NavisCore Diagnostic and Troubleshooting Guide

Ascend Communications, Inc.

Product Code: 80074
Revision 00
September 1998

ASCEND COMMUNICATIONS, INC. END-USER LICENSE AGREEMENT

ASCEND COMMUNICATIONS, INC. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE AND ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE “PROGRAM”) TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE(S) OR USING THE ASCEND SWITCH(ES) CONTAINING THE SOFTWARE, AND BEFORE USING THE ACCOMPANYING USER DOCUMENTATION. OPENING THE PACKAGE(S) OR USING THE ASCEND SWITCH(ES) CONTAINING THE PROGRAM WILL INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, ASCEND IS UNWILLING TO LICENSE THE PROGRAM TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE PROGRAM WITHIN TEN (10) DAYS FROM SHIPMENT TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR LICENSE FEE WILL BE REFUNDED. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE PROGRAM BETWEEN YOU AND ASCEND, AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION OR UNDERSTANDING BETWEEN THE PARTIES.

1. License Grant. Ascend hereby grants to you, and you accept, a non-exclusive, non-transferable license to use the computer software, including all patches, error corrections, updates and revisions thereto in machine-readable, object code form only (the “Software”), and the accompanying User Documentation, only as authorized in this License Agreement. The Software may be used only on a single computer owned, leased, or otherwise controlled by you; or in the event of inoperability of that computer, on a backup computer selected by you. You agree that you will not pledge, lease, rent, or share your rights under this License Agreement, and that you will not, without Ascend’s prior written consent, assign or transfer your rights hereunder. You agree that you may not modify, reverse assemble, reverse compile, or otherwise translate the Software or permit a third party to do so. You may make one copy of the Software and User Documentation for backup purposes. Any such copies of the Software or the User Documentation shall include Ascend’s copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Program or any portions thereof may be made by you or any person under your authority or control.

2. Ascend’s Rights. You agree that the Software and the User Documentation are proprietary, confidential products of Ascend or Ascend's licensor protected under US copyright law and you will use your best efforts to maintain their confidentiality. You further acknowledge and agree that all right, title and interest in and to the Program, including associated intellectual property rights, are and shall remain with Ascend or Ascend's licensor. This License Agreement does not convey to you an interest in or to the Program, but only a limited right of use revocable in accordance with the terms of this License Agreement.

3. License Fees. The license fees paid by you are paid in consideration of the license granted under this License Agreement.

4. Term. This License Agreement is effective upon your opening of the package(s) or use of the switch(es) containing Software and shall continue until terminated. You may terminate this License Agreement at any time by returning the Program and all copies or portions thereof to Ascend. Ascend may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Ascend, you agree to return to Ascend the Program and all copies or portions thereof. Termination of this License Agreement shall not prejudice Ascend's rights to damages or any other available remedy.

5. Limited Warranty. Ascend warrants, for your benefit alone, for a period of 90 days from the date of shipment of the Program by Ascend (the "Warranty Period") that the program diskettes in which the Software is contained are free from defects in material and workmanship. Ascend further warrants, for your benefit alone, that during the Warranty Period the Program shall operate substantially in accordance with the User Documentation. If during the Warranty Period, a defect in the Program appears, you may return the Program to the party from which the Program was acquired for either replacement or, if so elected by such party, refund of amounts paid by you under this License Agreement. You agree that the foregoing constitutes your sole and exclusive remedy for breach by Ascend of any warranties made under this Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE PROGRAM IS LICENSED "AS IS", AND ASCEND DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES OF NONINFRINGEMENT.

6. Limitation of Liability. Ascend's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the greater of: (i) ten thousand US dollars ($10,000) or (ii) the total license fee paid to Ascend for the use of the Program. In no event shall Ascend be liable for any indirect, incidental, consequential, special, punitive or exemplary damages or lost profits, even if Ascend has been advised of the possibility of such damages.

7. Proprietary Rights Indemnification. Ascend shall at its expense defend you against and, subject to the limitations set forth elsewhere herein, pay all costs and damages made in settlement or awarded against you resulting from a claim that the Program as supplied by Ascend infringes a United States copyright or a United States patent, or misappropriates a United States trade secret, provided that you: (a) provide prompt written notice of any such claim, (b) allow Ascend to direct the defense and settlement of the claim, and (c) provide Ascend with the authority, information, and assistance that Ascend deems reasonably necessary for the defense and settlement of the claim. You shall not consent to any judgment or decree or do any other act in compromise of any such claim without first obtaining Ascend's written consent. In any action based on such a claim, Ascend may, at its sole option, either: (1) obtain for you the right to continue using the Program, (2) replace or modify the Program to avoid the claim, or (3) if neither (1) nor (2) can reasonably be effected by Ascend, terminate the license granted hereunder and give you a prorata refund of the license fee paid for such Program, calculated on the basis of straight-line depreciation over a five-year useful life. Notwithstanding the preceding sentence, Ascend will have no liability for any infringement or misappropriation claim of any kind if such claim is based on: (i) the use of other than the current unaltered release of the Program and Ascend has provided or offers to provide such release to you for its then current license fee, or (ii) use or combination of the Program with programs or data not supplied or approved by Ascend to the extent such use or combination caused the claim.

8. Export Control. You agree not to export or disclose to anyone except a United States national any portion of the Program supplied by Ascend without first obtaining the required permits or licenses to do so from the US Office of Export Administration, and any other appropriate government agency.

9. Governing Law. This License Agreement shall be construed and governed in accordance with the laws and under the jurisdiction of the Commonwealth of Massachusetts, USA. Any dispute arising out of this Agreement shall be referred to an arbitration proceeding in Boston, Massachusetts, USA by the American Arbitration Association.

10. Miscellaneous. If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorneys' fees and expenses of arbitration. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

Contents

Chapter 2 Viewing Switch, Module, and Physical Port Details

Chapter 3 Generating Physical Port Statistics

Chapter 6 Monitoring Logical Ports

Chapter 7 Monitoring ATM Logical Ports

Chapter 16 Monitoring MIB Values

Chapter 17 Resolving NMS Problems

Appendix D Signalled QoS, BBC, ATC, and BEI Service Category Mappings

Appendix E Using SVC Failure Information

Appendix F Accessing Control Files

Index

List of Figures

List of Tables

About This Guide

The *NavisCore Diagnostic and Troubleshooting Guide* describes how to monitor and troubleshoot activity and events on an Ascend-switch network. For information on using HP OpenView, see the appropriate HP documentation.

This guide supports the following Network Management Station (NMS) and switch software releases:

- NavisCore, Release 4.0
- B-STDX, Release 6.0
- CBX 500, Release 3.0
- GX 550, Release 1.0

What You Need to Know

As a reader of this guide, you should be familiar with UNIX operating system commands and be familiar with HP OpenView. You should possess a working knowledge of relational database software to properly maintain SYBASE, which is the database software used by NavisCore.

This guide is written for system administrators who are responsible for monitoring the network, and for diagnosing and troubleshooting network problems. This guide assumes that you have:

- Experience in managing Ascend switches and the NMS.
- Installed the switch hardware and the NMS. See the appropriate installation guide for more information:
  - *B-STDX 8000/9000 Hardware Installation Guide*
  - *CBX 500 Hardware Installation Guide*
  - *GX 550 Hardware Installation Guide*
  - *Network Management Station Installation Guide*
- Read the software release notices that accompany your switch software and NavisCore for the most current product information and requirements.
- Configured I/O-module attributes and physical ports on your switch. See the *NavisCore Physical Interface Configuration Guide* for instructions.

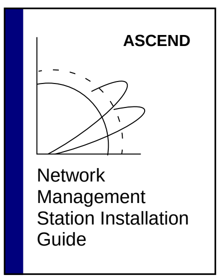
Reading Path

This section describes all of the documents that support the NavisCore NMS and switch software. The documents are grouped as follows:

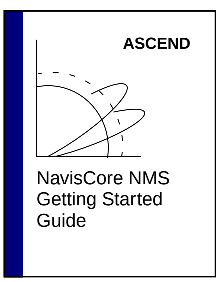
- NMS Documentation
- Switch Software Documentation

NMS Documentation

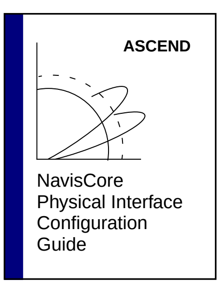
Read the following documents to install and operate NavisCore Release 4.0.



This guide describes prerequisite tasks, hardware and software requirements, and instructions for installing Solaris, HP OpenView, and NavisCore on the NMS.



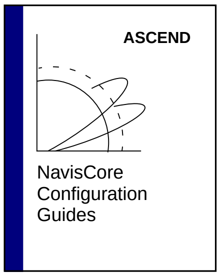
This guide describes how to configure and manage NavisCore, network maps, and Ascend switches.



This guide describes how to configure processor and I/O modules on Ascend switches.

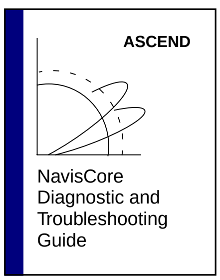
Switch Software Documentation

Read the following documents to configure switch software for B-STDX Release 6.0, CBX Release 3.0, and GX Release 1.0.

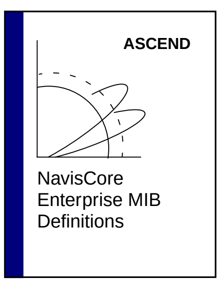


These guides describe how to configure WAN services on the STDX, B-STDX, CBX, and GX switch platforms:

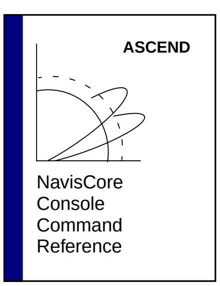
- *NavisCore Frame Relay Configuration Guide*
- *NavisCore ATM Configuration Guide*
- *NavisCore IP Navigator Configuration Guide*
- *NavisCore ISDN Configuration Guide*
- *NavisCore SMDS Configuration Guide*



This guide describes how to diagnose and troubleshoot your NavisCore switch network.



This document gives a brief overview of SNMP and describes the NavisCore Enterprise MIB definitions.



This reference lists and describes the NavisCore switch console commands.

How to Use This Guide

This guide contains the following information:

Read	To Learn About
Chapter 1	Using NavisCore to monitor and troubleshoot the network.
Chapter 2	Monitoring hardware details of switches, processor modules, I/O modules, and physical ports.
Chapter 3	Monitoring statistics on physical port activity.
Chapter 4	Monitoring performance data on physical port activity.
Chapter 5	Running diagnostic tests and loopback tests on processor modules, I/O modules, physical ports, and channels.
Chapter 6	Monitoring logical port statistics and attributes common to multiple network services.
Chapter 7	Monitoring ATM logical port attributes and statistics.
Chapter 8	Monitoring IP configuration parameters and statistics.
Chapter 9	Monitoring Frame Relay logical port attributes and statistics.
Chapter 10	Monitoring SMDS logical port attributes and statistics, PDU diagnostic statistics, management addresses, and routes.
Chapter 11	Monitoring ISDN configuration parameters and statistics.
Chapter 12	Monitoring trunk status and statistics.
Chapter 13	Monitoring ATM circuit status and statistics.
Chapter 14	Monitoring Frame Relay circuit status and statistics.
Chapter 15	Configuring traps to inform you of network events.
Chapter 16	Monitoring MIB values.
Chapter 17	Resolving NMS problems.
Appendix A	Interpreting trap-alarm condition messages.
Appendix B	Interpreting major and minor error codes that are displayed when you run background diagnostic tests.
Appendix C	Copying data into or out of any NavisCore database.
Appendix D	Understanding signalled QoS, BBC, and BEI service category mappings.

Read	To Learn About
Appendix E	Understanding SVC failure information.
Appendix F	Accessing control files on B-STDX CP, CBX 500 SP, and GX 550 hard disks.

Conventions

This guide uses the following conventions, when applicable:

Convention	Indicates	Example
`Courier Bold`	User input on a separate line.	**`eject cdrom`**
[*bold italics*]	Variable parameters to enter.	**[*your IP address*]**
`Courier Regular`	Output from a program.	`Please wait...`
Boldface	User input in text.	Type **cd install** and ...
Menu => Option	Select an option from the menu.	NavisCore => Logon
Italics	Book titles, new terms, and emphasized text.	*Network Management Station Installation Guide*
Boxes around text	Notes, warnings, cautions.	See examples below.

Notes provide additional information or helpful suggestions that may apply to the subject text.

Cautions notify the reader to proceed carefully to avoid possible equipment damage or data loss.

Warnings notify the reader to proceed carefully to avoid possible personal injury.

Related Documents

This section lists the related Ascend and third-party documentation that you may find helpful to read.

Ascend

- *GX 550 Hardware Installation Guide* (80077)
- *CBX 500 Hardware Installation Guide* (80011)
- *B-STDX 8000/9000 Hardware Installation Guide* (80005)
- *Networking Services Technology Overview* (80001)
- *NavisCore NMS Getting Started Guide* (80070)
- *NavisCore Network Management Station Installation Guide* (80014)
- *NavisCore Physical Interface Configuration Guide* (80080)
- *NavisCore ATM Configuration Guide* (80072)
- *NavisCore Frame Relay Configuration Guide* (80071)
- *NavisCore IP Navigator Configuration Guide* (80056)
- *NavisCore SMDS Configuration Guide* (80073)
- *NavisCore ISDN Configuration Guide* (80039)
- *NavisCore Console Command Reference* (80075)
- *NavisCore Reading Roadmap* (80069)
- *NavisXtend Accounting Server Administrator's Guide* (80046)
- *NavisXtend Statistics Server User's Guide* (80078)

Third Party

- *Solaris 2.5.1 System Configuration and Installation Guide*
- *HP OpenView 4.11 Network Node Manager Documentation Set*
- *SYBASE SQL Server Reference Manual: Volumes 1 and 2*
- *SYBASE SQL Server System Administration Guide*

Customer Comments

Customer comments are welcome. Please respond in one of the following ways:

- Fill out the Customer Comment Form located at the back of this guide and return it to us.
- Email your comments to cspubs@ascend.com
- FAX your comments to 978-392-9768, attention Technical Publications.
- Open a case in CaseView for documentation.

Customer Support

To obtain patch software, release notes, or support, access the Ascend FTP Server or contact the Technical Assistance Center at:

- 1-800-DIAL-WAN (U.S. and Canada)
- 0-800-96-2229 (U.K.)
- 1-978-952-7299 (all other areas)

Acronyms

This guide uses some of the following acronyms:

Acronym	Description
ATC	ATM Transfer Capability
ATM	Asynchronous Transfer Mode
BBC	Broadband Bearer Classes
BEI	Best Effort Indicator
BERT	Bit Error Rate Test
CDV	cell delay variation
CIR	committed information rate
CLLM	Consolidated Link Layer Management
CLP	cell loss priority
CP	Control Processor (B-STDX)
CSU	channel service unit
DLCI	Data Link Connection Identifier
DSU	data service unit
EFCI	Explicit Forward Congestion Indication
FCP	Flow Control Processor (CBX 500)
HSSI	High-Speed Serial Interface
ILMI	Interim Link Management Interface
IOA	input/output adapter
IOM	input/output module
IOP	input/output processor
IP	Internet Protocol
ISDN	Integrated Services Digital Network
MIB	Management Information Base
NMS	Network Management Station
NP	Node Processor (GX 550)
OAM	Operations, Administration, and Maintenance

Acronym	Description
OCU	office channel unit
OSPF	Open Shortest Path First
PDU	protocol data unit
PRAM	parameter random access memory
PVC	permanent virtual circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SAAL	Signaling ATM Adaptation Layer
SLIP	Serial Line Internet Protocol
SNMP	Simple Network Management Protocol
SP	Switch Processor (CBX 500)
SPVC	soft permanent virtual circuit
SVC	switched virtual circuit
UDP	User Datagram Protocol
UPC	usage parameter control
VC	virtual channel
VCI	virtual channel identifier
VPI	virtual path identifier
VPN	virtual private network

1

Overview

This chapter describes how to monitor the various objects that make up an Ascend network, and provides an overview of how to troubleshoot your network problems.

Monitoring Switches and Services

In an Ascend network, you monitor *network objects*, which include switches, I/O modules, their physical ports, and the logical ports, trunks, and circuits that network services use to transfer data between switches. Ascend network services include:

- ATM
- Frame Relay
- IP
- SMDS
- ISDN

Each switch supports one or more of these services. For information on supported services, see the hardware installation guide for your switch.

You use NavisCore to monitor Ascend network objects and to perform other network management tasks. NavisCore is a network management application that runs under HP OpenView on a Network Management Station (NMS).

Accessing NavisCore Monitoring Functions

The Monitor menu in HP OpenView allows you to access NavisCore monitoring functions. You use two selections on the Monitor menu to access these functions:

- Ascend Objects
- Ascend IP Objects

Table 1-1 describes each of the NavisCore monitoring functions you can access from the Ascend Objects menu selection, as well as the section of this guide (or another guide) where you can find detailed information on the function. Keep in mind that the monitor functions allow you to view attributes and statistics only. You cannot modify attributes.

> You do not need to log on to view information through the Monitor menu. NavisCore monitoring functions do not require Operator passwords.

Table 1-1. Monitor Menu Options

Select: Monitor ⇒ Ascend Objects ⇒	To view	See
Show Detail	Switch back panel	"Viewing Switch Details" on page 2-9
Show Detail. Double-click on the CP, SP, or NP slot and select Active at the prompt	Attributes for the command processor (CP), switch processor (SP), or node processor (NP) and system timing	"Viewing CP and SP Status" on page 2-19 and "Viewing NP Status" on page 2-23
Show Detail. Double-click on the IOM or BIO module slot	Attributes for the selected IOM or BIO module	"Viewing B-STDX 8000/9000 and CBX 500 IOM Status" on page 2-29 and "Viewing BIO Module Status" on page 2-36
Show Detail. Double-click on the physical port	Attributes and status messages for the selected physical port	"Reviewing Physical Port Status" on page 2-44
Show Detail. Double-click on the physical port. Choose Logical Port	Attributes and status messages for the selected logical port	"Viewing Logical Port Status" on page 6-1
Show Logical Ports	Attributes and status messages for the selected logical port	"Viewing Logical Port Status" on page 6-1
Show All Subnets	Subnets for this network map	"Viewing Switch Subnets" on page 2-7

Table 1-1. Monitor Menu Options (Continued)

Select: Monitor ⇒ Ascend Objects ⇒	To view	See
Show All Clusters	Clusters for this network map	"Viewing Switch Clusters" on page 2-8
Show All Switches	Switch attributes	"Viewing Switch Status" on page 2-1
Show Circuits	The configuration, status, and routing information for all circuits in the network map	"Viewing Point-to-Point ATM PVCs" on page 13-1; "Viewing Frame Relay PVCs" on page 14-1
Show All Multicast DLCIs	Status information about multicast DLCIs	"Viewing the Status of Multicast DLCIs" on page 9-25
Show All Management DLCIs	Status information about management DLCIs	"Viewing the Status of Management DLCIs" on page 9-26
Show All Management VPIs/VCIs	Status information about a management connection	"Viewing All Management VPI/VCIs" on page 7-50
Show All Management Addresses	Status information about management addresses	"Viewing SMDS Management Address Status" on page 10-11
Show All Accounting Parameters	Accounting parameters for the selected switch	*NavisXtend Accounting Server Administrator's Guide*
Show All ATM Traffic Descriptors	Traffic descriptors for the entire switch	"Viewing Traffic Descriptor Attributes for the Entire Switch" on page 7-34
Show All Soft PVC Parameters	A submenu of soft PVC status information	"Viewing Soft PVCs" on page 13-47
Show All SVC Parameters	A submenu of SVC status information	"Viewing ATM SVCs" on page 13-55; "Viewing Frame Relay SVCs" on page 14-30
Show All CAC Parameters	A submenu of CAC parameters defined for the selected switch	"Viewing CAC Parameters for ATM Circuits" on page 13-87; "Viewing CAC Parameters for Frame Relay Circuits" on page 14-25
Show All Customers/VPNs	A submenu of Customer and VPN information	"Viewing Customer/VPN Parameters" on page 12-22

Table 1-1. Monitor Menu Options (Continued)

Select: Monitor ⇒ Ascend Objects ⇒	To view	See
Show Trunks	Operational status and available bandwidth for any trunk in the network map	"Viewing the Trunk Status" on page 12-2
Show SMDS Routes	SMDS routes configured for this switch	"Viewing SMDS Route Status" on page 10-13
Show All PNNI Node Parameters	A submenu of Private Network-to-Network Interface (PNNI) node parameters defined for all the CBX 500 and GX 550 switches in the network	"Viewing PNNI Logical Port and Node Parameters" on page 7-14

► In addition to the information you can view through the Ascend Objects menu selection, you can view IP attributes and statistics through the Ascend IP Objects menu selection. See Chapter 8, "Monitoring IP" for details.

