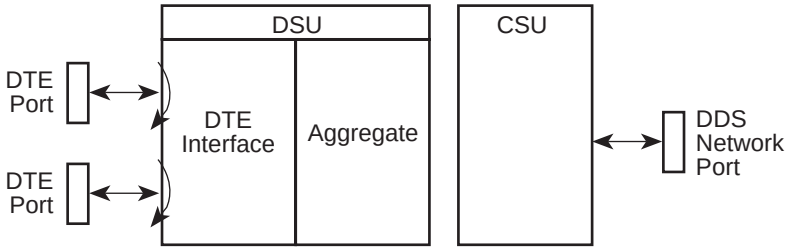


DDS Leased-Line Access Unit

496-14933

External DTE Loopback

DTE External Loopback loops the user data port back to the DTE interface on a per-interface basis without affecting operation of the remaining interfaces. This loopback is located as close as possible to the customer interface (see figure below).



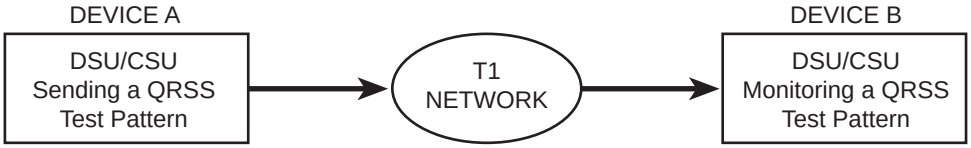
DDS Frame Relay Access Unit

496-14931

Using Pattern Tests (for All Devices)

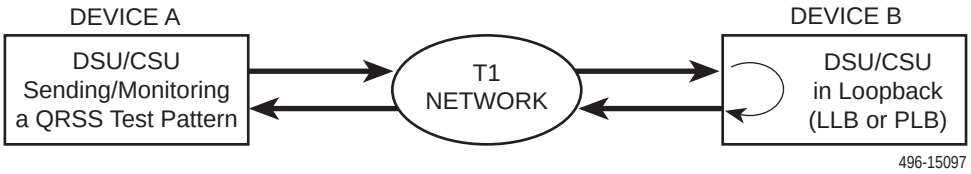
Pattern tests enable a device to send or monitor a known bit pattern. These tests generate industry-standard, MIB-defined bit patterns that can be used to determine whether information is being correctly transmitted across a circuit. These patterns can be sent by the Network T1 and Data Ports interfaces.

You can use a pattern test by itself to test one end of a circuit, or you can use a pattern test with a loopback mode to test both ends of a circuit. The following figure demonstrates a pattern tests that tests one end of a circuit.



496-15096

The following figure demonstrates a pattern test combined with a loopback mode that tests both ends of a circuit.



NOTE:

You can send a 1-in-8 pattern out of the Network T1 interface, but you cannot monitor it. The 1-in-8 pattern is a low-density bit test so that errors of the sort that would be detected by a 1-in-8 pattern will likely appear in the line status fields of the Network T1 Status dialog.

Running Tests

The following sections discuss how to:

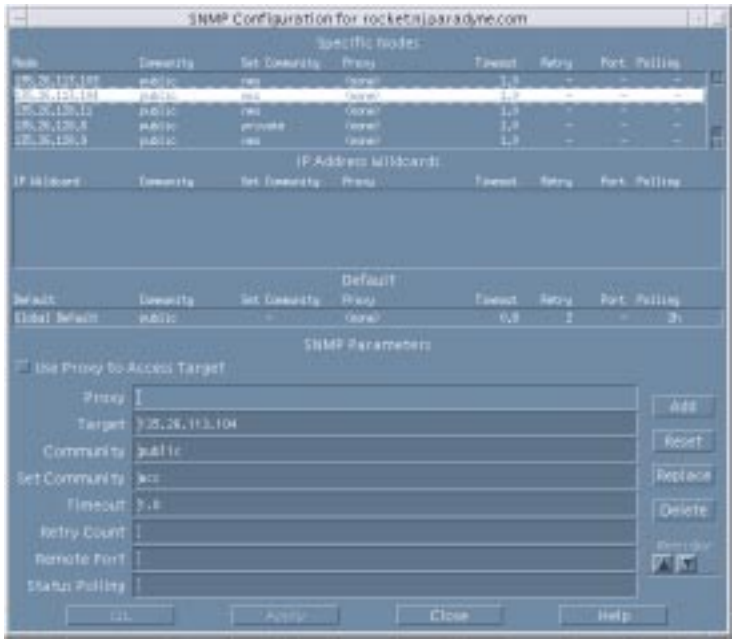
- Set Community Names
- Implement the start of a test
- Verify that a test is running
- Check the test results

Setting the Community Name

Before you set loopback modes or run pattern tests, ensure that the Write Community Name matches that of the device on which you want perform the action.

To set the Write Community Name from within OpenView:

1. Click on the Options menu and select SNMP Configuration. The SNMP Configuration dialog appears.

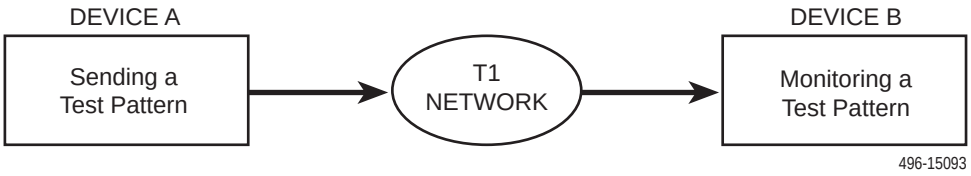


2. Fill out fields as appropriate and click on OK to apply the changes and close the dialog.

Starting Tests

Pattern tests can test one end of a circuit or both ends of a circuit. This section describes how to use each of these methods.

To test one end of a circuit, you must have a device (Device A) send a pattern to another device (Device B), where Device B monitors the integrity of the pattern and tests one end of a circuit as shown in the following figure.



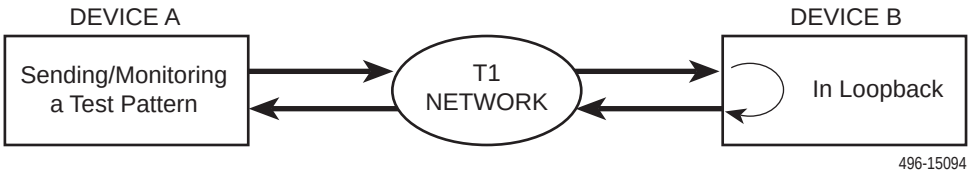
▶ Procedure

To test one end of a circuit:

1. Double-click on Device A to bring up the Device Display.
2. Click on a device interface.
3. Click on the Tests button. A dialog appears.
4. Choose a pattern to send to Device B from the dialog that is displayed.
5. Double-click on Device B to access a representation of the device.
6. Select the interface through which Device B is communicating with Device A by clicking on its symbol.
7. Click on the Diagnose menu and select Tests. A Loopback and Pattern Tests dialog appears.
8. Choose a monitor pattern from the list to check the progress and results of the tests.

The results of the pattern test are displayed in the Results message area. See *Checking the Pattern Test Results* on page 6-16.

To test both ends of a circuit, you must have a device (Device A) send a pattern to another device (Device B). Device B loops the pattern back to Device A so that Device A can monitor the integrity of the pattern and test both ends of the circuit as shown in the following figure.



▶ Procedure

To test both ends of a circuit:

1. Double-click on Device A to open the Device Display.
2. Click on the interface you want to test.
3. Click on the Tests button. A Loopback and Pattern Tests dialog appears.
4. From the Remote loopback list, choose an up code to put Device B in loopback mode. (Alternately, you can select Device B and then choose a loopback from the Local loopback list.)
5. Choose a pattern to send to Device B.
6. Choose a monitor pattern to verify the test.

The results of the pattern test are displayed in the Results message area. See *Checking the Pattern Test Results* on page 6-16.

Verifying that a Test Is Running

You can verify that a test has started and is running using the following procedure.