Monitoring the Network Map

After you display an HP OpenView network map, you can monitor the status of a network object through color indicators as described in Table 1-2.

Table 1-2. Network Map Status Indicators

Object Color	Description/Action
Yellow	An I/O module in the switch may be out of sync. Display the Show Switch Back Panel dialog box and review the status of each module. If necessary, synchronize PRAM.
Wheat	The switch object is not managed. You unmanage an object to prevent the NMS from polling the object while you configure it. To manage an object, from the Options menu, select Manage Object.
Red	The object is in a failed state and cannot actively communicate with the NMS. The problem is potentially serious and may require you to install new hardware or re-configure network equipment.
Green	The object/switch is actively communicating with the NMS.

Viewing an Object Description

The Object Description dialog box enables you to view and modify certain attributes for the following objects:

- A selected object on the network map, such as a switch
- Map description for a selected object
- Submap description for a selected object

Viewing a Switch Description

To view and modify the HP OpenView attributes for a switch:

1. Select the switch object on the network map.

2. From the Edit menu, select Describe/Modify Object. The Object Description dialog box appears (see Figure 1-1).

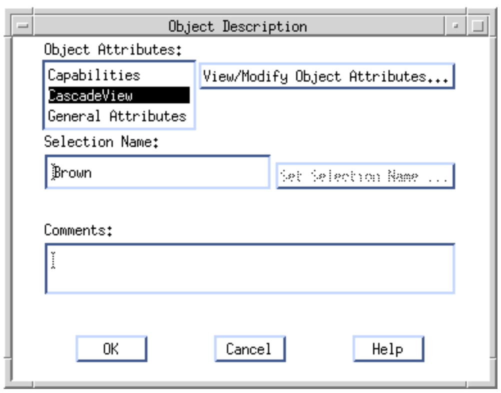


Figure 1-1. Object Description Dialog Box

3. In the Object Attributes field, select CascadeView and choose View/Modify Object Attributes. The Attributes for Object [*name*] dialog box appears (see Figure 1-2).

> See the *HP OpenView User's Guide* for information about modifying object capabilities and general attributes.

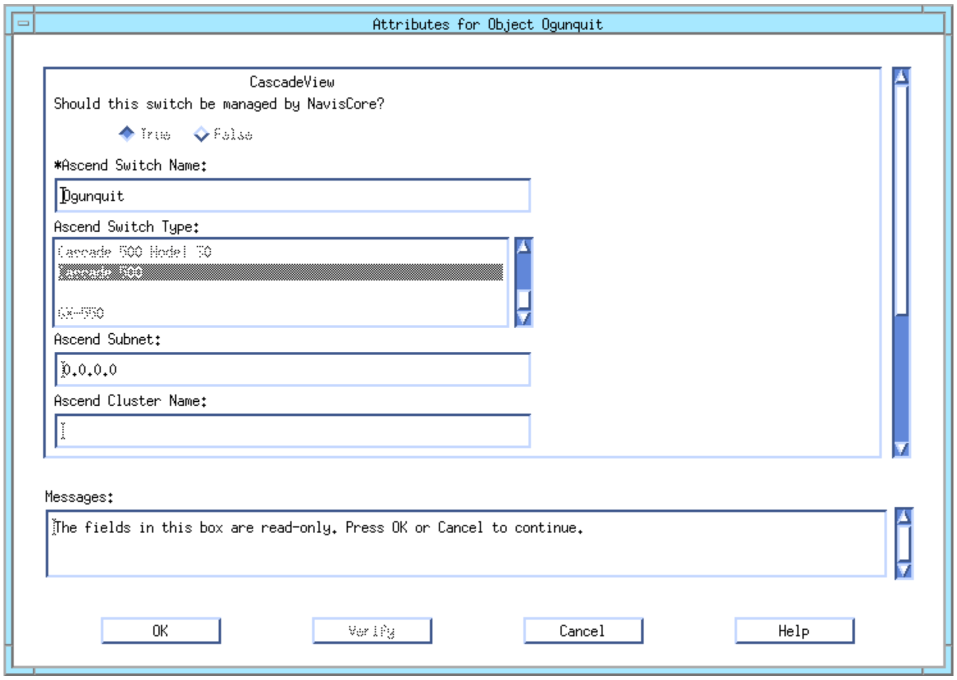


Figure 1-2. Attributes for Object [Switch] Dialog Box

Table 1-3 describes each of the dialog box fields.

Table 1-3. Attributes for Object Fields

Field	Description
Should this switch be managed by NavisCore?	Displays True if NavisCore manages the switch.
Ascend Switch Name	Displays the switch name.
Ascend Switch Type	Displays the switch type.
Ascend Subnet	Displays the subnet IP address for this switch. A subnet divides a large network into smaller pieces. Subnets support a three-level hierarchy in which the host number field is divided into two parts, the subnet number and the host number on that subnet.
Ascend Cluster Name	Displays the name of the cluster to which this subnet belongs.
Messages	Provides additional information about the fields in the Object for Attributes dialog box.

Viewing a Map Description

To view a map description for a selected object icon:

1. On the network map, select the object icon.
2. From the Map menu, select Maps ⇒ Describe/Modify. The Map Description dialog box appears (see Figure 1-3).

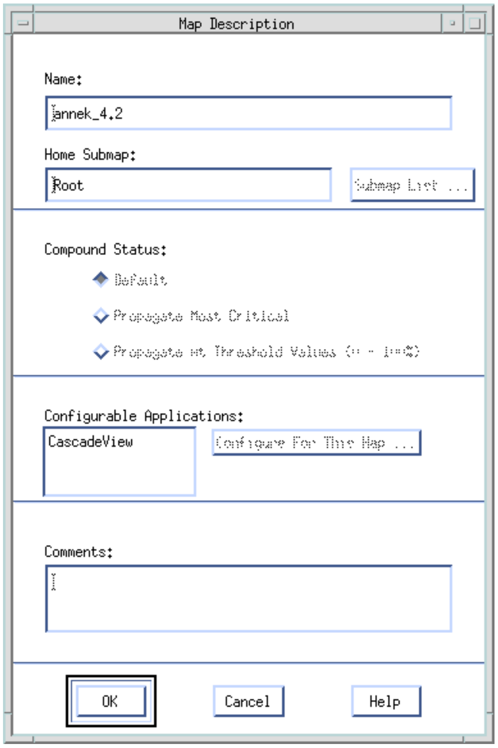


Figure 1-3. Map Description Dialog Box

Table 1-4 describes each of the dialog box fields.

Table 1-4. Map Description Fields

Field	Description
Name	The name that identifies the map.
Home Submap	If a home submap exists, the system displays the name that identifies the home submap. A home submap is the root home location.

Table 1-4. Map Description Fields (Continued)

Field	Description
Compound Status	Displays the desired status propagation: *Default* – Causes OpenView to propagate status according to a predefined algorithm. *Propagate Most Critical* – Causes HP OpenView to propagate the status of the most critical symbol in the child submap, up to the symbols of the parent object. *Propagate At Threshold Values (0 - 100%)* – Enables you to set threshold values that determine when HP OpenView propagates status. The value shown for each field is the default value: %warning 30, %minor 20, %major 10, %critical 5. Compound status indicates how HP OpenView propagates the status of a symbol in a low-level submap, up to parent submaps, to warn you of a problem. For more information, see the *HP OpenView User's Guide*.
Configurable Applications	Select CascadeView and choose Configure For This Map to view the map configuration.
Comments	Additional comments that further describe the map.

Viewing a Submap Description

To view a submap description for a selected object icon:

1. On the network map, select the object icon.
2. From the Map menu, select Submap ⇒ Open/List. The Submaps in Map dialog box appears (see Figure 1-4).

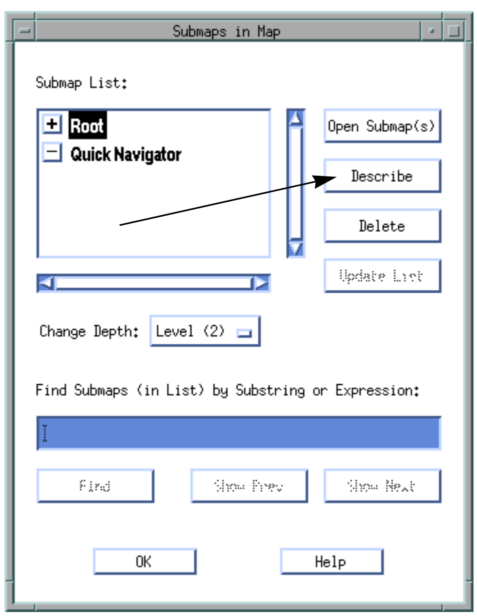


Figure 1-4. Submaps in Map Dialog Box

3. Select a submap from the Submap List and choose Describe. The Submap Description dialog box appears (see Figure 1-5).

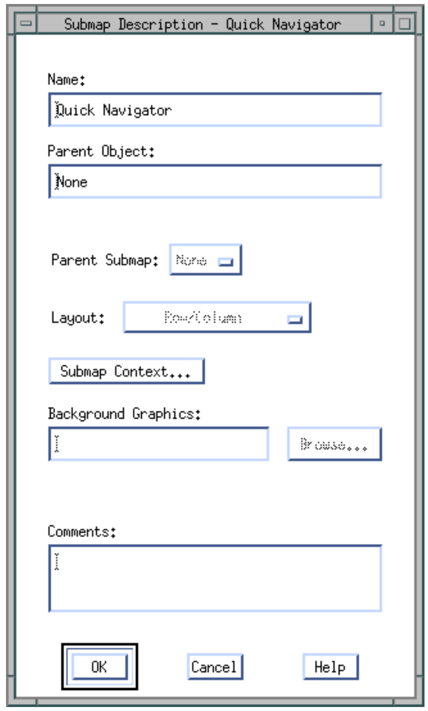


Figure 1-5. Submap Description Dialog Box

Table 1-5 describes each of the dialog box fields.

Table 1-5. Submap Description Fields

Field	Description
Name	The name that identifies the submap.
Parent Object	If a parent object exists, the system displays the name of the object in this field.
Parent Submap	If a parent submap exists, the system displays the name of the parent submap. This is a submap that is the parent to any child submaps. The home submap usually is the parent submap with associated child submaps, however you can configure child submaps to be the home submap.
Layout	NavisCore uses the default Row/Column. This option affects how the objects are arranged on the screen.
Background Graphics	HP OpenView field. Specifies any background graphics used for the map background.
Comments	Additional comments that further describe the submap.

Generating Reports

You can use UNIX scripts or the NavisCore Report menu to generate reports at the network, node, circuit, trunk, SVC, or IP level.

Using Scripts to Generate Reports

Table 1-6 describes the UNIX scripts and associated commands that you can use to generate reports. You issue these commands at the UNIX prompt.

> You must have the Sybase SQR package installed before you can run these scripts. Be sure to run the script from your home directory. The scripts listed in Table 1-6 will attempt to write to the current directory. Errors occur if you do not have write permission for the directory. These scripts create the report (with a .lis extension) in the directory where the report is run.

Table 1-6. Commands Used to Generate Network Reports

Report Script Command	Report Name	Description
/opt/CascadeView/bin/cv-network-rpt.sh	allnetwork.lis	Network report
/opt/CascadeView/bin/cv-circuit-rpt.sh	allckt.lis	Circuit report
/opt/CascadeView/bin/cv-node-rpt.sh	allnode.lis	Node report
/opt/CascadeView/bin/cv-trunk-rpt.sh	alltrk.lis	Trunk report
/opt/CascadeView/bin/cv-svcparam-rpt.sh	allsvc.lis	SVC parameters report

Using NavisCore to Generate Reports

The NavisCore Report menu contains Generate and View submenus from which you can generate and view the following types of reports:

- Single Node Report
- All Node Report
- Network Report
- Trunk Report
- Circuit Report
- IP Reports

Table 1-7 describes each of the Generate and View report options. The system generates an error message if you attempt to view a report before the report has been generated.

Table 1-7. Generate and View Report Options

Report Option	Action/Description
Generate or View Single Node Report	To select this option: • Select the node for use in a report from the network map. • Then select this Report menu option. NavisCore enables you to view the report while it is generating. The system saves the node report in a file and uses the node name as the prefix of the filename.
Generate or View All Nodes Report	After you select this option, no further action is required. All nodes in the NMS database (specified in *cascadeview.cfg*) are included in the report.
Generate or View Network/Trunk/Circuit Report	When you select the Network, Trunk, or Circuit option, the system prompts you for the network number. Enter the network number to generate a network, trunk, or circuit report for the specified network. Press Enter without specifying a network number to generate a network, trunk, or circuit report for all networks. You can view the network, trunk, or circuit report until you select the Generate option to generate another report.
Generate or View IP Reports	To select this option: • Select the Report menu option (IP Reports). • Then select IP Interface, BGP Config, or Route Maps for the report type. • Specify the name of the switch when prompted. The system saves the IP report in a file and uses the report type as the filename prefix. For example, for an IP Interface report, the filename prefix is "ipinterface."
Where are reports sent?	All reports are sent to the */opt/CascadeView.var/cvReport* directory of the user's HOME.

Troubleshooting Network Problems

A network is usually a complex system of many interconnected hardware and software components. Because of this inherent complexity, the problems that occur in networks tend to be complex as well.

You need to prepare to resolve network problems before they occur. Three things you can do to prepare for these problems are:

1. Know your network components.
2. Know your network problem solving tools.
3. Have a troubleshooting process in place.

This section will help you develop such a process and understand how to use this guide in implementing that process.

Know Your Network Components

Take an inventory of your network hardware and software components from time to time and understand the interfaces that connect them. Your network components and their interfaces will eventually act as test points — places in the network for isolating problems — when you perform your troubleshooting tasks.

Figure 1-6 shows a sample network that consists of many types of network components, including Ascend switches. Some sample test points (TP) are indicated by arrows.

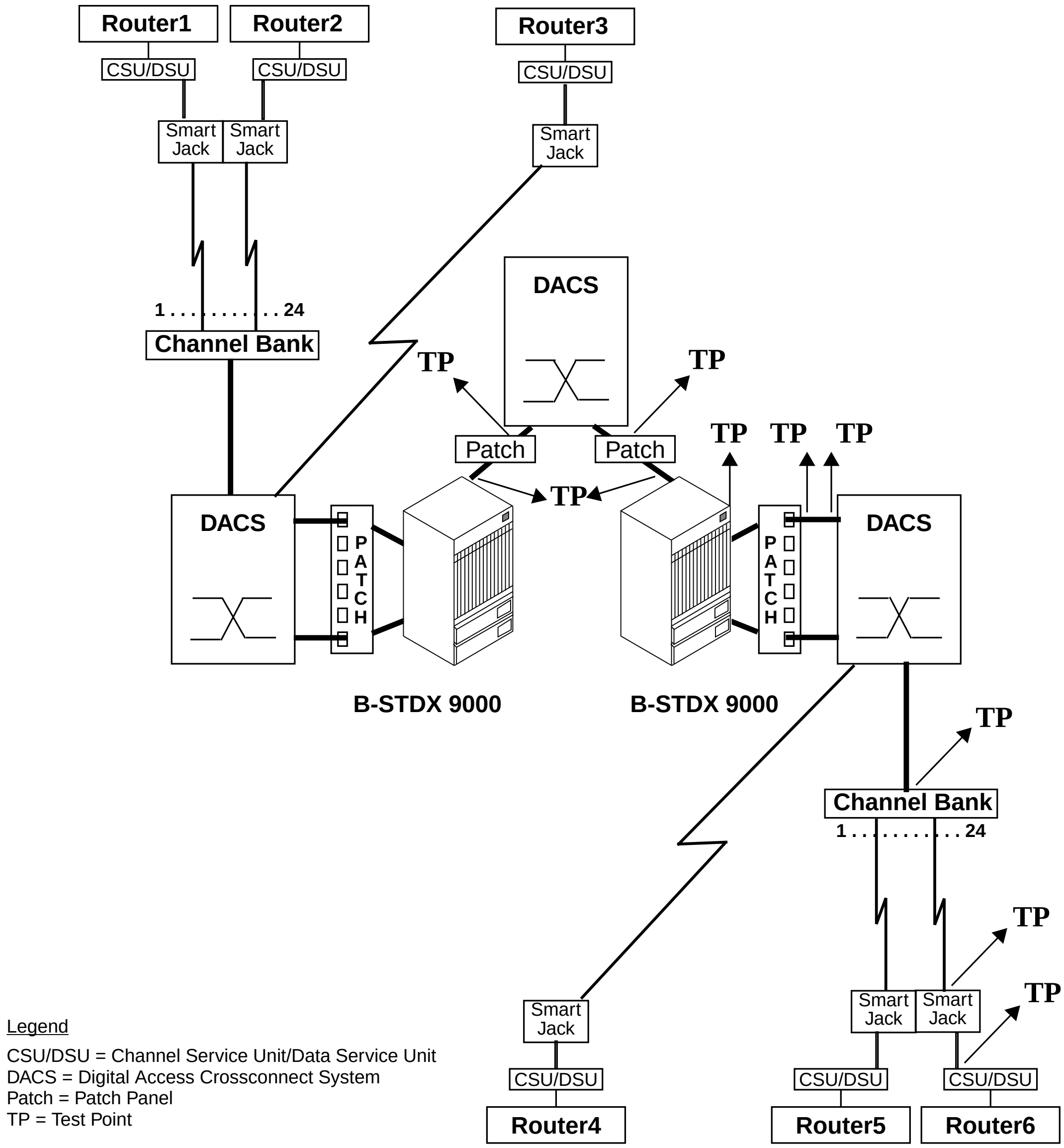


Figure 1-6. Sample Network

In some cases, knowledge of your network alone can help you isolate and correct problems quickly. For example, suppose that SNMP traps indicate that Router4 in the sample network is suddenly unreachable, but Router5 and Router6 have no problem exchanging data with the rest of the network. You could troubleshoot the problem as follows:

1. Based on your knowledge of the network, you know that Router4, Router5 and Router6 all send data and receive data via the same DACS.
2. Since Router5 and Router6 have no problems communicating with the rest of the network, the DACS is probably not the source of the problem.