▶ Procedure

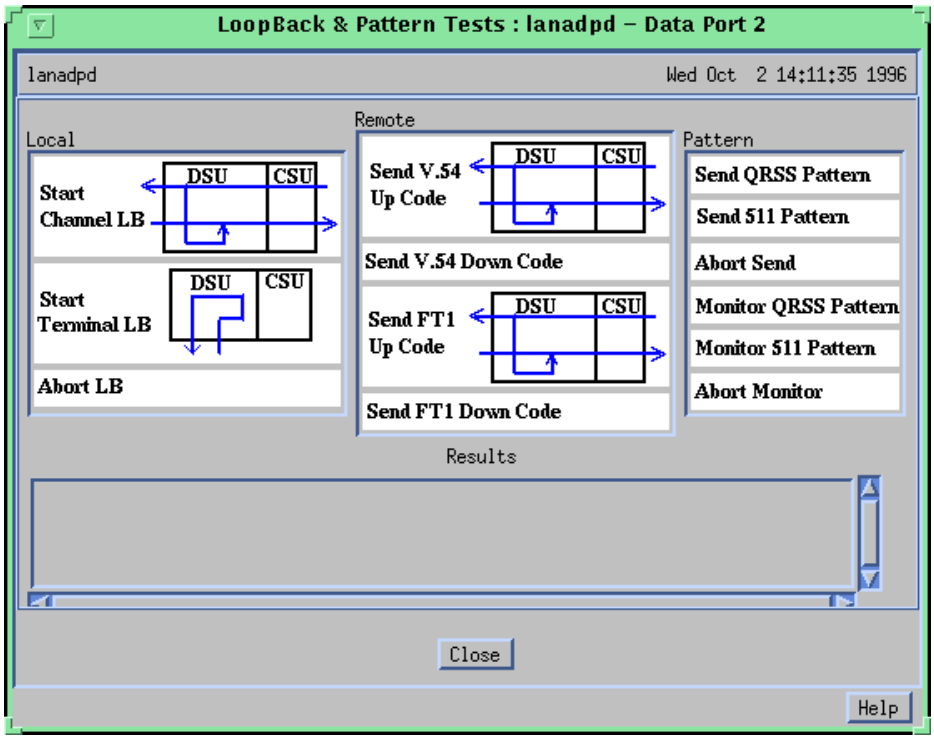
To verify the start of a test:

1. Open a Device Display for the device you are testing.
2. Place your cursor over the interface (port) that is under test and press the right mouse button. A pop-up menu appears.
3. Select Status from the pop-up menu. A dialog is opened that specifies the Administrative and Operational state of the interface. That is, it specifies Up, Down, or Testing.

To verify whether or not an interface is in test, note the color displayed by the device icon in the Device Display. If the interface is in test, it is displayed as a salmon color.

Checking the Pattern Test Results

When you start a pattern test, loopback test, or both, a dialog similar to the following appears.



Using the dialog, you can select the type of test you want to run, and the results of the test are displayed in the Results field of the dialog.

The following results can be returned from a Monitor Pattern test.

- **In Sync No Bit Errors**

  Indicates that the device is operational.

- **In Sync With Bit Errors**

  Indicates that the device is marginal.

- **Not in Sync**

  Indicates that the device is down.

SNMP Management Connectivity

A

Overview

This appendix provides examples of device management through LAN adapters, routers, and PPP/SLIP connections. Also included are the device settings used to achieve this connectivity. These examples do not represent all the possible configurations.

Connecting Devices through a LAN Adapter

LAN adapters connect devices to Ethernet networks as shown in Figure A-1. The figure shows a 3364 or 9621 device connected to a LAN adapter. The device configurations that enable this type of connectivity to a management system are described in the sections that follow.

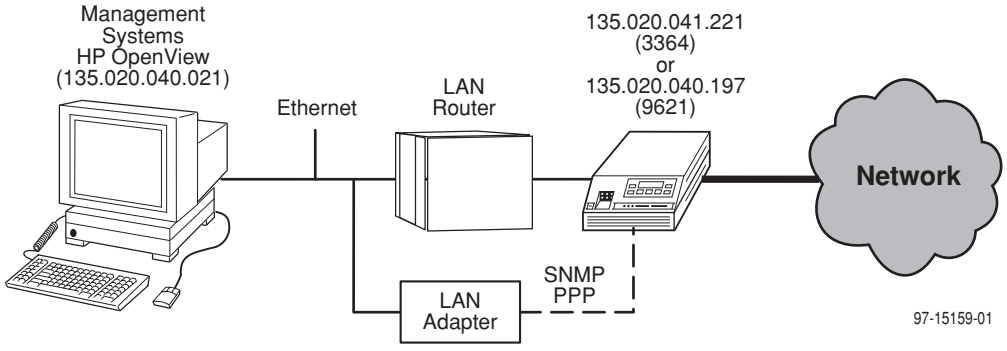


Figure A-1. Connecting Devices Using a LAN Adapter

3364 Device Configuration

The following device settings configure a 3364 device for the operation depicted in Figure A-1. Refer to the *ACCULINK 336x E1 Network Termination Unit Operator's Guide* for a description of how to configure the device using the device's front-panel interface.

User Options	Value
Self-Test	Enab
Com Use	SNMP
Com Typed	Async
Com Clk	Int, Ext
Com Rate	19.2
Char Length	8
CParity	None
CStop Bits	1
Ignore DTR	Yes
Aux Use	None
Aux Rate	19.2

Alarm Options	Value
Alrm Msg	Enab
SNMP Trap	Enab

General SNMP Options	Value
System Name	3364dev
System Location	NJMIS
System Contact	Charlie Parker
CommunityName1	Public
Access 1	R/W
CommunityName2	not used
Access 2	not used
IP Adr	XXX.020.041.221
NetMask	255.255.255.000
Com IP Adr	XXX.020.041.221
Com NetMask	255.255.255.000
Com Link	PPP
Aux IP Adr	not used
Aux NetMask	not used
Def Netwk	Com

SNMP Trap Options	Value
Num Trap Mgrs	1
Trap 1 IP Adr	XXX.020.040.021
Trap 1 Dst	Com
Gen Trap	Both
Entp Trap	Enab
Link Trap	Both
Trap I/F	All

9621 Device Configuration

The following device settings configure a 9621 device for the operation depicted in Figure A-1. Refer to the *FrameSaver 9620 User's Guide* for a description of how to configure the device using the device's terminal interface.

User Interface Options: Communication Port	**Value**
Port Use	Net Link
Port Type	Asynchronous
Data Rate (Kbps)	19.2
Character Length	8
Parity	None
Stop Bits	1
Ignore Control Leads	Disable
RIP	None

Alarm Options	**Value**
ASCII Alarm Messages	Com Port
Alarm & Trap Dial-Out	Disable
Trap Disconnect	Disable
Call Retry	Disable
Dial-Out Delay Time (Min)	5
Alternate Dial-Out Directory	None

Management and Communications Options: Communications Protocol	**Value**
Node IP Address	XXX.020.040.197
Node Subnet Mask	255.255.255.000
Communication Port IP Address	XXX.020.040.197
Communication Port Subnet Mask	255.255.255.000
Communication Port Link Protocol	PPP
Alternate COM Port IP Address	XXX.020.021.002
Alternate COM Port Subnet Mask	255.255.255.000
Default Network Destination	COM

Management and Communications Options: General SNMP Management	**Value**
SNMP Management	Enable
Community Name 1	public
Name 1 Access	Read/Write

Management and Communications Options: SNMP Traps	**Value**
SNMP Traps	Enable
Number of Trap Managers	1
NMS1 IP Address	XXX.020.040.021
Destination	COM
General Traps	Both
Enterprise Specific Traps	Enable
Link Traps	Both
Link Traps Interfaces	All
DLCI Traps on Interfaces	All

Connecting Devices Through a Router

Figure A-2 shows an AAC device connected to a LAN router. The device configurations that enable this type of connectivity are given in *AAC Device Configuration*.

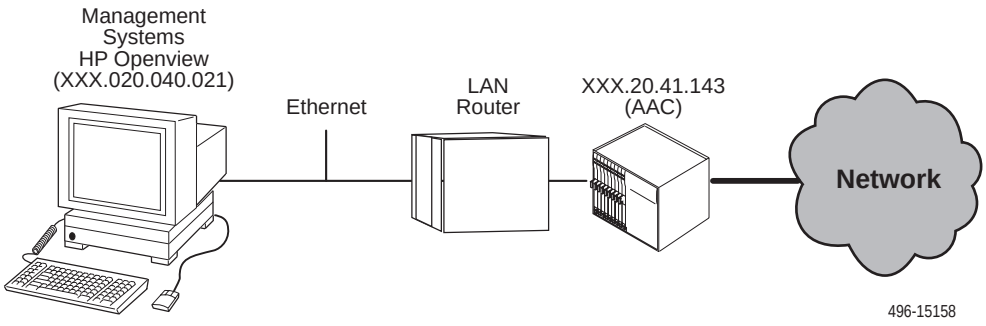


Figure A-2. Connecting an AAC Device Using a LAN Router

AAC Device Configuration

The following device settings configure an AAC device for operation as shown in Figure A-2. Refer to the *ACCULINK Access Controller Reference Guide* for a description of how to configure the device using the device's terminal interface.