3. You take the following action:
   - Check Router4's configuration.
   - Check Router4's CSU/DSU and its smart jack.
   - Check the link between Router4's smart jack and the DACS.

Know Your Troubleshooting Tools

Take an inventory of all Ascend and third-party hardware and software troubleshooting tools that are available to you, and understand the types of problems that they can troubleshoot.

Troubleshooting tools from Ascend include:

NavisCore — Provides configuration functions, performance statistics, traps/alarms and diagnostic capabilities.

Console Commands — Provides many of the same management functions as NavisCore through commands that you issue at the switch console.

NavisXtend Family of Products — Provides additional network management and troubleshooting tools such as bulk statistics and accounting statistics.

Many network troubleshooting tools are available from a variety of third-party vendors. Examples of these include:

Protocol Analyzers — Analyze packets transmitted on a network (usually LANs). Analyzers are typically used to analyze ISO Layer 3 (and above) protocols such as TCP/IP, Novell IPX, IBM SNA, and AppleTalk, but can also analyze ISO Layer 2 protocols (e.g., Ethernet and Token-Ring).

WAN Analyzers — Analyze packets transmitted over WAN links. They typically support all of the commonly found WAN interfaces (e.g., EIA/TIA-232 and ITU-T V.35) and protocols (e.g., HDLC, Frame Relay, and ISDN).

Optical Time Domain Reflectometer (TDR) — Tests fiber-optic cables for transmission problems.

Optical Power Source and Meter — Tests fiber-optic cables for transmission problems. They tend to be less expensive than optical TDRs.

Oscilloscope — Tests voltages on EIA/TIA-232 and EIA/TIA-422 interfaces.

Breakout Box — Provides status information on EIA/TIA-232-D leads between DTEs and DCEs.

Standard TCP/IP Commands — Standard TCP/IP commands such as PING and TRACEROUTE can help you determine if destinations are reachable.

Management Software — Routers, hubs, and other network devices typically come with graphical or command line management software that can be used for troubleshooting purposes.

Have a Troubleshooting Process in Place

When problems occur, you need a proven troubleshooting process to deal with the kinds of complex problems you will encounter in your network. You should base your troubleshooting process on the following guidelines:

1. Identify the problem.
2. Verify the problem.
3. Isolate the problem.
4. Take corrective action.

Identify the Problem

You cannot troubleshoot a network problem in a timely manner unless you are aware of its existence shortly after it occurs. Examples of indicators that inform you of network problems are:

LEDs — The light emitting diodes (LEDs) on network hardware components tell you whether the component is functioning properly. For example, green LEDs indicate that the component is functioning properly while red LEDs indicate that the component is malfunctioning or is not operational.

Traps — Traps (also known as alarms, alerts and events) are SNMP messages that indicate that some type of network event has occurred. Some traps indicate serious problems while other traps indicate normal events. See Chapter 15, "Managing Traps" for more information on traps.

Network Map Object Colors — In NavisCore, network objects (such as switches) change colors to indicate status, such as a change from green to red to indicate that a problem exists. See "Monitoring the Network Map" on page 1-4 for more information on map object colors.

User Complaints — Any network problem that disrupts end-user communications will eventually result in user complaints and calls to Customer Service.

Verify the Problem

Verify the problem once you are notified that one has occurred. The NavisCore monitoring dialog boxes provide configuration and statistical information that help you to verify the existence of network problems.

For example, suppose that you receive a trap that indicates that a T1 physical port is down. You would view the monitoring dialog boxes for that port to see if packets are being transmitted or received.

Table 1-8 lists the categories of problems you can verify and the associated chapters that you should use while verifying them.

Table 1-8. Problem Categories and Chapter References

Problem Category	Chapter
Processor Modules and IOMs	Chapter 2
Links and Physical Ports	Chapter 2, Chapter 3, Chapter 4
Logical Ports (General)	Chapter 6
ATM Logical Ports	Chapter 7
IP	Chapter 8
Frame Relay Logical Ports	Chapter 9
SMDS	Chapter 10
ISDN	Chapter 11
Trunks	Chapter 12
ATM Circuits	Chapter 13
Frame Relay Circuits	Chapter 14
NavisCore/NMS	Chapter 17

Isolate the Problem

Isolate the problem once you have verified it. You can isolate the problem in several ways:

- Run diagnostics and loopbacks, which can narrow the problem to a specific area:
  - See Chapter 5, "Testing Modules, Ports, and Channels" for information on running diagnostics and loopbacks on processor modules, IOMs, physical ports, and channels.
  - See "Testing ATM Circuits" on page 13-90 for information on running OAM loopbacks on ATM circuits.
  - See "Testing Frame Relay PVCs" on page 14-54 for information on running loopbacks on Frame Relay PVCs.
- Correlate all the information you have gathered while identifying and verifying the problem. In some cases, you can isolate a problem by analyzing the sum of all the traps, statistical information, user complaints, and other information you collect.
- Review your network topology. In some cases, knowledge of your network topology alone can help you isolate a problem. See "Know Your Network Components" on page 1-12 for more information about topology and problem isolation.

Take Corrective Action

Corrective action can come in many forms, depending on the specific problem you have encountered.

When the source of the problem lies within your administrative control, you can take action yourself by, for example, reconfiguring your network or replacing malfunctioning components. Ascend technical support staff are available to help you whenever you need assistance solving network problems. See "Customer Support" on page -xl for more information.

In other cases, the source of the problem may not lie within your administrative control. For example, you may have isolated the source of the problem to a router at a customer site. If you determine that the problem lies outside your administrative control, compile all of the information you have gathered and share it with the administrative staff who will be responsible for resolving the problem.

Troubleshooting Process Flowchart

Figure 1-7 summarizes the troubleshooting process and lists the chapters that can help you during each phase of the process.

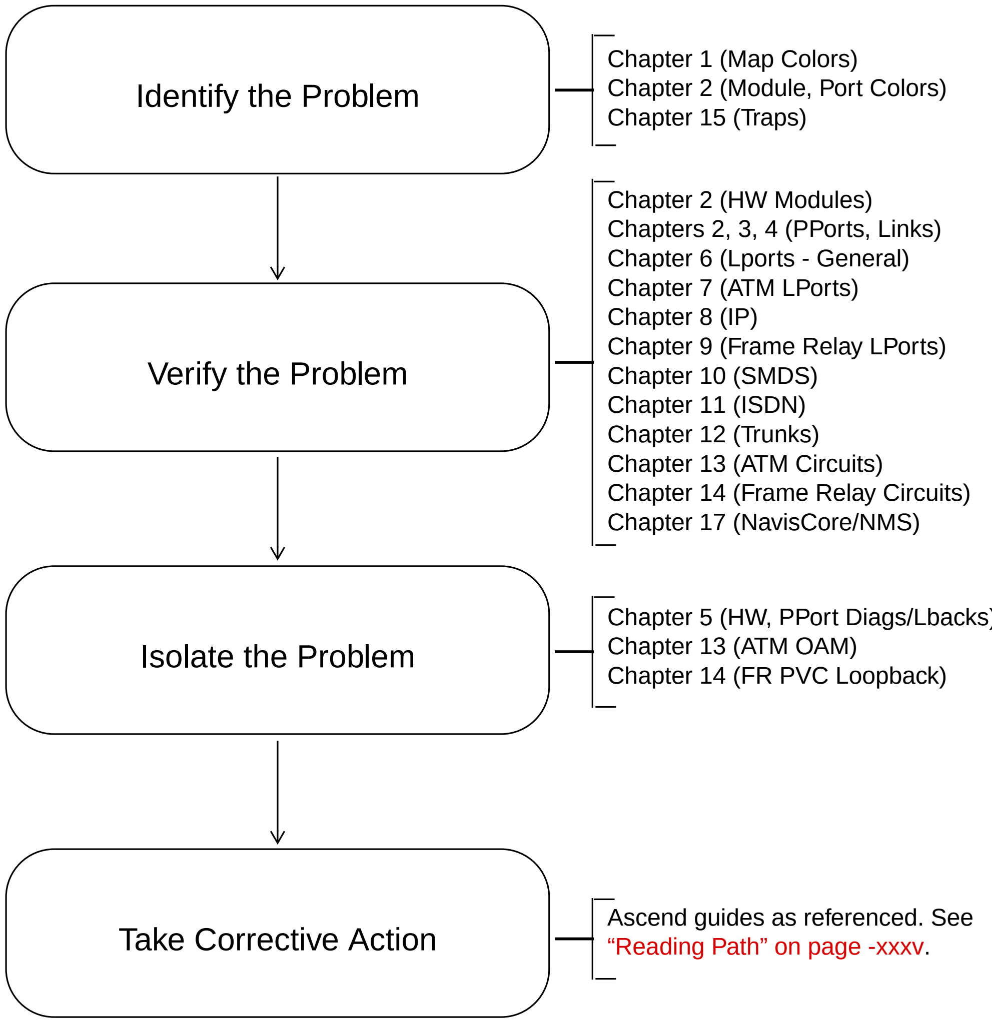


Figure 1-7. Troubleshooting Process Flowchart

2

Viewing Switch, Module, and Physical Port Details

This chapter explains how to view the status and hardware details of a switch, including its processor modules, I/O modules (IOMs), and physical ports.

Viewing Switch Status

This section describes how to view switch status from:

- The Monitor menu
- The Switch Back Panel dialog box

Viewing Switch Status from the Monitor Menu

To display status and configuration information for all switches on the network map:

1. From the Monitor menu, select Ascend Objects ⇒ Show All Switches. The Show All Switches dialog box appears (see Figure 2-1).

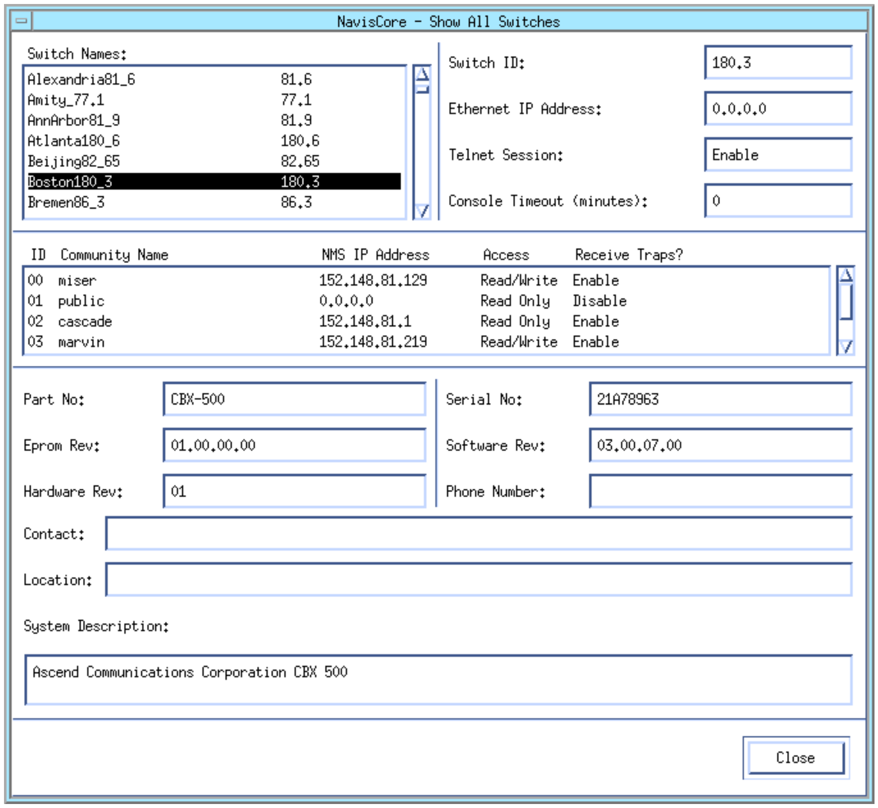


Figure 2-1. Show All Switches Dialog Box

2. Select the name of the switch from which you want to retrieve status information.

Table 2-1 describes the dialog box fields.

Table 2-1. Show All Switches Fields

Field	Displays...
Switch ID	The switch number used as the host assignment in the switch's internal IP address.
Ethernet IP Address	The external IP address for the switch's LAN connection from the CP, SP, or NP to the NMS. You assign this IP address to the Ethernet module during configuration.
Telnet Session	Whether Telnet access to the switch is enabled or disabled.
Console Timeout (minutes)	How long (in minutes) the console can be inactive before it is logged off.
Community Name	The name used to control access to the switch's configuration. The Community Name is used with the NMS IP address to identify whether the specified NMS has authority to send intrusive commands to the switch. The default name for the first NMS is *cascade* (case-sensitive).

Table 2-1. Show All Switches Fields (Continued)

Field	Displays...
NMS IP Address	The address of the NMS configured to communicate with the selected switch. Traps generated from the selected switch are sent to this IP address. To send SNMP commands to the switch and to download switch software, the NMS IP address must match the switch IP address.
Access	The access privileges between the NMS and the selected switch. The first NMS always has read/write access. An NMS with read-only access can receive traps but cannot send write commands to the switch.
Receive Traps	Whether traps generated from the selected switch are sent to this NMS IP address. An NMS with read-only privileges can receive traps but is restricted from sending write commands to the switch.
Part No.	The part number of the CP, SP or NP.
Eprom Rev	The switch's EPROM revision level, 2.0 or greater.
Hardware Rev	The CP, SP, or NP hardware revision level.
Serial No.	The switch serial number.
Software Rev	The revision number for the firmware currently running on the switch.
Phone Number	The telephone number for the contact person.
Contact	The name of the contact person.
Location	The physical location of the switch.
System Description	The switch type. This parameter is taken directly from the switch and appears only if the NMS is actively communicating with the selected switch.

Viewing Switch Status from the Switch Back Panel Dialog Box

To view switch status from the Switch Back Panel dialog box:

1. Select the switch object (B-STDX, CBX, or GX) on the network map.

1. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears. See “Viewing Switch Details” on page 2-9 for more information on this dialog box.

2. Select Actions ⇒ View Switch Attributes.

3. Choose Go. The Show Switch Attributes dialog box appears (see Figure 2-2).

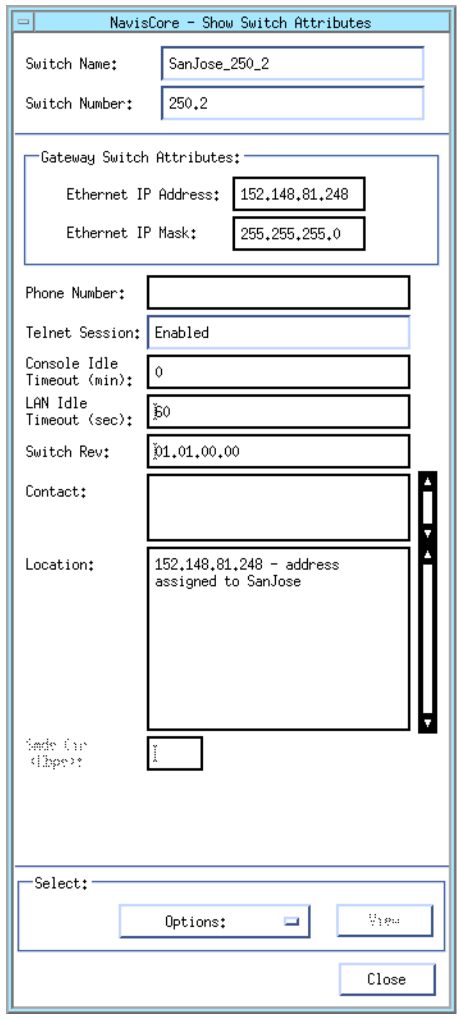


Figure 2-2. Show Switch Attributes Dialog Box

Table 2-2 describes the option menu selections. Table 2-3 describes the fields on the Show Switch Attributes dialog box.

Table 2-2. Show Switch Attributes Option Menu Selections

Option	Function
NMS Entries	Displays a table of entries, one for each NMS that can communicate with the switch. See Table 2-1 for a description of the fields in this table.
Tuning	Displays a dialog box that shows the following switch-tuning attributes: *Reroute Count* – The number of virtual circuits for which the switch requests a reroute during a single reroute batch event. *Reroute Delay (sec.)* – The delay, in seconds, between each reroute batch event. See the *NavisCore NMS Getting Started Guide* for more information on Reroute Count and Reroute Delay functions.
Accounting	Displays NavisXtend accounting attributes. See the *NavisXtend Accounting Server Administrator's Guide* for more information.
Clock Sources	Displays switch clock sources. See the *NavisCore NMS Getting Started Guide* or the *NavisCore Physical Interface Configuration Guide* for more information on clock sources.
Console Authen...	Displays a dialog box that shows the following console authentication information: *Authentication Domain Name* – The authentication domain name for the switch. *Authentication* – Enabled if console login authentication is enabled for the switch. Otherwise, Disabled. See the *NavisCore NMS Getting Started Guide* for more information on console authentication.
Bulk Stats	Displays a dialog box that shows the following bulk statistics attributes (if applicable): *Bulk Transfer State* – The bulk statistics transfer state (Active, Inactive, Pending or Failed). *Bulk Collector Address* – The IP address of the statistics server to which the switch transfers bulk statistics data. See the *NavisXtend Statistics Server User's Guide* for more information.
RIP Configuration	Displays RIP configuration parameters for switches that run IP Navigator. See "Viewing the Logical Port RIP Parameters" on page 8-11 for a description of these parameters.
Trap Config...	Displays the trap configuration for the switch. See "Managing the Trap Configuration for a Switch" on page 15-12 for more information.
Time Server...	Displays the time server configuration. See the *NavisCore NMS Getting Started Guide* for more information on the time server configuration.
Set Switch Time	Displays the switch time setting. See the *NavisCore NMS Getting Started Guide* for more information on the switch time setting.

Table 2-3. Show Switch Attributes Fields

Field	Displays...
Switch Number	The switch number used as the host assignment in the switch's internal IP address.
Ethernet IP Address	The external IP address for the switch's LAN connection from the NP/SP/CP to the NMS. You assign this IP address to the Ethernet module in the switch during configuration.
Ethernet IP Mask	The mask used to partition the IP address into network number, subnetwork number, and host.
Phone Number	The phone number of an administrative contact.
Telnet Session	Whether Telnet access to the switch is enabled or disabled.
Console Timeout (minutes)	How long (in minutes) the console can be inactive before it is logged off.
LAN Idle Timeout	The idle timeout interval, in seconds, for the Ethernet interface that connects the switch to the NMS. If the Ethernet interface receives no valid IP traffic during this period, the interface is marked as idle and will not be used for outbound traffic. Receipt of a valid IP packet restarts the idle timeout counter and reactivates the interface if it is idle.
Switch Rev.	The switch software revision level.
Contact	The name of the contact person.
Location	The physical location of the switch.
SMDS (in Kbps)	The committed information rate (CIR), in Kbps, allocated to the SMDS virtual paths originating at this switch. See the *NavisCore SMDS Configuration Guide* for more information.
Number of Power Supplies	The number of power supplies installed in the switch.

Viewing Switch Subnets

To display a list of subnets defined for the selected switch:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show All Subnets. The Show All Subnets dialog box appears (see Figure 2-3).

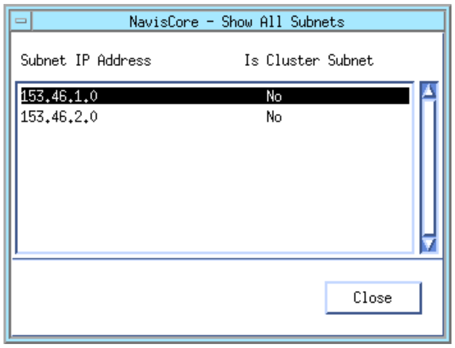


Figure 2-3. Show All Subnets Dialog Box

This dialog box displays the following information:

Subnet IP Address — Identifies the subnet IP addresses for this switch. A subnet divides a large network into smaller pieces. Subnets support a three-level hierarchy in which the host number field is divided into two parts: the subnet number and the host number on that subnet.

Is Cluster Subnet — Displays Yes or No to indicate whether the subnet is part of a cluster.

Viewing Switch Clusters

To display a list of clusters defined for a selected switch:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show All Clusters. The Show All Clusters dialog box appears (see Figure 2-4).

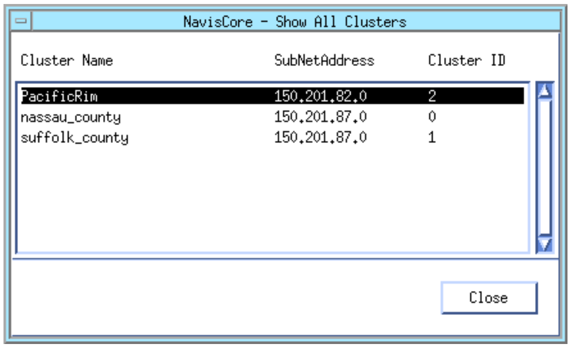


Figure 2-4. Show All Clusters Dialog Box

This dialog box displays the following information:

Cluster Name — Displays the subnet IP address for a cluster subnet.

Subnet Address — Identifies the subnet IP address for this cluster. A subnet divides a large network into smaller pieces. Subnets support a three-level hierarchy in which the host number field is divided into two parts: the subnet number and the host number on that subnet.

Cluster ID — Displays a value from 0 to 7 to indicate the cluster ID part of the IP address.

Viewing Switch Details

The Show Detail function polls the switch for the appropriate operational status of the power supplies, fan modules, processor modules, and IOMs.

To view details of a switch:

1. Select the appropriate switch object (B-STDX, CBX, or GX) on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears. The exact appearance of the Switch Back Panel dialog box depends on the type of switch you are monitoring. However, the back panels are similar in appearance for B-STDX 8000/9000 and CBX 500 switches.

Figure 2-5 shows the Switch Back Panel dialog box for a B-STDX 8000/9000 switch.

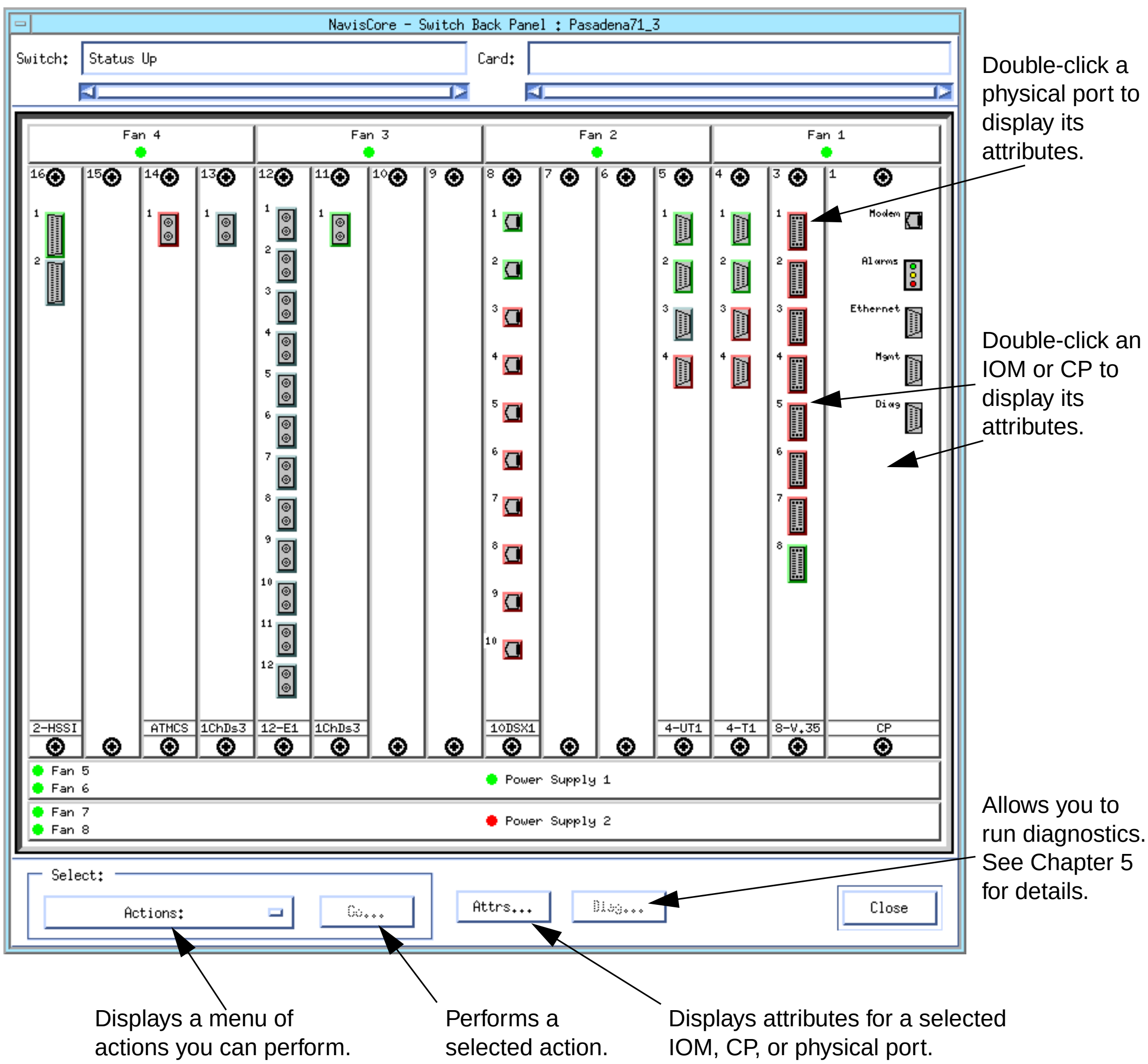


Figure 2-5. Switch Back Panel Dialog Box (B-STDX 8000/9000)

Figure 2-6 shows the Switch Back Panel dialog box for a CBX 500 switch.

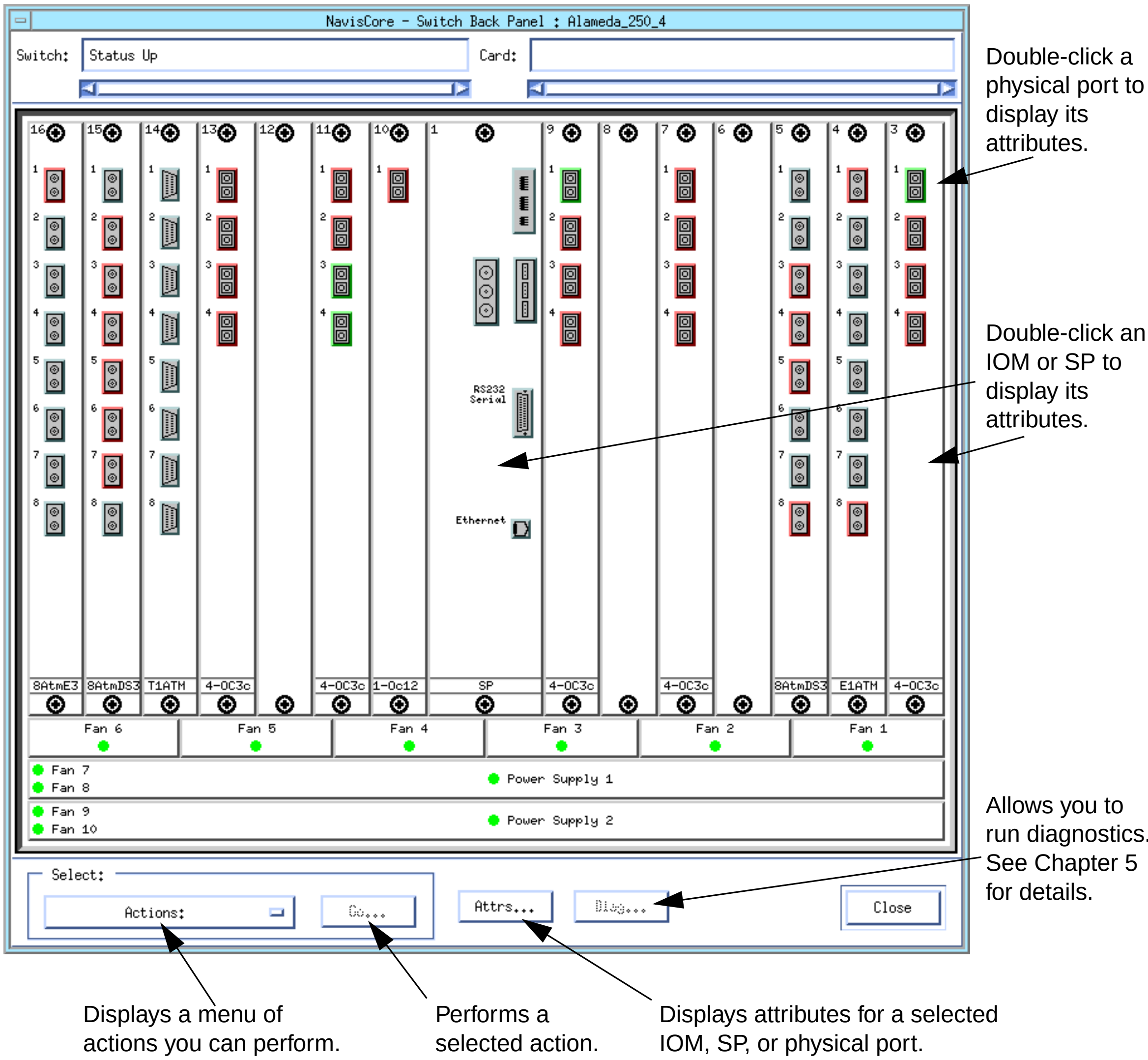


Figure 2-6. Switch Back Panel Dialog Box (CBX 500)

Figure 2-7 shows the Switch Back Panel dialog box for a GX 550 switch.

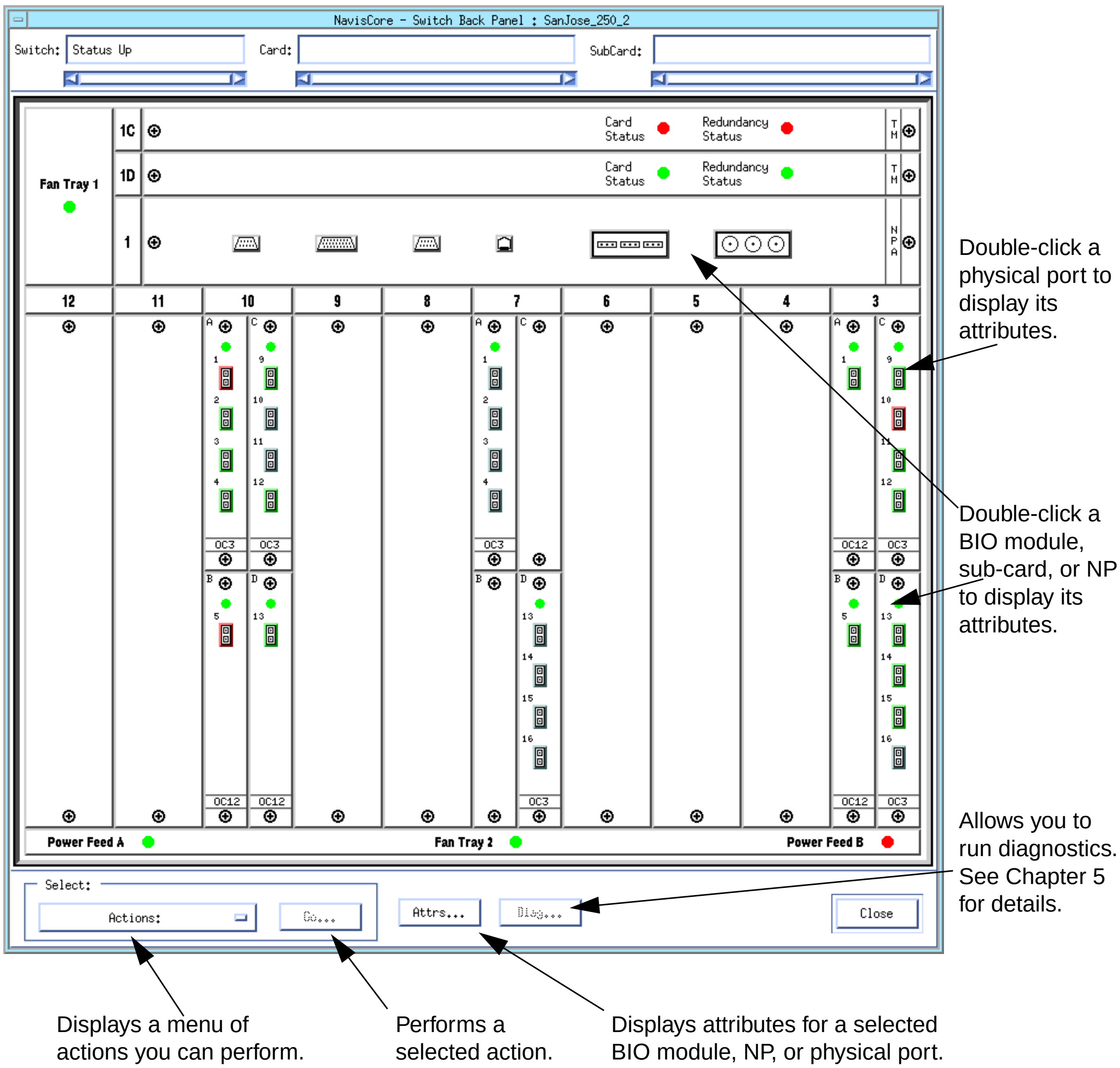


Figure 2-7. Switch Back Panel Dialog Box (GX 550)

Table 2-4 describes the options menu and buttons on the Switch Back Panel dialog box.

Table 2-4. Switch Back Panel Dialog Box Option Menu and Buttons

Button/Options Menu	Function
Actions	Select from a list of several options. Table 2-5 describes these options.
Go	Perform a selected option.
Attrs	View attributes for the selected item: an IOM, BIO module, CBX 500 SP, B-STDX 8000/9000 CP, GX 550 NP, or physical port. You can also select the item and double-click to view the corresponding View Attributes dialog box.
Diag	Access diagnostics for a selected module. See Chapter 5, "Testing Modules, Ports, and Channels" for details.
Close	Exit this dialog box.

Table 2-5. Actions Option Menu Selections

Option	Function
View Switch Attributes	View the configured switch attributes, including the local IP address of the switch. For more information, see "Viewing Switch Status from the Switch Back Panel Dialog Box" on page 2-4.
View Front Panel	View the front panel of the switch. For more information, see "Viewing the Front Panel" on page 2-15.
View Port Redundancy	View the physical port redundancy configuration. For more information, see "Viewing Physical Port Redundancy" on page 2-66.
ISDN Status (*B-STDX only*)	View call status for ISDN IOMs in B-STDX 8000/9000 switches. For more information, see Chapter 11, "Monitoring ISDN."
Enable Popup Help	Enables popup help. For more information, see "Using Popup Help" on page 2-14.
Disable Popup Help	Disables popup help. For more information, see "Using Popup Help" on page 2-14.

Status Light Indicators

Status lights on the Switch Back Panel dialog box indicate the operational status of fans and power supply units as follows:

- A green LED indicates that the fan or power supply unit is operational.
- A red LED indicates that the fan or power supply unit is not operational.
- A blue LED on a fan or power supply unit indicates that the NMS cannot access the unit for status.

> When an A or B DC power-feed fails on a CBX 500 switch, the green LEDs flash on all power supplies. Since all the LEDs are not synchronized, watch the LEDs of one power supply rather than focusing on the blinking pattern of all power supplies.

Physical Port Colors

Physical ports use color to indicate operational status. They use the following color scheme:

- A gray physical port indicates that the port is unknown. This condition usually occurs if the configuration does not exist or a logical port is not defined.
- A green physical port indicates that the port is accurately configured and operational.
- A red physical port indicates that the port is configured but has an admin status of Down, an operational status of Down, and/or all logical ports have an admin status or an operational status of Down.
- A cyan physical port indicates that the port is configured but one or more (but not all) logical ports have an admin status or an operational status of Down. Note that cyan is a light blue color.

  To determine the specific logical ports that are down, check your trap event browser or log, or use NavisCore to check logical port status. See Chapter 15, “Managing Traps” for more information on traps. See “Viewing Logical Port Status” on page 6-1 for more information on logical port status.

IOM and Processor Module Colors

IOMs and processor modules also use color to indicate their operational status. They use the following color scheme:

- A red module indicates that the module has failed or is not present.
- A yellow module indicates that the module is in a marginal state or out of sync.
- A gray module indicates that it is operational.

Subcard Colors

BIO subcards on GX 550 switches also use color to indicate their operational status. They use the following color scheme:

- A red subcard indicates that it has failed or is not present.
- A yellow subcard indicates that it is in a marginal state or “out of sync.”
- A gray subcard indicates that it is operational.

Using Popup Help

Popup Help provides quick access to summary information about a selected GX 550 NP, CBX 500 SP, B-STDX 8000/9000 CP, IOM, or physical port.

To enable Popup Help:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Select Actions ⇒ Enable Popup Help.
4. Choose Go.
5. Drag the pointer of your mouse to the SP, CP, NP, IOM, or physical port for which you want to obtain summary information. The information appears after a couple seconds.

To disable Popup Help:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Select Actions ⇒ Disable Popup Help.
4. Choose Go.

Viewing the Front Panel

The Show Switch Front Panel dialog box displays the front panel of a switch. To view a switch front panel:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Select Actions ⇒ View Front Panel.
4. Choose Go. The Switch Front Panel dialog box appears. The exact appearance of the Switch Front Panel dialog box depends on the type of switch you are monitoring. Figure 2-8 shows the Switch Front Panel dialog box for a B-STDX 8000/9000 switch.