CPU Card: TCP/IP Options	Value
DEFAULT IP PORT	local
DEFAULT IP SLOT	n/a
DEFAULT IP UNIT	n/a
HOST IP ADDR	XXX.20.41.143
HOST NETMASK	255.255.255.0
RPT1 IP ADDR	XXX.020.040.021
RPT1 COMMUN STR	public
RPT2 IP ADDR	0.0.0.0
RPT2 COMMUN STR	
RPT1 IP ADDR	0.0.0.0
RPT1 COMMUN STR	

To export alarms to the SNMP management system, set the alarms to **Report** on the *Main Menu→Alarms→Filter* screen of the terminal interface configuration utility.

Connecting Devices Through SLIP/PPP Connections

Figure A-3 shows an 3174 device connected to the management system through a PPP Connection. The device configurations that enable this type of connectivity are given in *3174 Device Configuration* on page A-8.

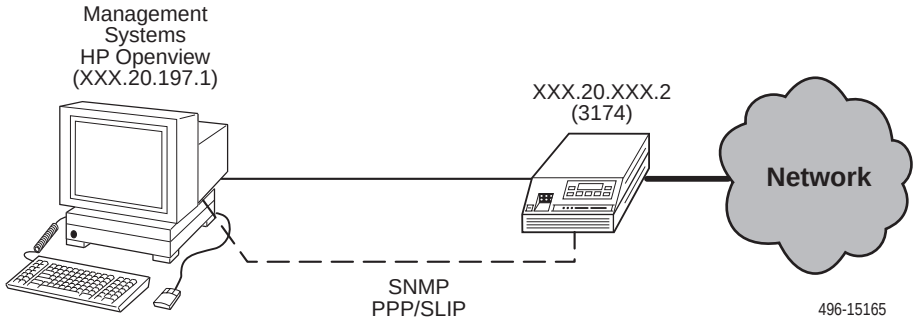


Figure A-3. Connecting Devices Using a SLIP/PPP Connection

MorningStar PPP Configuration on Management System

MorningStar is a software product that runs on a management system to enable PPP connectivity to a device. The MorningStar Systems and Startup files were modified as follows:

- To the **`/usr/etc/ppp/Systems`** file the following line was added:

  `XXX.20.197.2 Any /dev/tty00 19200 0 " "`

- To the **`usr/etc/ppp/Startup`** file the following line was added:

  `/usr/etc/pppd XXX.20.197.1:XXX.20.197.2 slip auto dedicated up netmask 255.255.255.0 debug 5`

3174 Device Configuration

The following device settings configure a 3174 device for operation as shown in Figure A-3. Refer to the *ACCULINK 317x E1 Data Service Unit /Channel Service Unit Operator's Guide* for a description of how to configure the device using the device's front-panel interface.

User Options	**Value**
Self-Test	Enab
Com Use	SNMP
Com Typed	Sync
Com Clk	Int
Com Rate	19.2
Aux Use	SNMP
Aux Rate	19.2

Alarm Options	**Value**
Alrm Msg	Enab
SNMP Trap	Enab

General SNMP Options	Value
System Name	3174dev
System Location	NJMIS
System Contact	Charlie Parker
CommunityName1	public
Access 1	R/W
CommunityName2	not used
Access 2	not used
IP Adr	XXX.020.191.002
NetMask	255.255.255.000
Com IP Adr	XXX.020.191.002
Com NetMask	255.255.255.000
Com Link	PPP
Aux IP Adr	not used
Aux NetMask	not used
Def Netwk	Com

SNMP Trap Options	Value
Num Trap Mgrs	1
Trap 1 IP Adr	XXX.020.040.021
Trap 1 Dst	Com
Gen Trap	Both
Entp Trap	Enab
Link Trap	Both
Trap I/F	All