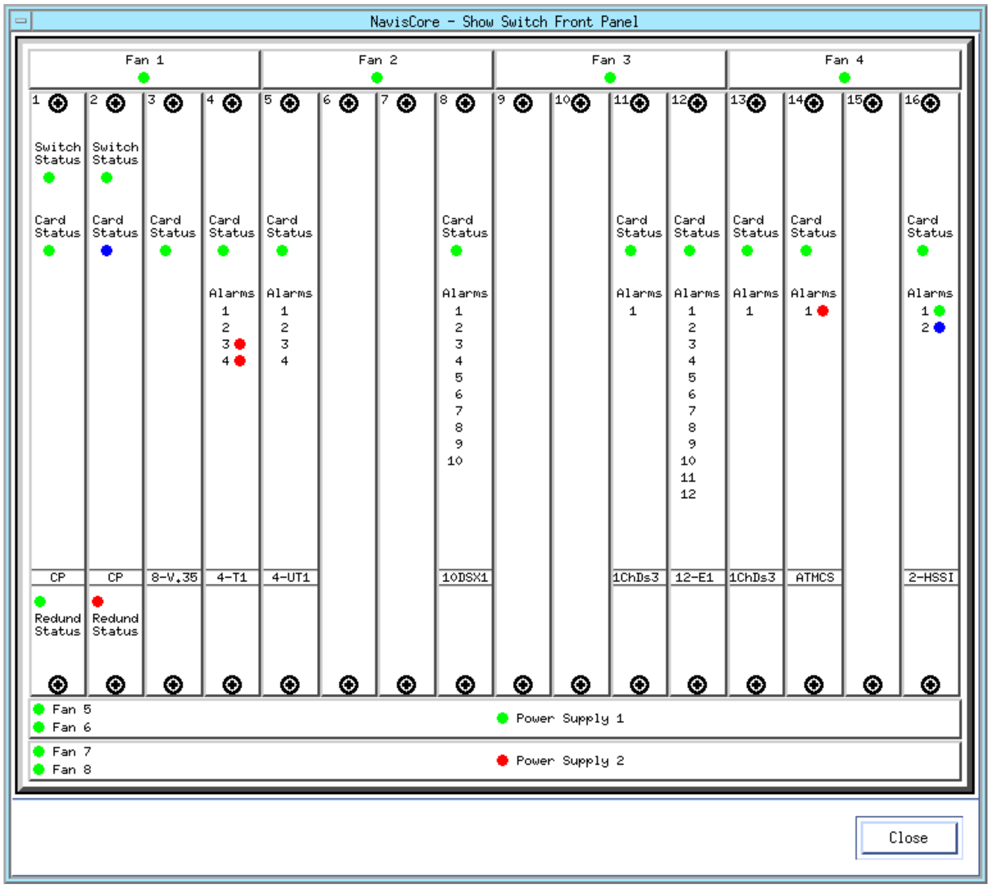


Figure 2-8. Show Front Panel Dialog Box (B-STDX 8000/9000)

Figure 2-9 shows the Switch Front Panel dialog box for a CBX 500 switch.

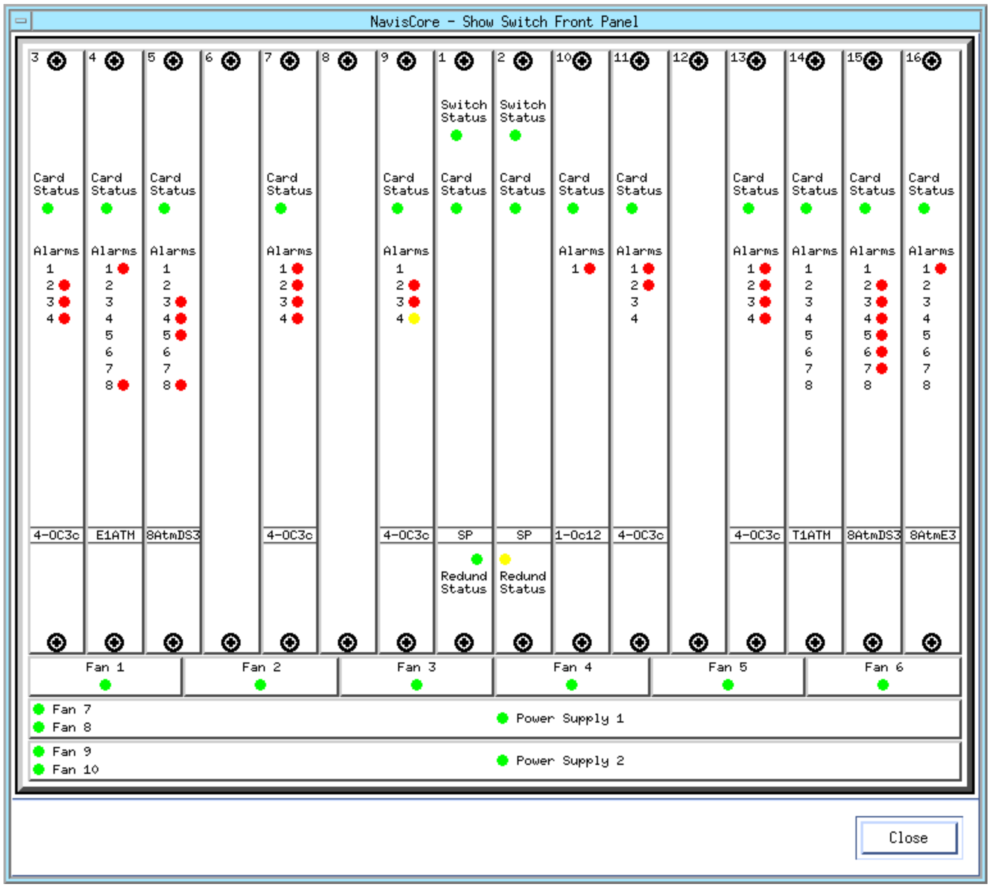


Figure 2-9. Show Front Panel Dialog Box (CBX 500)

Figure 2-10 shows the Switch Front Panel dialog box for a GX 550 switch.

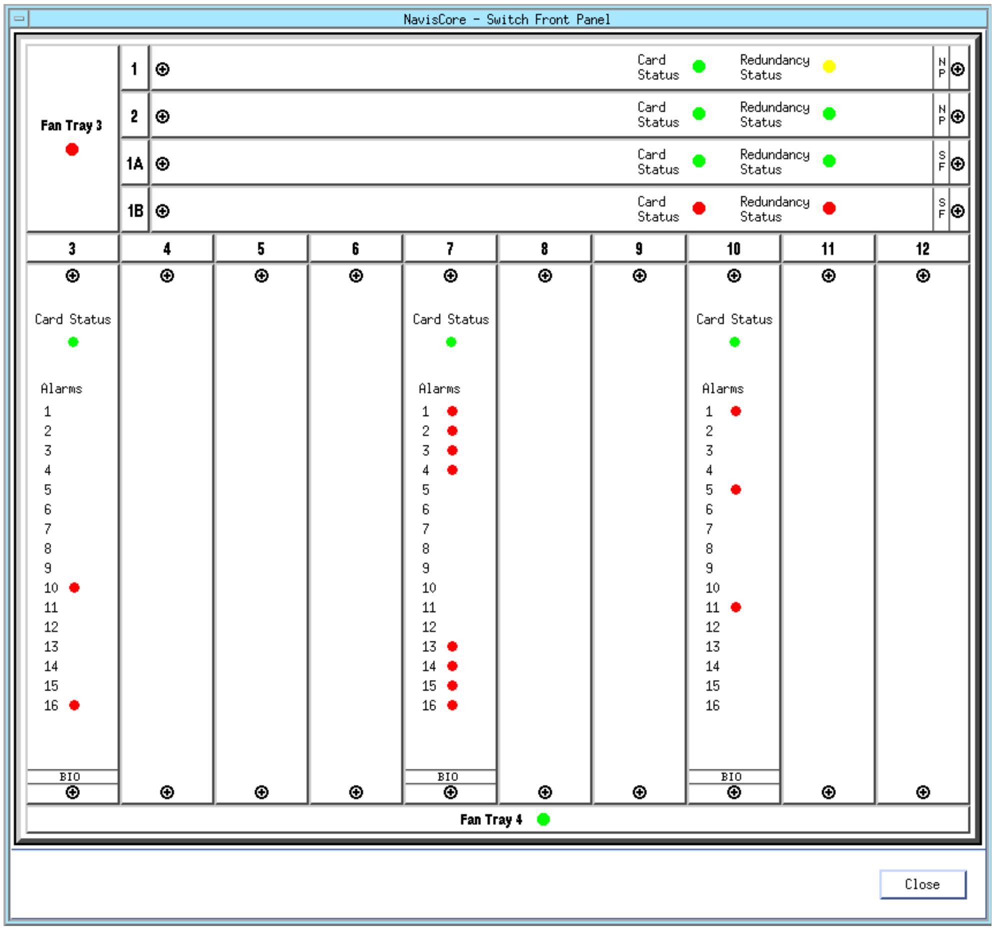


Figure 2-10. Show Front Panel Dialog Box (GX 550)

Switch Front Panel Status Light Indicators

As with the Switch Back Panel dialog box, status lights indicate the operational status of the fans, power supply units, and IOMs.

Switch and Module Status Light Indicators

- A green LED indicates the module is operational.
- A red LED indicates the module is not operational.
- A blue LED indicates that the NMS cannot access the processor module, the fan and/or the power supply unit for status.

Alarm Status Light Indicators

The number and type of alarms differ depending on the type of module you are using.

- No LED indicates there are no alarm conditions.
- A red LED indicates a red alarm condition. For various IOMs, a red alarm condition occurs when a loss of signal occurs.

  A flashing red LED may indicate a blue alarm condition. This condition occurs when an intermediate device, such as an office channel unit (OCU), that is currently in red alarm passes alarm information along to the device at the opposite end (such as a T1 physical port).
- A yellow LED indicates a yellow alarm condition. For various IOMs, this alarm indicates that a remote device (such as a CSU) is transmitting a red alarm. The remote device is not receiving any transmission signals from the circuit and the circuit is acting as a one-way link.

Viewing CP and SP Status

To view CP (B-STDX 8000/9000) or SP (CBX 500) information:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 2-5 on page 2-9 or Figure 2-6 on page 2-10).
3. Double-click the CP or SP slot. The Select Card dialog box appears.
4. Select Active or Standby.
5. Choose OK. The View Card Attributes dialog box appears (see Figure 2-11 for CP attributes; Figure 2-12 for SP attributes).

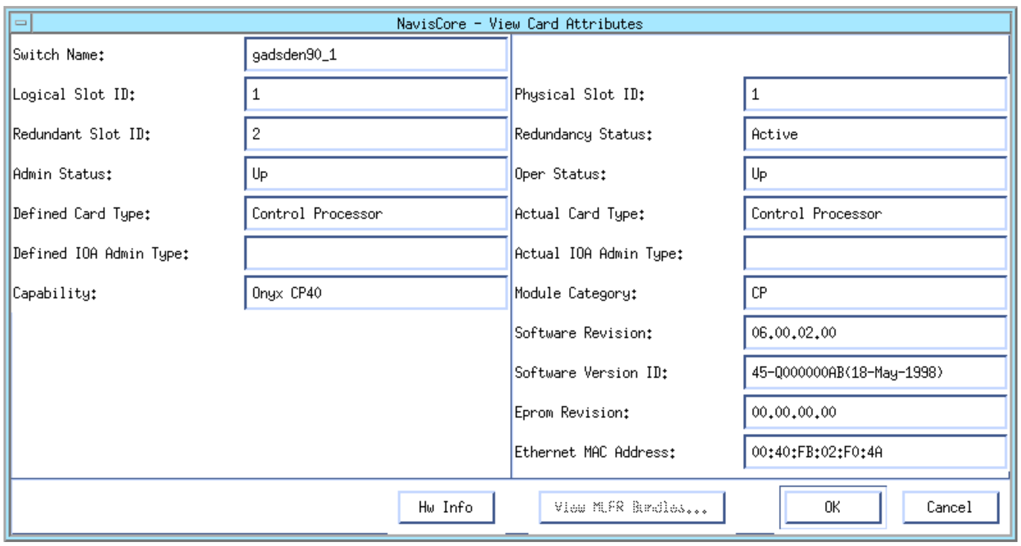


Figure 2-11. View Card Attributes Dialog Box (CP)

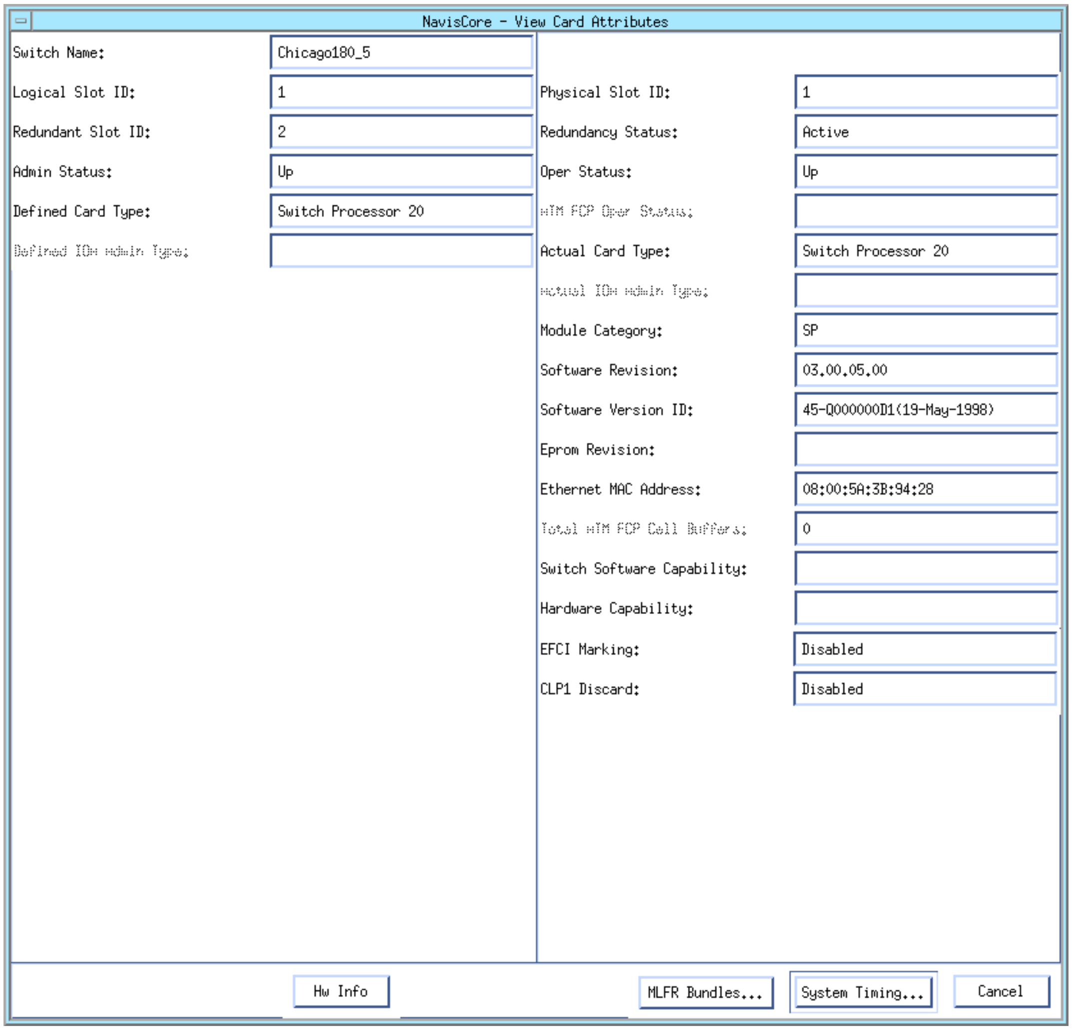


Figure 2-12. View Card Attributes Dialog Box (SP)

Table 2-6 describes the buttons on the View Card Attributes dialog box.

Table 2-6. View Card Attributes Dialog Box Buttons (CP and SP)

Button	Description
Hw Info	Allows you to access hardware information. See "Viewing Manufacturing Information" on page 2-39 for more information on viewing hardware information.
MLFR Bundles	Allows you to access Multilink Frame Relay (MLFR) bundles information. See "Monitoring Multilink Frame Relay" on page 9-19 for more information on viewing MLFR bundles.
System Timing (*SP Only*)	Allows you to access configured system-timing options. See "Viewing System-Timing Options" on page 2-25 for more information on viewing system-timing options.

Table 2-7 describes the CP and SP attribute fields.

Table 2-7. View Card Attributes Fields (CP and SP)

Field	Displays...
Switch Name	The name of the switch in which this CP or SP resides.
Logical Slot ID	The number of the slot in which this CP or SP is configured.
Redundant Slot ID	The number of the slot of the redundant CP or SP (if applicable).
Admin Status	One of the following values: *Up (Default)* – The CP or SP becomes fully operational at switch start-up. To become operational, the module gets its application code from the PCMCIA hard drive, which resides in the adapter module (for example, the SPA for an SP). *Down* – The CP or SP does not come online at switch start-up. The configuration is saved in the switch configuration table but is not downloaded to the switch. Use this option when running foreground diagnostics. *Maintenance* – The CP or SP does not receive the application code at switch start-up. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem.
Defined Card Type	The configured model type for this CP or SP. For the CP, this field displays “Control Processor” only. For the SP, examples include Switch Processor 20 (for SP Model 20) or Switch Processor 40 (for SP Model 40).
Defined IOA Admin Type	Does not apply.
Capability (*CP only*)	The CP’s capability (such as CP Basic or CP Plus).
Physical Slot ID	The number of the slot in which the CP or SP resides.
Redundancy Status	The redundancy status of this CP or SP: Active, Standby, or N/A.
Oper Status	The operational status of this CP or SP (e.g., “Up” or “Down”).
ATM FCP Oper Status (*SP only*)	Does not apply.
Actual Card Type	The actual CP or SP type as defined by the firmware.
Actual IOA Admin Type	Does not apply.
Module Category	The type of processor module, CP or SP.
Software Revision	The switch software revision number.
Software Version ID	The build number and date of the switch code software.
Eprom Revision	The EPROM firmware revision number.

Table 2-7. View Card Attributes Fields (CP and SP) (Continued)

Field	Displays...
Ethernet MAC Address	The Ethernet MAC address, in hexadecimal, of this CP or SP.
Total ATM FCP Cell Buffers (*SP only*)	Does not apply.
Switch Software Capability (*SP only*)	Does not apply.
Hardware Capability (*SP only*)	Does not apply.
EFCI Marking (*SP only*)	Whether ATM Explicit Forward Congestion Indication (EFCI) marking is enabled or disabled. When EFCI is enabled, the switch determines if congestion (or impending congestion) exists in a node in an ATM network. If you do not enable EFCI for the SP, you can still enable it for individual physical ports. If enabled, the congested node modifies the EFCI bit in the ATM cell header to indicate congestion. If the equipment connected to the switch can use the EFCI bit to adjust its transmission rate, it may lower the connection cell rate to relieve congestion.
CLP1 Discard	Whether ATM Cell Loss Priority 1 (ATM CLP-1) discard is enabled or disabled. If enabled, CLP-1 cells are discarded under certain conditions.

Viewing NP Status

To view NP (GX 550) information:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (Figure 2-7 on page 2-11).
3. Double-click on the NP slot. The View Card Attributes dialog box appears (see Figure 2-13).

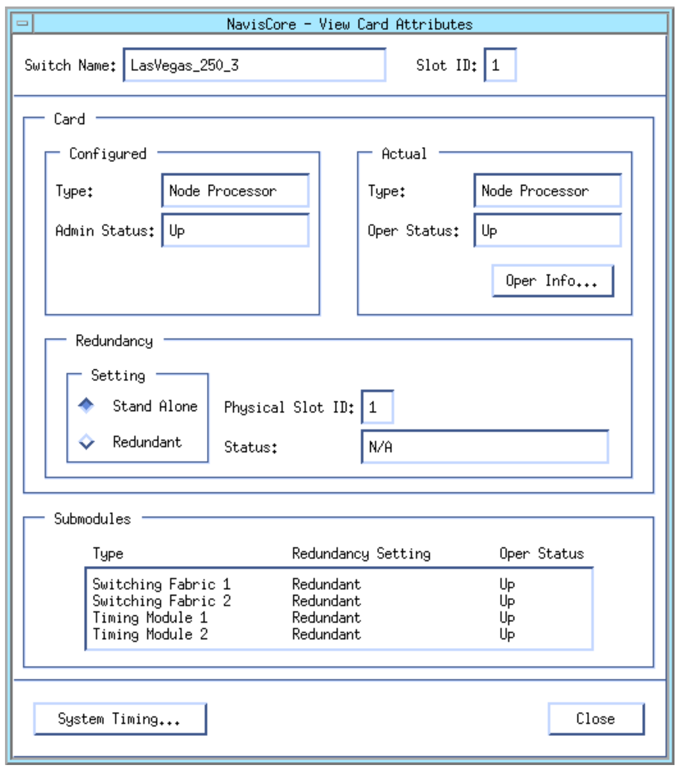


Figure 2-13. View Card Attributes Dialog Box (NP)

Table 2-8 describes the buttons on the View Card Attributes dialog box.

Table 2-8. View Card Attributes Dialog Box Buttons (NP)

Button	Function
Oper Info	Displays manufacturing information about the NP. See "Viewing Manufacturing Information for an NP" on page 2-40 for more information.
System Timing	Displays configured system-timing options. See "Viewing System-Timing Options" on page 2-25 for more information.
Close	Exits the dialog box.

Table 2-9 describes the NP attribute fields.

Table 2-9. View Card Attributes Fields (NP)

Field	Displays...
Switch Name	The name of the switch in which this NP resides.
Slot ID	The number of the slot in which this NP is configured.
Configured	
Type	The configured NP type.
Admin Status	One of the following: *Up (Default)* – The NP becomes fully operational at switch start-up. To become operational, the module gets its application code from the PCMCIA hard drive, which resides in the NPA module. *Down* – The NP does not come online at switch start up. The configuration is saved in the switch configuration table but is not downloaded to the switch. Use this option when running foreground diagnostics. *Maintenance* – The NP does not receive the application code at switch start-up. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem.
Actual	
Type	The actual module type as defined by the firmware.
Oper Status	The operational status of this NP (e.g., “Up”).
Redundancy	
Setting	The redundancy setting, either Stand Alone or Redundant.
Physical Slot ID	The number of the slot in which the NP resides.
Status	The redundancy status (if applicable), either active or standby.
Submodules	
Type	Lists the types of submodules in the NP: Switching Fabric 1, Switching Fabric 2, Timing Module 1 or Timing Module 2.
Redundancy Setting	The redundancy setting of each submodule: Stand Alone or Redundant.
Oper Status	The operational status of this submodule (e.g., “Up”).

Viewing System-Timing Options

You can view the configured system-timing options for the CBX 500 SP and the GX 550 NP.

To view system-timing options:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 2-6 on page 2-10 or Figure 2-7 on page 2-11).
3. Double-click on the SP or NP slot.

   If you select an SP, the Select Card dialog box appears. Choose Active or Standby. The View Card Attributes dialog box appears.

   If you select an NP, the View Card Attributes dialog box appears.
4. Choose System Timing. The Show System Timing dialog box appears (see Figure 2-14).

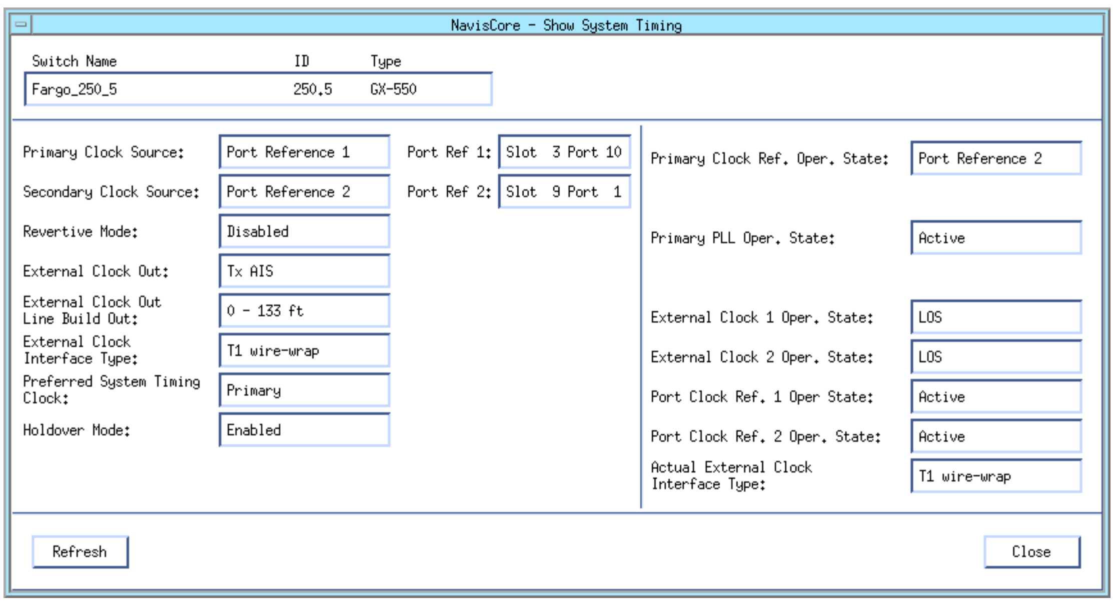


Figure 2-14. Show System Timing Dialog Box

The Show System Timing dialog box displays the configured timing settings and monitors the clock status. Table 2-10 on page 2-26 describes these fields.

5. Choose Refresh to update this information.
6. Choose Close to return to the View Card Attributes dialog box.

Table 2-10. Show System-Timing Fields

Field	Displays...
Primary and Secondary Clock Source	The configured primary and secondary clock sources: *Internal* – The switch uses the Stratum 3 clock on the SPA and NPA module as the primary (or secondary) clock source. *External Clock 1* – The switch uses the primary external clock connection on the SPA and NPA module to provide the primary (or secondary) clock source. *External Clock 2* – The switch uses the secondary external clock connection on the SPA and NPA module to provide the primary (or secondary) clock source. *Port Reference 1* – This option appears only if you first configure one of the physical ports on the switch as the Primary System Clock Source. The switch uses an incoming clock signal on a selected physical port as the primary (or secondary) clock source. *Port Reference 2* – This option appears only if you first configure one of the physical ports on the switch as the Secondary System Clock Source. The switch uses an incoming clock signal on a selected physical port as the primary (or secondary) clock source.
Revertive Mode	The configured revertive mode (if the primary clock source fails): *Enabled* – If the switch loses the primary clock source, causing the secondary clock source to take over system timing, the system automatically reverts back to the primary clock source when it becomes available again. *Disabled* – If the switch loses primary clock source, the secondary clock source takes over system timing. However, the system will not automatically revert back to the primary clock source once it is restored. ***Note:*** *If you disable Revertive Mode, use the Manual Restore button on the Set System Timing dialog box to revert back to the primary clock source.*
External Clock Out	The following External Clock Out options: *Primary* – The external clock output references the clock that the switch uses as the primary source. *Secondary* – The external clock output references the clock that the switch uses as the secondary source. *Loopback ext1* – The clock that is wired to the external clock input #1 on the SPA and NPA module is fed directly to the external clock output jack. *Tx AIS* – In the event of system clock loss, the external clock output transmits an AIS signal.
External Clock Out Line Build Out	The length of the external clock line (in feet) connected to the external clock output on the SPA and NPA module.
External Clock Interface Type	The configured external clock interface type: *T1 wire-wrap* (the default) – The SP/NP accepts T1 timing inputs and provides T1 timing outputs. *E1 BNC* – The SP/NP accepts E1 timing inputs and provides E1 timing outputs.

Table 2-10. Show System-Timing Fields (Continued)

Field	Displays...
Preferred System Timing Clock	The following Preferred System-Timing Clock methods: *Primary* – The switch uses the clock source specified in the Primary Clock Source field. *Secondary* –The switch uses the clock source specified in the Secondary Clock Source field. ***Note:*** *If the primary clock source becomes unavailable, the system automatically provides the secondary clock source to the IOMs.*
Holdover Mode	Whether Stratum 3 clock holdover mode is enabled or disabled. When enabled, an SP or NP maintains Stratum 3 timing accuracy for 24 hours in the event that an SP's or NP's timing reference source fails. The clock's local oscillator in the SP or NP is not locked by an external synchronization reference, but instead uses storage techniques to maintain its accuracy. When clock holdover mode is disabled, it uses no storage techniques to sustain accuracy.
Port Ref 1	The slot number and physical port number of the physical port that acts as the Primary System Clock Source. This means that the switch uses an incoming clock signal on a selected physical port as the primary clock source. This field is blank if a physical port is not used as the Primary System Clock Source.
Port Ref 2	The slot number and physical port number of the physical port that acts as the Secondary System Clock Source. This means that the switch uses an incoming clock signal on a selected physical port as the secondary clock source. This field is blank if a physical port is not used as the Secondary System Clock Source.
Primary Clock Ref. Oper. State	The actual primary clock source: Internal, External, Port Reference 1, or Port Reference 2.
Secondary Clock Ref. Oper. State (*If applicable*)	The actual secondary clock source: Internal, External, Port Reference 1, or Port Reference 2.
Primary PLL Oper. State	The current state of the primary synchronization PLL. *Active* – Clock source is in lock and active as a timing reference. *Inactive. In-Lock* – Clock source is not active as a timing reference, but is in lock. *Unusable* – Indicates that at the time the PLL state was sampled, the PLL output could not be used as a system timing reference (e.g., the PLL is configured to use an external reference and that reference is physically disconnected).
Secondary PLL Oper. State (*If applicable*)	The current state of the secondary synchronization PLL.

Table 2-10. Show System-Timing Fields (Continued)

Field	Displays...
External Clock 1 Oper. State	The current state of external clock 1. *Active* – Valid clock source. *AIS* – Detected an AIS condition. *LOS* – Detected loss of signal. *LOF* – Detected loss of frame.
External Clock 2 Oper. State	The current state of external clock 2.
Port Clock Ref. 1 Oper. State	The current state (active, down, or unavailable) of the physical port configured as port reference 1. Note that: • The current state is always down for CBX 500 SPs that do not use a physical port as a clock reference. • The current state is always unavailable for GX 550 NPs that do not use a physical port as a clock reference.
Port Clock Ref. 2 Oper. State	The current state (active, down, or unavailable) of the physical port configured as port reference 2. Note that: • The current state is always down for CBX 500 SPs that do not use a physical port as a clock reference. • The current state is always unavailable for GX 550 NPs that do not use a physical port as a clock reference.
Actual External Clock Interface Type	The actual external clock interface type. T1 wire-wrap (the default) specifies a North American SPA or NPA. This option accepts T1 timing inputs and outputs. E1 BNC specifies an international SPA or NPA for E1 inputs and outputs.

Viewing B-STDX 8000/9000 and CBX 500 IOM Status

To view IOM information:

1. Select the switch object on the network map.
2. From the monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 2-6 on page 2-10 or Figure 2-5 on page 2-9).
3. Double-click on an IOM slot. The View Card Attributes dialog box appears. The fields vary depending on the type of switch and card. Figure 2-15 shows the attributes for a 4-port ATM OC-3c/STM-1 module in a CBX 500 switch.

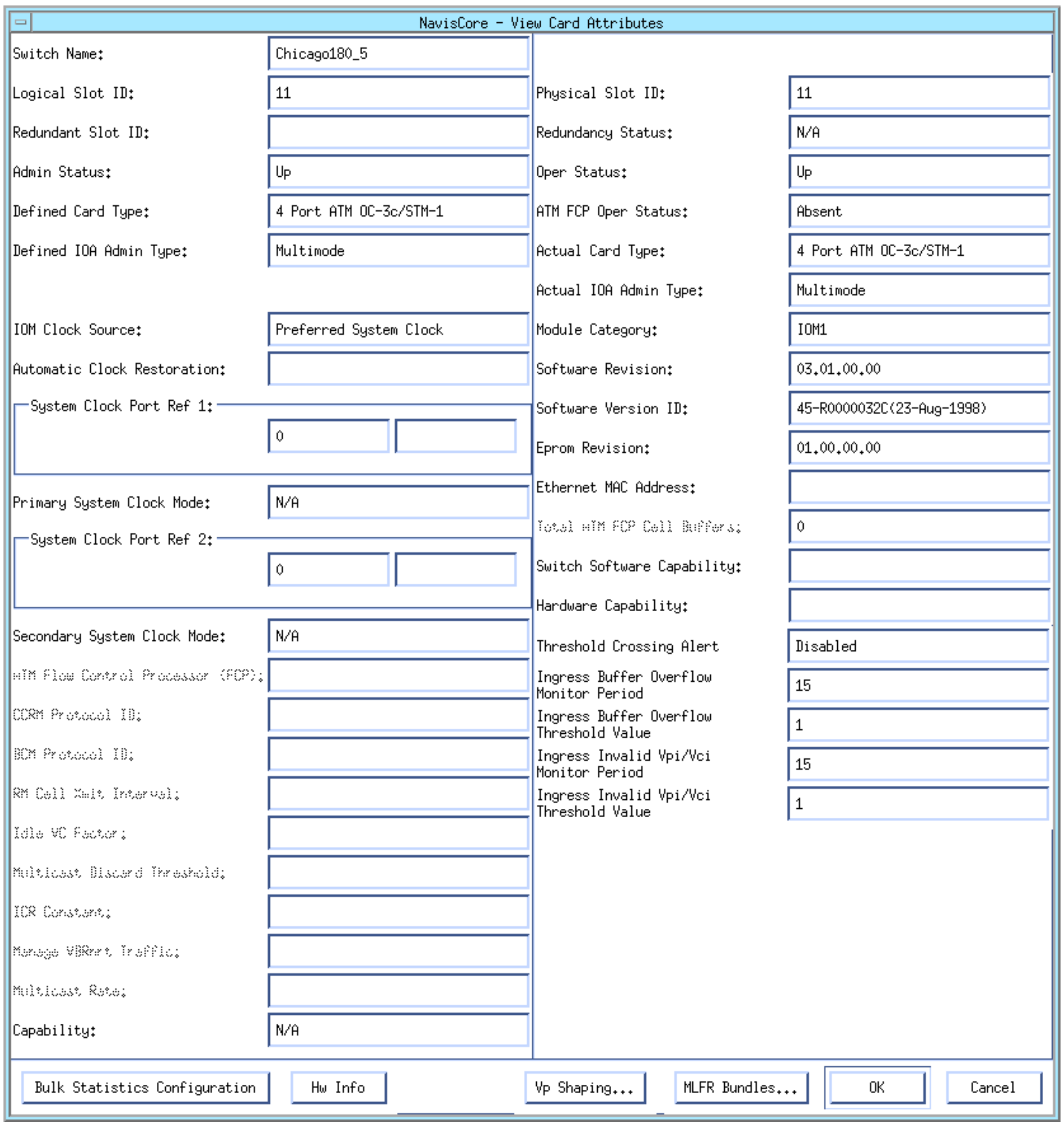


Figure 2-15. View Card Attributes Dialog Box (CBX 500 IOM)

Table 2-11 describes the buttons that appear on this dialog box.

Table 2-12 describes the attributes fields for a BTDX 8000/9000 IOM. Table 2-13 describes the attributes fields for a CBX 500 IOM. See the *NavisCore Physical Interface Configuration Guide* for more information on these fields.

Table 2-11. View Card Attributes Dialog Box Buttons (IOMs)

Button	Function
Bulk Statistics Configuration	Displays the bulk statistics configuration of the IOM. See the *NavisXtend Bulk Statistics Collector User's Guide* for details.
Hw Info	Displays manufacturing information about the IOM. See "Viewing Manufacturing Information" on page 2-39 for details.
VP Shaping (*CBX 500 only*)	Displays VP shaping thresholds for ATM IOMs on CBX 500 switches. See "Monitoring VP Shaping" on page 2-57 for details.
MLFR Bundles	Displays Multilink Frame Relay trunk bundles associated with the IOM. See "Monitoring Multilink Frame Relay" on page 9-19 for details.

Table 2-12. View Card Attributes Fields (B-STDX IOM)

Field	Displays...
Switch Name	The name of the switch in which this IOM resides.
Logical Slot ID	The number of the slot for which this IOM is configured.
Redundant Slot ID	The redundant module's slot number (if applicable).
Admin Status	One of the following: *Up (default)* – The IOM becomes fully operational at switch start-up. To become operational, the module gets its application code from the PCMCIA hard drive, which resides in the CP module. *Down* – The IOM does not come on-line at switch start up. The configuration is saved in the switch configuration table but is not downloaded to the switch. Use this option when running foreground diagnostics. See "Foreground Diagnostics" on page 5-9 for more information. *Maintenance* – The IOM does not receive the application code at switch start-up. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem.
Defined Card Type	The configured IOM type.
Defined IOA Admin Type	The type of interface defined for this slot, if applicable.

Table 2-12. View Card Attributes Fields (B-STDX IOM) (Continued)

Field	Displays...
Capability	The IOM's service capability. Possible values are as follows: *Frame Relay* – The module supports Frame Relay networking services only. *Multi-Service(16)* – 16 MB module that supports multiple networking services. *Multiple Service* – 8 MB module that supports multiple networking services.
External Clock (*12-port E1 IOM only*)	This field displays the transmit clock source for the timing section of the IOM.
ISDN PRI Switch Type (*ISDN IOMs only*)	This field displays the ISDN central office switch type for the card.
Number of D-Channels on Card (*ISDN IOMs only*)	This field displays the number of ISDN D-Channels that the card currently supports.
Channel Identification (*ISDN IOMs only*)	This field displays whether channel ID assignment is performed by the Ascend switch (Preferred) or by the central office switch (Exclusive).
Physical Slot ID	The number of the slot in which the IOM resides.
Redundancy Status	The redundancy status, Stand Alone, Redundant, or N/A.
Oper Status	The operational status of this IOM (for example, "Up").
Actual Card Type	The actual IOM type as defined by the firmware.
Actual IOA Admin Type	The type of IOA attached to the IOM.
Module Category	The category of the IOM (for example, IOPA, ATM-T3).
Software Revision	The switch software revision number.
Software Version ID	The build number and date of the switch software.
Eprom Revision	The EPROM firmware revision number.
Ethernet MAC Address	Does not apply.