Glossary

1-in-8 Test	A test pattern consisting of a one (1) followed by seven zeros (on the network only).
511	A random bit test 511 bytes in length.
AAC	ACCULINK Access Controller. A T1 product which permits connection to a variety of network services.
alert	An occurrence of interest within the network. Alerts include alarms and change of status experienced by modems and data service units, as well as alarms experienced by multiplexers, and event messages reported by multiplexers.
AMI	Alternate Mark Inversion. A line coding technique used to accommodate the ones density requirements of E1 or T1 lines.
ANSI	American National Standards Institute. A member of ISO, ANSI accredits and implements standards.
ANSI-T1-403	ANSI specification that defines T1 operation.
APL	Analog Private Line. The private circuit used for data transmission. Also called 4-wire private line, private line, or leased line.
ASCII	American Standard Code for Information Interchange. The standard for data transmission over telephone lines. A 7-bit code establishes compatibility between data services. The ASCII code consists of 32 control characters (nondisplayed) and 96 displayed characters.
asynchronous transmission	A data transmission that is synchronized by a transmission start bit at the beginning of a character (five to eight bits) and one or more stop bits at the end.
ATM	Asynchronous Transfer Mode. A high-speed, low-delay, connection-oriented switching and multiplexing technique using 53-byte cells to transmit different types of data simultaneously.
ATT-54016	AT&T specification that defines T1 operation.
B8ZS	Bipolar 8 Zero Substitution. Encoding scheme for transmitting clear channel signals over a T1 line.
baud	A unit of signaling speed that is equal to the number of symbols per second. This is not necessarily the same as bits per second, although the terms are frequently interchanged.
BER	Bit Error Rate. The number of bits in error over a given period compared to the number of bits transmitted successfully.
BERT	Bit Error Rate Test. A local pattern test used to analyze the network circuit that causes the device to transmit and monitor for a test pattern. Both the control and tributary devices must be connected to the network.
BES	Bursty Error Seconds. A second in which more than one but less than 320 CRC6 error events have occurred.
bit	Binary digit. The smallest unit of information, representing a choice between a one or a zero (sometimes called mark or space).
bps	Bits per second. Indicates the speed at which bits are transmitted across a data connection.

buffer A storage device used to compensate for differences in the data flow rate when transmitting data from one device to another.

busied out One of a device's operational states. When a device is in the busy out (or make busy) state, it will not be able to answer calls. If the busied out device is on a rotary, the rotary will skip the device when servicing incoming calls. A device that has its dial line busied out may switch to the service line for further use.

byte A sequence of successive bits (usually eight) handled as a unit in data transmission.

carrier A carrier is a rack with 17 slots; one control slot (for a Shared Diagnostic Unit) and 16 device slots.

CCA Circuit Card Assembly. A printed circuit board to which separate components are attached.

CCITT Consultative Committee on International Telegraphy and Telephony. An advisory committee established by the United Nations to recommend communications standards and policies. It was renamed ITU in March 1993.

CCITT V.54 CCITT standard for local and remote diagnostic loopback tests.

CNMP Common Network Management Platform. Used to identify HP OpenView elements that relate to the ACCULINK 3100 Series products.

control A device that is, for diagnostic purposes, at the logical head of a hierarchical network. It is the unit from which tests and commands are issued to other units on the same circuit. There is only one control per link.

control channel The diagnostic communications link to network devices.

CRC Cyclic Redundancy Check. A mathematical method of confirming the integrity of received digital data.

CSS Controlled Slip Seconds. A period in which a frame was added or deleted because of a variance in timing.

CSU Channel Service Unit. A device that connects service user equipment such as a DSU to the local digital telephone loop, protects the line from damage, and regenerates the signal.

D4 The transmission standard that specifies 12 frames as a superframe that is used for frame synchronization and to locate signaling bits.

dB Decibel.

dBm A decibel referenced to one milliwatt into 600 ohms. This unit measures relative signal power.

DCE Data Communications Equipment. The equipment that provides the functions required to establish, maintain, and end a connection. It also provides the signal conversion required for communication between the DTE and the network.

DCLB Data Channel LoopBack. Loops the data received from the network interface, for all DS0 channels allocated to the selected port, back to the network.

dial A device operating on a Public Switched Telephone Network (PSTN) line and requiring a dialing method and protocol to conduct data transmission.

dial backup A method of restoring service for data communications during a private line failure by switching the data traffic to the public telephone network.

Dial Standby One of a leased-line device's operational states. The Dial Standby mode allows the device to switch back to leased-line operation while still maintaining the dial line.

dialog A box or window that displays status or configuration information about an object or subject.

DLB	DTE Loopback. Loopback mode that loops the information received on the DTE T1 network interface back to the network as close to the network interface as possible.
DLC	Data Link Control Layer. SNA layer responsible for the transmission of data between two nodes over a physical link.
DLCI	Data Link Connection Identifier. The virtual circuit number corresponding to a particular connection between two destinations. This number is used as part of the frame relay header. The total number of DLCIs between endpoints make up the PVC. DLCIs are a local means of identifying a PVC.
DS0	Digital signal level 0 (zero). A 64 kbps digital telecommunications signal or channel.
DS1	Digital signal level 1. A digital signal transmitted at the rate of 1.544 Mbps in North America.
DSL	Digital Subscriber Line. The non-loaded, local-loop copper connection between the customer and the first node within the network.
DSLAM	Digital Subscriber Line Access Multiplexer. A platform for DSL modems that provides high-speed data transmission with POTS over traditional twisted-pair wiring.
DSU	Data Service Unit. Data communications equipment that provides timing, signal regeneration, and an interface to data terminal equipment. A subrate DSU/CSU is normally referred to as a DSU.
DSX-1	Digital Signal Cross Connect level 1. An interconnection point for terminals, multiplexers and transmission facilities.
DTE	Data Terminal Equipment. The equipment, such as a computer or terminal, that provides data in the form of digital signals for transmission.
DTLB	Data Terminal Loopback. Loopback mode that loops the data for a particular synchronous data port back to the port just before it is combined with the rest of the T1 data stream.
EER	Excessive Error Rate. An error rate that is greater than the threshold that has been configured in the device.
EGP	Exterior Gateway Protocol. Protocol that distributes routing information to the routers that connect autonomous systems.
EIA	Electronic Industries Association. This organization provides standards for the data communications industry to ensure uniformity of interface between DTEs and DCEs.
EIA-530A/RS449 V.35	An Electronic Industries Association's standard defining an interface.
Enterprise MIB	MIB objects unique to a specific company's devices.
ES	Errored Second. A second with one or more ESF error events (one or more CRC6 error events or OOFs).
ESF	Extended Superframe. The T1 transmission standard that specifies 24 frames as an extended superframe to be used for frame synchronization and to locate signaling bits.
facility	A leased or dial transmission path.
facility alarm	An alert that NMS displays indicating that the device has detected an abnormal condition on the facility (line) that could cause data errors. The facility alarm only applies to leased or Analog Private Line (APL) devices.
FDL	Facility Data Link. The selected framing bits in the ESF format used in a wide-area link that are used for control, monitoring, and testing.
frame	One identifiable group of bits that includes a sequence of bits for control, framing, etc.

frame relay A high-speed connection-oriented packet switching WAN protocol using variable-length frames.

frame relay header The DLCI identifier contained within the frame relay packet.

frame relay switching The ability to route frame relay packets based on the source port and frame relay header (DLCI). The header contains a DLCI identifier that distinguishes the port for which the data is intended.

FT1 Fractional Timing 1. ANSI standard for DCLB tests.

HDLC High-Level Data Link Control. A communications protocol defined by the International Standards Organization (ISO).

ICMP Internet Control Management Protocol. Internet protocol that allows for the generation of error messages, tests packets, and informational messages related to IP.

idle One of a dial line device's operational states that indicates an installed device is not currently in use.

IP Internet Protocol. An open networking protocol used for Internet packet delivery.

IP complex mode A mode of managing a DSLAM chassis which is the opposite of IP conservative mode. The DSLAM chassis, associated card and endpoints each require an unique IP address that is visible to the NMS network.

IP conservative mode A mode of managing a DSLAM chassis, associated card and endpoints where only one IP address is visible to the NMS network.

IPC Interworking Packet Concentrator. A device that concentrates traffic from multiple LANs onto a high-speed WAN interface.

ITU International Telecommunications Union. The telecommunications agency of the United Nations, established to provide standardized communications procedures and practices. Before March 1993 it was called CCITT.

LAN adapter A device that allows a serial device to be connected to a LAN.

leased A device operating on a private line where no dialing is necessary to make the connection. A dial device can be configured to run on a leased line. A local leased line device can be switched over to dial mode while attached to a leased line.

LLB Line LoopBack. A test in which the received signal on the network interface is looped back to the network without change.

LOF Loss of Frame. Occurs when a DS1 terminal is unable to synchronize on the DS1 signal for some interval.

LOFC Loss Of Frame Count. The number of LOFs declared.

loopback test Any test that verifies a device's integrity by connecting the device's output to the device's input, then checks the received signal for errors.

LOS Loss of Signal. The T1 line condition where there are no pulses.

make busy A condition indicating that the device is holding the dial line busy to prevent receiving calls.

MIB Management Information Base. A database of managed objects used by SNMP to provide network management information and device control.

MVL Multiple Virtual Lines. A proprietary local loop access technology that permits several services to concurrently and discretely use a single copper wire loop.

NAM Network Access Module. It is a type of CCA that accesses or acts as an interface with the network.