Table 2-13. View Card Attributes Fields (CBX 500 IOM)

Field	Displays...
Switch Name	The name of the switch in which this IOM resides.
Logical Slot ID	The ID of the slot in which this IOM is configured.
Redundant Slot ID	Not supported.
Admin Status	One of the following values: *Up (default)* – The IOM becomes fully operational at switch start-up. To become operational, the module gets its application code from the PCMCIA hard drive, which resides in the SPA module. *Down* – The IOM does not come on-line at switch start up. The configuration is saved in the switch configuration table but is not downloaded to the switch. Set the IOM to Down when you run foreground diagnostics. See "Foreground Diagnostics" on page 5-9 for more information. *Maintenance* – The IOM does not receive the application code at switch start-up. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem.
Defined Card Type	The configured IOM type.
Defined IOA Admin Type	The type of interface (for example, Singlemode) defined for this slot, if applicable.
IOM Clock Source	The internal timing source for the IOM. This setting applies only to the IOM's physical ports whose Xmit Clock Source field is set to Internal. It does not effect physical ports whose Xmit Clock Source field is set to Loop-Timed, since the clock for these ports is derived from the non-external clock source coming into the port. Options include: *Preferred System Clock (default)* – Indicates the preferred system clock provides the IOM clock source, which can be either the primary or secondary system clock (whichever of the two is currently up). *Local Clock* – Indicates the local clock on the IOM provides the clock source. *Primary System Clock Only* – Indicates the primary system-clock source provides the IOM clock source. *Secondary System Clock Only* – Indicates the secondary system-clock source provides the IOM clock source.
Automatic Clock Restoration	The revertive state (enabled or disabled) of the system-timing clock reference. If enabled, and the clock reference is switched to the secondary system clock due to a problem with the primary system clock, the clock reference will revert back to the primary clock upon its recovery. Otherwise, the clock reference does not automatically revert back to the primary system clock.

Table 2-13. View Card Attributes Fields (CBX 500 IOM) (Continued)

Field	Displays...
System Clock Port Ref 1	Whether the IOM provides the primary system clock source to the SP module. Options include: *No Physical Port (default)* – Indicates the SP does not get its primary system-clock source from a port on this IOM. *Physical Port* n – Indicates the physical port that provides the primary system-clock source to the SP. The incoming clock signal on the selected port is provided to the SP as the primary system-clock source.
Primary System Clock Mode (*DS3/E3 modules only*)	One of the following values: *PLCP* – Indicates the module uses a Physical Layer Convergence Protocol (PLCP) frame, which transmits 12 ATM cells every 125 μs. *Line Rate* – Indicates the module uses the DS3 line rate as the clock mode. The DS3 line rate is 44.5 Mbps. Line Rate is the only option for E3 modules. *N/A* – Not applicable.
System Clock Port Ref 2	Whether the IOM provides the secondary system-clock source to the SP module. Options include: *No Physical Port (default)* – Indicates the SP does not get its secondary system-clock source from a port on the IOM. *Physical Port* n – Indicates the physical port that provides the secondary system-clock source to the SP. The SP uses the incoming signal on the selected port as the secondary system clock source.
Secondary System Clock Mode (*DS3/E3 modules only*)	One of the following values: *PLCP* – Indicates the module uses a PLCP frame, which transmits 12 ATM cells every 125 μs. *Line Rate* – Indicates the module uses the DS3 line rate as the clock mode. The DS3 line rate is 44.5 Mbps. Line Rate is the only option for E3 modules. *N/A* – Not applicable.
ATM Flow Control Processor (FCP)	Whether ATM FCP capabilities are enabled or disabled. If ATM FCP is enabled, the dialog box displays the available attributes for the ATM FCP (such as CCRM Protocol ID, BCM Protocol ID, etc.).
CCRM Protocol ID	The protocol number in Cascade Communications Resource Management (CCRM) cells. The value of this field must be different from the BCM Protocol ID field. Otherwise, the ATM FCP is misconfigured.
BCM Protocol ID	The protocol ID number in Backward Congestion Message (BCM) cells. The value of this field must be different from the value of the CCRM Protocol ID field. Otherwise, the ATM FCP is misconfigured.
RM Call Xmit Interval	The RM call transmission interval in milliseconds.

Table 2-13. View Card Attributes Fields (CBX 500 IOM) (Continued)

Field	Displays...
Idle VC Factor	The number of idle RM call transmission intervals that can take place before the VC is declared idle. An idle RM call transmission interval is one in which no cells are received.
Multicast Discard Threshold	The discard threshold for multicast circuits.
ICR Constant	The factor that the ATM FCP uses to calculate the initial cell rate (ICR) for a circuit from its minimum cell rate (MCR) and peak cell rate (PCR).
Manage VBRnrt Traffic	"Enabled" if Variable Bit Rate Non-Real Time (VBRnrt) traffic is treated as available bit rate (ABR) traffic. Otherwise, this field displays "Disabled."
Multicast Rate	The current multicast shaping rate as a fraction of the line rate. The multicast rate parameter determines the rate at which the multicast queue is dequeued on the ATM Flow-Control Processor.
Capability	"FCP" if ATM FCP is enabled. Otherwise, the field is blank.
Physical Slot ID	The number of the slot in which this IOM resides.
Redundancy Status	Not supported.
Oper Status	The operational status of this IOM.
ATM FCP Oper Status	The operating status of the ATM FCP: Absent (the ATM FCP is not installed), Up, or Down.
Actual Card Type	The actual IOM type as defined by the firmware.
Actual IOA Admin Type	The type of IOA attached to the IOM.
Module Category	The category of the IOM (for example, IOM1).
Software Revision	The switch software revision number.
Software Version ID	The build number and date of the switch software.
Eprom Revision	The EPROM firmware revision number.
Ethernet MAC Address	Does not apply.
Total ATM FCP Cell Buffers	The total number of ATM Flow-Control Processor cell buffers (if applicable).

Table 2-13. View Card Attributes Fields (CBX 500 IOM) (Continued)

Field	Displays...
Switch Software Capability	The IOM's configured Automatic Protection Switching (APS) capability or VP shaping capability. This field displays "APS" if the APS capability is enabled. This field displays "VP Shaping" if VP shaping is enabled. If this field is not blank, compare the value of this field to the value of the Hardware Capability field, which indicates the IOM's actual APS or VP shaping capability based on its hardware. If the values of these two fields do not match, a configuration mismatch exists. Reconfigure the IOM so that its APS or VP shaping parameters match the IOM's hardware capabilities.
Hardware Capability	The IOM's actual APS capability or VP shaping capability based on its hardware. This field displays "APS" if the APS capability is enabled. This field displays "VP Shaping" if the VP shaping capability is enabled.
Threshold Crossing Alert	Whether ATM Threshold Crossing Alert (TCA) is enabled or disabled for the IOM.
Ingress Buffer Overflow Monitor Period	The ATM TCA ingress buffer overflow alert period (in minutes).
Ingress Buffer Overflow Threshold Value	The ATM TCA ingress buffer overflow threshold.
Ingress Invalid Vpi/Vci Monitor Period	The ATM TCA ingress invalid VPI/VCI alert period (in minutes).
Ingress Invalid Vpi/Vci Threshold Value	The ATM TCA ingress invalid VPI/VCI threshold.

Viewing BIO Module Status

To view information about a GX 550 BIO module:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (Figure 2-7 on page 2-11).
3. Double-click on the BIO module. Note that you may double-click on either the entire module or any of the subcards. The View Card Attributes dialog box appears (see Figure 2-16).

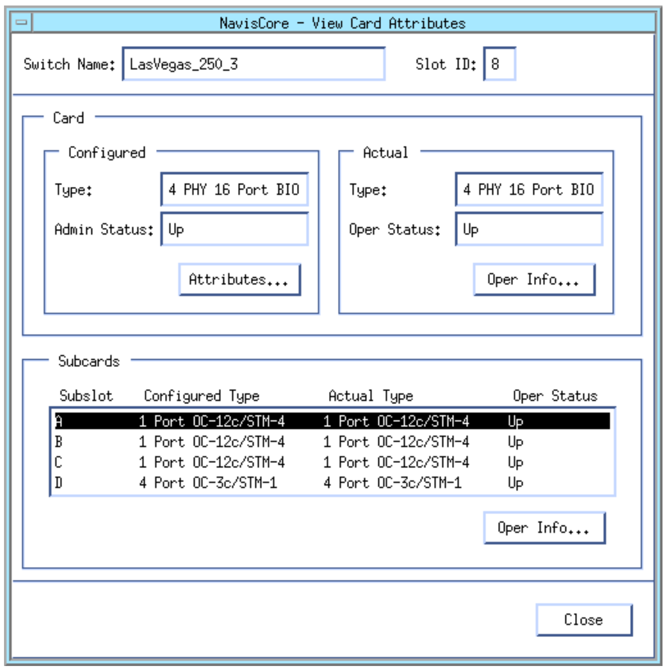


Figure 2-16. View Card Attributes Dialog Box (BIO Module)

Table 2-14 describes the buttons on the View Card Attributes dialog box.

Table 2-14. View Card Attributes Dialog Box Buttons (BIO Module)

Button	Function
Attributes	Displays additional BIO module attribute information. See "Displaying Additional Attributes for a BIO Module" on page 2-38 for more information.
Oper Info (Actual)	Displays manufacturing information about the BIO module. See "Viewing Manufacturing Information for a BIO Module and a BIO Subcard" on page 2-42 for more information.
Oper Info (Subcards)	Displays manufacturing information about a selected subcard on a BIO module. See "Viewing Manufacturing Information for a BIO Module and a BIO Subcard" on page 2-42 for more information.

Table 2-15 describes the BIO module attribute fields.

Table 2-15. View Card Attributes Fields (BIO Module)

Field	Displays...
Switch Name	The name of the switch in which this BIO module resides.
Slot ID	The number of the slot in which this BIO module is installed.
Configured	
Type	The configured card type for this BIO module.
Admin Status	One of the following: *Up (default)* – The BIO module becomes fully operational at switch start-up. To become operational, the module gets its application code from the PCMCIA hard drive, which resides in the NPA module. *Down* – The BIO module does not come online at switch start up. The configuration is saved in the switch configuration table but is not downloaded to the switch. Use this option when running foreground diagnostics. See “Foreground Diagnostics” on page 5-9 for more information. *Maintenance* – The BIO module does not receive the application code at switch start-up. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem.
Actual	
Type	The actual card type as defined by the firmware.
Oper Status	The operational status of the BIO module.
Subcards	
Subslot	The subslot in which the subcard is installed: A, B, C, or D.
Configured Type	The configured types for the subcards in the BIO module: (for example, 4-port OC-3c/STM-1). If no subcard is installed in the subslot, this field displays “Empty.”
Actual Type	The actual type of the subcard as defined by the firmware.
Oper Status	The operational status of each subcard.

Displaying Additional Attributes for a BIO Module

To display additional BIO module attributes, choose Attributes from the View Card Attributes dialog box (see Figure 2-16). The View Additional Card Attributes dialog box appears, as shown in Figure 2-17.

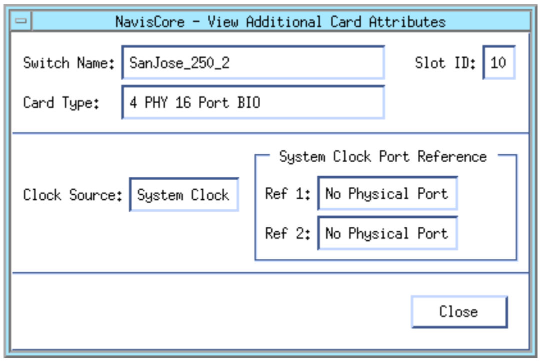


Figure 2-17. View Additional Card Attributes Dialog Box

Table 2-16 describes the additional BIO module attributes fields.

Table 2-16. View Additional Card Attributes Fields (BIO Module)

Field	Displays...
Switch Name	The name of the switch in which this BIO module resides.
Card Type	The configured BIO module type.
Slot ID	The number of the slot in which this BIO module is installed.
Clock Source	The module's internal or external clock source. If the module uses a physical port as its clock source, physical port information appears in the System Clock Port Reference fields.
System Clock Port Reference	
Ref 1	The physical port configured on the BIO module as the primary system clock source. The module uses an incoming clock signal on a selected physical port as the primary (or secondary) clock source. "No Physical Port" appears if a physical port is not configured as the primary system clock source.
Ref 2	The physical port configured on the BIO module as the secondary system clock source. The module uses an incoming clock signal on a selected physical port as the primary (or secondary) clock source. "No Physical Port" appears if a physical port is not configured as the secondary system clock source.

Viewing Manufacturing Information

You can view manufacturing information about processor modules, IOMs, and BIO modules in Ascend switches. The way in which you view this information depends on the type of switch you are monitoring.

Viewing B-STDX 8000/9000 and CBX 500 Manufacturing Information

To view manufacturing information for CP, SP, and I/O modules:

1. Select the appropriate switch object on the network map.

2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.

3. Double-click on the CP, SP, or IOM slot.

If you select an IOM, the View Card Attributes dialog box appears.

If you select a CP or SP, the Select Card dialog box appears. Select Active or Standby and choose OK. The View Card Attributes dialog box appears.

4. Choose HW Info. The View Hardware Attributes dialog box appears (see Figure 2-18).

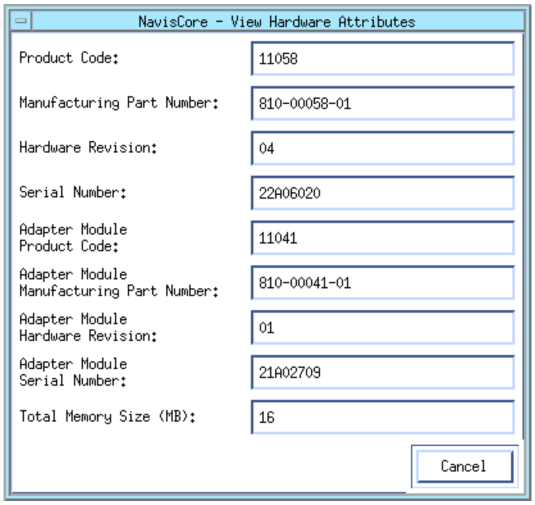


Figure 2-18. View Hardware Attributes Dialog Box

Table 2-17 describes the fields on the View Hardware Attributes dialog box.

Table 2-17. View Hardware Attributes Fields

Field	Displays...
Product Code	The product code for the CP, SP, or IOM.
Manufacturing Part Number	The manufacturing part number of the CP, SP, or IOM.
Hardware Revision	The hardware revision number of the CP, SP, or IOM.
Serial Number	The serial number of the CP, SP, or IOM.
Adapter Module Product Code	The product code for the attached adapter module.
Adapter Module Manufacturing Part Number	The manufacturing part number of the attached adapter module.
Adapter Module Hardware Revision	The hardware revision number of the attached adapter module.
Adapter Module Serial Number	The serial number of the attached adapter module.
Total Memory Size (MB)	The total amount of memory in the CP, SP, or IOM.

Viewing GX 550 Manufacturing Information

You can view manufacturing information for an NP, BIO module, or BIO module subcard.

Viewing Manufacturing Information for an NP

To view manufacturing information for an NP:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Double-click on the NP card. The View Card Attributes dialog box appears.
4. Choose Oper Info. The View Card Operational Info dialog box appears, as shown in Figure 2-19.

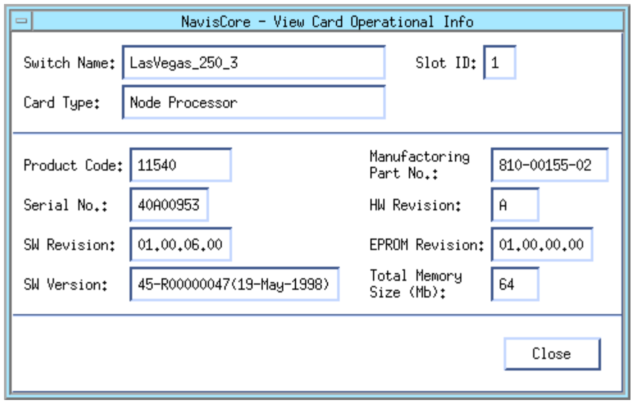


Figure 2-19. View Card Operational Info Dialog Box (NP)

Table 2-18 describes the fields on the View Card Operational Info dialog box.

Table 2-18. View Card Operational Info Fields (NP)

Field	Displays...
Switch Name	The name of the switch.
Card Type	The NP type.
Slot ID	The number of the slot in which the NP is installed.
Product Code	The NP product code.
Serial No.	The NP serial number.
SW Revision	The switch software revision number.
SW Version	The build number and date of the switch software.
Manufacturing Part No.	The NP part number.
HW Revision	The hardware revision number.
Eprom Revision	The EPROM firmware revision number.
Total Memory Size (MB)	The amount of memory, in megabytes, in the NP.

Viewing Manufacturing Information for a BIO Module and a BIO Subcard

To view manufacturing information for a BIO module or BIO module subcard:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Double-click on the BIO module. Keep in mind that clicking on a specific subcard selects the entire BIO module. The View Card Attributes dialog box for the BIO module appears (see Figure 2-20).
4. Follow the call-out instructions in Figure 2-20.

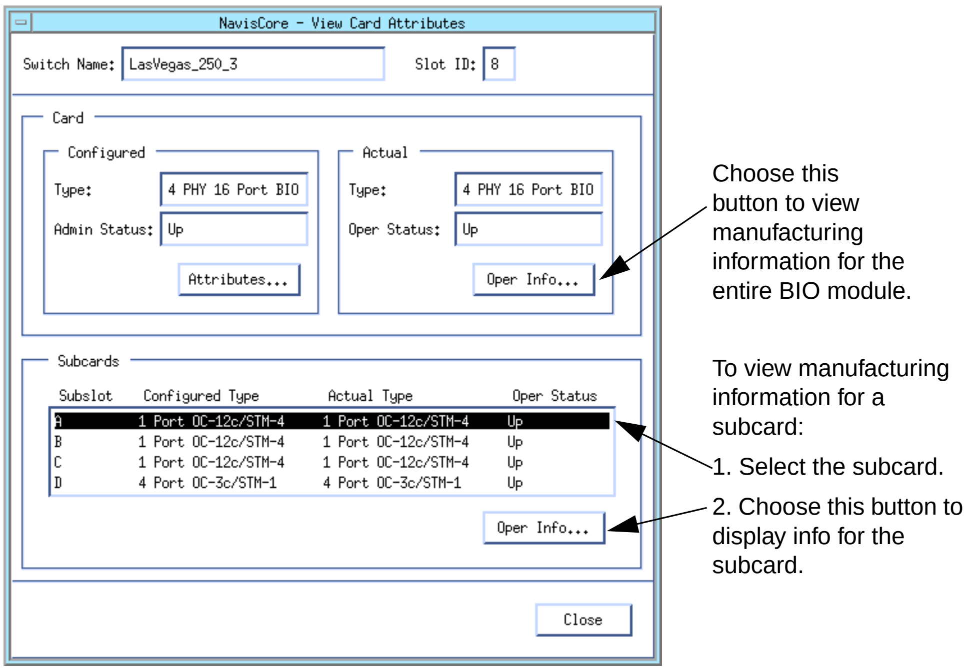


Figure 2-20. View Card Attributes Dialog Box (BIO Module)

The View Card/Subcard Operational Info dialog boxes appear. These dialog boxes are similar to the View Card Operational Info dialog box for the NP, shown in Figure 2-19 on page 2-41.

Table 2-19 describes the fields on the View Card/Subcard Operational Info dialog boxes.