NMS	Network Management System. A computer system used for monitoring and controlling network devices.
OOF	Out Of Frame. An error condition in which frame synchronization bits are in error.
out of threshold	One or more of the analog parameter thresholds has been exceeded. The probable cause is poor line conditions or improper threshold settings. Thresholds may be set through NMS commands.
pattern test	A local test causing the device to transmit and monitor for a particular test pattern. This test disrupts the transmission of primary data.
phase jitter	A rapid or repeated shifting of the relative phase of a signal resulting in unwanted distortion.
PLB	Payload Loopback. Loopback mode that loops the information received on the T1 network interface back to the network after it has passed through receive and transmit framing section.
PPP	Point-to-Point Protocol. A protocol for packet transmission over serial links, specified by Internet RFC 1661.
PRM	Performance Report Messages. Messages indicating the current state of a T1 line as specified by ANSI-T1-403.
proxy ARP	Proxy Address Resolution Protocol. A technique for using a single IP address for multiple networks. A device responds to ARP requests with its own physical address, then routes packets to the proper recipients.
PVC	Permanent Virtual Circuit. The DSU's in-band management channel that supports remote management via a Telnet connection. It is the logical link, identified by a DLCI, used for routing frames over the network from their source to their destination.
QRSS	Quasi-Random Signal Source. A test pattern simulating a random pattern of digital ones and zeros used to simulate normal transmission.
RADSL	Rate Adaptive Digital Subscriber Line. A technique for the use of an existing twisted-pair line that permits simultaneous POTS and high-speed data communication at adaptive symmetric and asymmetric rates.
RBS	Robbed Bit Signaling. Signaling used for voice-call processing over a T1 line.
remote loopback	A test that sends a signal to the remote device to test the local device, the remote device, and the circuit between them.
RLB	Repeater LoopBack. Loops the signal being sent to the network back to the DTE Drop/Insert and data ports after it has passed through the framing circuitry of the device.
RTU	Remote Termination Unit. A DSL device installed at the customer premises.
SES	Severely Errored Seconds. Usually defined as a second during which a specific number of CRC errors was exceeded, or an OOF or other critical error occurred.
SLIP	Serial Link Internet Protocol. Protocol for serial operation in an Internet network.
SLV	Service Level Verifier. A feature that monitors and ensures frame relay network service levels.
SNMP	Simple Network Management Protocol. Protocol for open networking management.
streaming terminal	The modem is in an antistreaming condition. The RTS input to the modem was held ON for a period exceeding the time selected by the RTS antistream configuration option.
Sub-normal Operating Speed	A condition indicating the leased or Analog Private Line (APL) device is operating at a speed below normal.

Sub-tree Truncation	Downstream health and status information has been truncated due overflowed system limits with large amounts of health and status information in the subnetwork. Recover this information by sending device health and status commands to specific modems.
synchronous transmission	Transmission in which the data characters and bits are transmitted at a fixed rate with transmitter and receiver synchronized. This eliminates the need for start and stop bits as used in asynchronous transmission, and is thus faster and more efficient.
T1	A term for a digital carrier facility used to transmit a DS1 formatted digital signal at 1.544 Mbps. It is used primarily in North America.
TCP	Transmission Control Protocol. An Internet standard transport layer protocol defined in STD 7, RFC 793. It is connection-oriented and stream-oriented.
TDM	Time Division Multiplexer. A device that enables the simultaneous transmission of multiple independent data streams into a single high-speed data stream by simultaneously sampling the independent data streams and combining these samples to form the high-speed stream.
trellis-coded modulation	Advanced error correction coding technique for primary data typically used on higher speed modems. This modulation scheme uses Forward Error Correction for multipoint and high-speed point-to-point applications.
tributary timeout	This indicates that the control DSU has not received a health and status update from the tributary DSU within the specified time.
tributary unit	A unit that is under the control of another unit.
UAS	Unavailable Seconds. A count of one-second intervals when service is unavailable.
UDP	User Datagram Protocol. A TCP/IP protocol describing how messages reach application programs within a destination computer.
V.54	An ITU-T standard for local and remote diagnostic loopback tests.
VC	Virtual Circuit. A logical connection or packet-switching mechanism established between two devices at the start of transmission.
VPC	Virtual Path Connection. In ATM, a unidirectional concatenation of Virtual Path Links (VPLs) between Virtual Path Terminators (VPTs).
Yellow Alarm	An outgoing signal transmitted when a DS1 terminal has determined that it has lost the incoming signal.

Index

Numbers

A

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

V