Table 2-19. View Card/Subcard Operational Info Dialog Box Fields

Field	Displays...
Switch Name	The name of the switch.
Card Type	The type of BIO module.
Subcard Type (subcard only)	The BIO subcard type.
Slot ID	The number of the slot in which the BIO module is installed.
Subslot (subcard only)	The number of the subslot on the BIO module in which the subcard is installed.
Product Code	The product code.
Serial No.	The serial number.
SW Revision	The switch software revision number.
SW Version (BIO module only)	The build number and date of the switch software.
Manufacturing Part No.	The part number.
HW Revision	The hardware revision number.
Eprom Revision	The EPROM firmware revision number.
Total Memory Size (MB) (BIO module only)	The amount of memory, in megabytes, in the BIO module.

Reviewing Standby STDX 3000/6000 Status

The Show Standby Switch function displays the status of an STDX 3000/6000’s redundant partner, including the power supply and fan status. This function does not apply to B-STDX 8000/9000s which have redundant IOMs rather than a redundant switch partner.

To display the status of a standby switch:

1. On the network map, select the switch that contains the redundant partner.
2. From the Monitor menu, select Ascend Objects ⇒ Show Standby Switch. The Show Standby Switch dialog box appears.
3. When you finish reviewing the status information, choose Close to exit the dialog box and return to the network map.

Reviewing Physical Port Status

The View (or Show) Physical Port Attributes function displays the specifics of all physical ports defined for a selected switch.

To display a physical port for a selected switch:

1. On the network map, double-click the appropriate switch object. The system displays the Switch Back Panel dialog box.

2. Double-click the physical port that you want to monitor.

The system displays the attributes of the selected physical port. Attributes and buttons vary depending on the type of physical port that you are monitoring. Figure 2-21 shows an example of an ATM OC-3 module Physical Port Attributes dialog box.

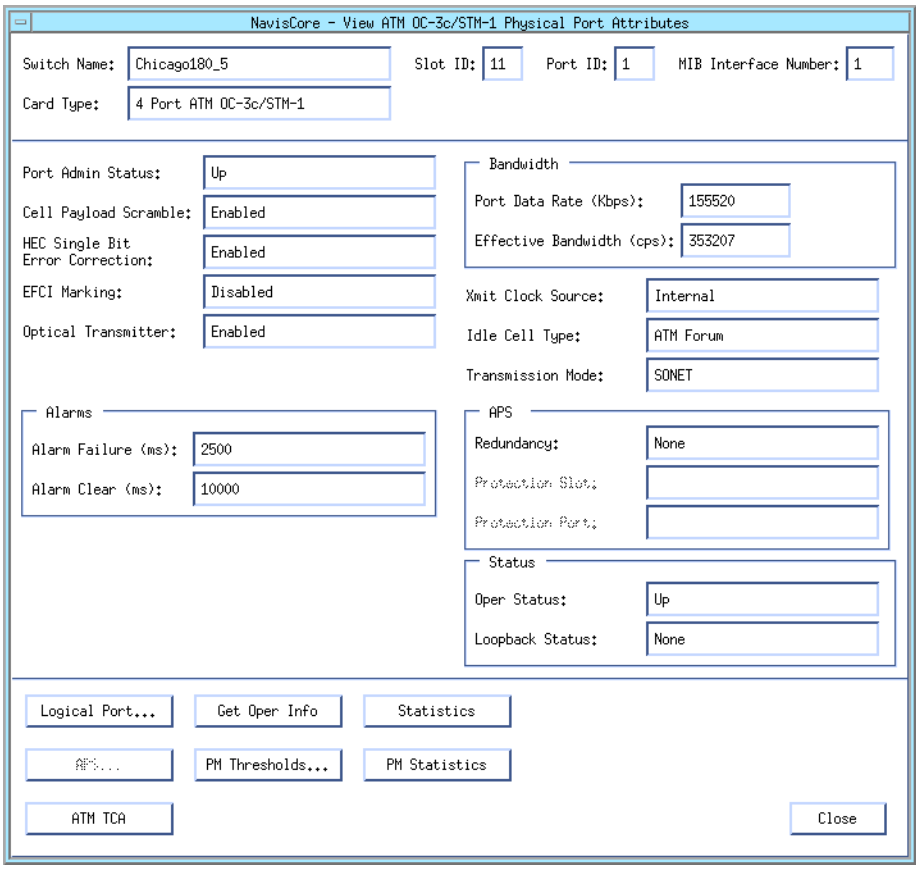


Figure 2-21. View Physical Port Attributes Dialog Box (OC3c/STM-1)

Table 2-20 describes the buttons on the various View Physical Port Attributes dialog boxes.

Table 2-20. View Physical Port Attributes Dialog Box Buttons

Button	Function
Logical Port	Displays the Show All Logical Ports in PPort dialog box.
Get Oper Info	Displays a status message in the Oper Status field that provides a brief status for the selected port. These status messages are described in the *NavisCore Physical Interface Configuration Guide*.
Statistics	Displays the summary statistics for the selected physical port. See "Viewing Physical Port Summary Statistics" on page 3-2 for details.
PM Thresholds	Displays configured performance-monitoring attributes. See the *NavisCore Physical Interface Configuration Guide* for details.
PM Statistics	Displays performance-monitoring statistics. See Chapter 4, "Monitoring Physical Port Performance" for details.
FDL (*T1 only*)	Displays facility data link (FDL) control information for Extended Superframe circuits. See "Displaying FDL Information for a T1 Port" on page 2-62 for details.
Chann Attr *(Channelized DS3 and DS3-1-0 Only)*	Displays configuration information for a selected channel. See "Viewing DS1 Channel Attributes" on page 2-52 for details.
Chan Alarm Status *(Channelized DS3 and DS3-1-0 Only)*	Displays alarm status information for a selected channel. See "Viewing DS1 Channel Alarms" on page 3-10 for details.
DS0s *(Channelized DS3-1-0 Only)*	Displays a dialog box that shows DS0 allocation. See "Viewing DS0 Channel Allocation" on page 2-56 for details.
ATM TCA *(ATM Only)*	Displays ATM Threshold Crossing Alert (TCA) monitoring information. See "Viewing ATM TCA Parameters" on page 2-64 for details.
APS (*OC-n/STM-n*)	Displays Automatic Protection Switching (APS) information. See "Viewing Physical Port Redundancy" on page 2-66 for details.
Close	Exits the dialog box and returns to the network map.

Table 2-21 briefly describes the fields on the View Physical Port Attributes dialog box. The fields vary depending on the type of physical port you are viewing.

Table 2-21. View (or Show) Physical Port Attributes Fields

Field	Displays...
Switch Name	The name of the switch.
Slot ID	The number of the slot that contains the selected IOM and port.
Port ID	The port number of the selected physical port.
Card Type	The type of IOM for the selected port.
MIB Interface Number	The MIB interface number for the physical port. The software assigns a unique number to each physical port on the switch.
Port Admin Status	“Up” or “Down” to indicate the port admin status.
Oper Status	A status message that describes the operational status of the physical port (e.g., Up or Down). Status messages are described in the *NavisCore Physical Interface Configuration Guide*. If this field is blank, the IOM did not respond to a status request (such as a request initiated by the Get Oper Info button).
Bandwidth (Kbps) (Effective Bandwidth)	The amount of available bandwidth (in Kbps) for this physical port.
Port Data Rate	An estimate of the port’s actual data rate in bits per second. If this field displays 0, it means there is no estimate for the port.
Application Mode *(Channelized DS3 and DS3-1-0 only)*	The DS3 signal application mode. The application mode is either M13 or C-bit parity. M13 application mode uses C-bits in a frame to indicate the presence or absence of stuffing bits. C-bit parity application mode uses the first C-bit in M-subframe 1 to identify the format as C-bit parity.
Transmit (Xmit) Clock Source	The transmit clock source. Options include: *Internal* (*default*) – The IOM’s internal timing source provides the clock source to this port. *Loop-Timed* – The clock source is derived from the signal coming into this port. *External* – An external connection provides the clock source. *Chassis* – The chassis provides the clock source.
External Clock Backup (*T1/E1 Only*)	Whether an internal or loop-timed transmit clock source is enabled if an external clock source fails.

Table 2-21. View (or Show) Physical Port Attributes Fields (Continued)

Field	Displays...
Clock Source Selection	The clock source. The switch can either supply or receive clock at a rate of up to 44.212 Mbps for the B-STDX 8000/9000. Options include: *DCE* – Configures the port to provide clock at the rate specified by the clock speed selection. Use this option when connecting to a DTE, where the switch provides both the transmit and receive clocks and uses a straight-through cable. Use a crossover cable to connect to a physical DCE. *DTE* – Configures the port to receive clock from an outside source, typically a CSU/DSU. However, you should set the clock speed even though it is not clocking. You need clock speed for logical port configuration. ***Note**: B-STDX 8000/9000 ports are always electrically DCE and require a crossover cable when interfacing with a modem or other DCE. See the* B-STDX 8000/9000 Hardware Installation Guide *for cable diagram pinouts.*
Clock Speed (Kbps)	The clock speed. If the clock source is set to DTE, the switch ignores the clock speed parameter for clocking purposes. However, you should set clock speed for the actual clock rate, since the cumulative total of all logical ports configured on the physical port cannot exceed the clock source setting. ***Note**: The total bandwidth of all physical ports on the HSSI module cannot exceed the maximum module capacity of 44.212 Mbps. If you exceed the maximum capacity, NavisCore displays an error message.*
Zero Encoding (Line Code) *(T1/E1 only)*	An encoding format for the T1/E1 interface. Zero encoding specifies the format of the data signal encoding. The signal has three different levels – positive, negative, and ground, which must be referenced from a master clock. ***Note**: Consult your facility service provider for more information about selecting a zero encoding method.* T1 options include: *B8ZS* (*default*) – (Bipolar with 8 zero substitution*)* Refers to the use of a specified pattern of normal bits and bipolar violation that is used to replace a sequence of eight zero bits. With B8ZS, a special code is added and then removed from the pulse stream in substitution for a 0 byte that has been transmitted by the user equipment. *Jammed Bit* – Refers to jammed bit zero encoding. Jammed Bit is also known as alternate mark inversion (AMI). Using this method, at least one pulse every eight bits is literally implemented by forcing a pulse in bit 8 of each channel. E1 option is set at high density bipolar of order 3 (HDB3).

Table 2-21. View (or Show) Physical Port Attributes Fields (Continued)

Field	Displays...
Link Framing (Circuit Type) *(T1/E1 only)*	The framing format. Framing configures the T1/E1 interface for a particular framing specification, enabling you to distinguish between the individual channels. It is accomplished by adding one additional bit to each frame. T1 link framing options include: *ESF (CCITT) (default)* – Extended Superframe. Extends the D4 framing format from 12 frames to 24 frames and uses modified framing bits to provide a cyclic redundancy check (CRC), secondary channel, and data link. The advantage of ESF framing over D4 framing is that it enables the Ascend equipment to monitor and respond to a maintenance message from the network. Facility Data Link (FDL) for CCITT is the European standard. *D4 Framing* – Consists of 12 frames (also called Superframe). It provides end-to-end synchronization and signaling associated with a particular channel. *ESF (AT&T)* – AT&T is the US Standard for Extended Superframe. *ESF (None)* – No Facility Data Link (FDL) messaging support. ***Note**: The customer premise equipment (CPE) must use the same framing specification as the Ascend physical port.* For E1 link framing options, you can have a setting of unstructured (no framing – entire bandwidth is available for data), or you can enable time slot 16 (TS16) and/or cyclic redundancy check 4 (CRC4). When you enable TS16, you can use channel 16 to send data. When you enable CRC4, a CRC is performed.
Transmission Mode (*OC-n/STM-n*)	The configured individual ports on this IOM as SONET (OC-*n*) or SDH (STM-*n*).
Max Buffer Size *(Not Supported on All Modules)*	The maximum number of bytes in the reassembly buffer. By selecting a smaller size, you provide more buffers to reassemble packets and reception is improved. However, the maximum buffer size must be large enough to hold the largest packet of information. Packets are discarded if the reassembly buffer is full.
Optical Transmitter	A safety feature intended to prevent personal injury during module repair, replacement, or cable connection. By default, this option is set to Off. The Off setting disables the transmit laser LED for this port and prevents the port from transmitting incoming traffic. You must set this option to On to transmit incoming traffic out of this port. **CAUTION:** THIS FIELD MUST BE SET TO **OFF** BEFORE YOU REMOVE THE OPTICAL CABLE. IF THE OPTICAL CONNECTORS ARE EXPOSED, THE TRANSMIT LASER BEAM CAN CAUSE PERSONAL INJURY. ***Note:** When you disable the transmit laser, the CPE or switch at the other end of the connection reports a red port alarm to indicate signal loss.*
Line Build Out (*DS3 modules only*)	0 – 225 feet (the default) for a short cable or 226 – 450 feet for a long cable. This measurement represents the length of the cable that connects the physical port to other network equipment.

Table 2-21. View (or Show) Physical Port Attributes Fields (Continued)

Field	Displays...
Line Length *(T1 and DSX only)*	The connection line length. *For T1 modules*, if “To DSX-1 Connect Point” is the connection type, this value specifies the distance from the T1 module to the network equipment. The default value is 0-133 ft. *For DSX modules,* this value is the distance measurement from the DSX-1 module to the network equipment. The default is 0-110.
Connection Type *(T1 only)*	The type of connection from the T1 module to the T1 network: *To DSX-1 Connect Point (default)* – The T1 module is connected to a T1 network, for example, a DACS. *To Network* – The T1 module is used as the T1 network interface.
Cell Payload Scramble *(ATM only)*	Enabled (the default) or disabled to indicate the Cell Payload Scramble function. The Cell Payload Scramble function prevents user data from being misinterpreted (that is, it prevents ATM cell header alienation).
Peak Cell Rates *(ATM only)*	The peak cell rate (PCR), which is the maximum transmission rate at which cells are transmitted. It defines the shortest time period between cells. You can configure up to eight PCR Queues, with the first four queues being the high priority queues and the remaining queues being the lower priority queues. The high priority queues are served first, and any remaining bandwidth is used to serve the lower priority queues. For more information about how to configure the peak cell rate, see the *NavisCore Physical Interface Configuration Guide*.
C-Bit Parity (*DS3 modules only*)	Whether the C-Bit Parity function is enabled (default) or disabled. Displays enabled (the default) or disabled to indicate the C-Bit Parity function. The C-Bit Parity function provides a way to monitor the end-to-end performance of T3 circuits. ***Note:*** *This feature requires C-bit parity-compatible customer premise equipment.*
PLCP Options (*ATM DS3/E3 only*)	Whether the Physical Layer Convergence Protocol (PLCP) option is enabled or disabled. When enabled, the physical port uses a PLCP frame, which transmits 12 ATM cells every 125 µs. Note that when PLCP is enabled, available bandwidth is reduced. When PLCP is disabled, the port operates in a direct mapping header error correction (HEC) mode.
EFCI Marking	Whether Explicit Forward Congestion Indicator (EFCI) is enabled or disabled (default). EFCI determines if congestion (or impending congestion) exists in a node. When EFCI is enabled, the congested node modifies the EFCI bit in the ATM cell header to indicate congestion. If the equipment connected to the switch can use the EFCI bit to adjust its transmission rate, it may lower the connection cell rate to relieve the congestion. EFCI is only set in the UBR queue and affects all connections in this physical port queue.
HEC Single Bit Error Correction	Whether configured single bit header error correction (HEC) is enabled (the default) or disabled on a per port basis.

Table 2-21. View (or Show) Physical Port Attributes Fields (Continued)

Field	Displays...
FEAC Loopback (*DS3 modules only*)	Whether the switch can respond to loopback commands on the Far-End Alarm and Control (FEAC) channel. When FEAC loopback is enabled (the default), the switch can respond to FEAC loopback commands from far-end equipment (loop-up and loop-down). These commands can put the port into remote loopback. When FEAC loopback is disabled, the switch ignores loop-up and loop-down commands on the FEAC channel.
Received FEAC Status (*DS3 modules only*)	A value in this field if the C-Bit Parity option is selected and a loopback test has been sent from a remote source. This function enables you to monitor the performance of T3 circuits.
Idle Cell Type	The idle cell type setting (ATM Forum or UNI), which determines the type of idle cell that the port transmits.
Alarm Failure (ms) *(Not supported on some modules)*	A value from 0 to 65535 ms that specifies how long the switch waits before declaring a physical layer problem (i.e., loss of signal) a real failure. The default value of 2500 ms (2.5 seconds) means the switch “soaks” the physical layer alarm for 2.5 seconds before declaring the physical port down. A value of 0 ms means the physical port goes down immediately following any physical layer failure.
Alarm Clear (ms) *(Not supported on some modules)*	A value from 0 to 65535 ms that specifies how long the switch waits once a failure is cleared before declaring a physical layer problem (i.e., loss of signal) resolved. The default value of 10000 ms (10 seconds) means the switch waits 10 seconds after the alarm clears before declaring the physical port up. A value of 0 ms means the physical port comes back up as soon as the physical layer failure alarm clears.
APS Redundancy *(SONET only)*	None if there is no APS redundancy; displays Intracard APS 1+1 if the redundant ports are on the same IOM; displays Intercard APS 1+1 if the redundant ports are on different IOMs. See “Viewing Physical Port Redundancy” on page 2-66 for more information on APS.
APS Protection Slot *(SONET only)*	The slot ID of the IOM that contains the redundant physical port. See “Viewing Physical Port Redundancy” on page 2-66 for more information on APS.
APS Protection Port *(SONET only)*	The port ID of the redundant physical port. See “Viewing Physical Port Redundancy” on page 2-66 for more information on APS.

Table 2-21. View (or Show) Physical Port Attributes Fields (Continued)

Field	Displays...
BIP Error Threshold *(ATM IWU only)*	The Bit Interleaving Parity error threshold, which indicates the physical port's sensitivity to network errors. Options include: • 10^-6 errors • 10^-5 errors • 10^-4 errors • ignore
Far End Loopback *(T1 and DSX-1 only)*	Whether far-end loopback capabilities are enabled or disabled.
Loopback Status	The port loopback status, if you enabled diagnostic loopback tests. The default is None.
In Band Line Loopback *(T1 and E1 only)*	CSU if the switch sends in-band line loopbacks. Otherwise, the switch responds to in-band line loopbacks.
Port Link Down Reason *(Channelized DS3 and DS3-1-0 only)*	The reason why a link is down. If the link is up, this field displays None.
ISDN PRI *(ISDN only)*	The ISDN PRI capability (On or Off).
ISDN Client IP Address *(ISDN only)*	The base IP address used for IP dynamic address assignment.
Application Mode (*Channelized DS3 and DS3-1-0 modules only*)	The DS3 application mode: either M13 or C-bit parity. M13 application mode uses C-bits in a frame to indicate the presence or absence of stuffing bits. C-bit parity application mode uses the first C-bit in M-subframe 1 to identify the format as C-bit parity.
Traffic Shaper Parameters *(ATM IWU/CS only)*	ATM IWU and ATM CS traffic shaper parameters. Each shaper has associated default values for priority, SCR, PCR, and MBS. See "Monitoring VP Shaping" on page 2-57 for more information.
Allocated Channels *(Channelized DS3 and DS3-1-0 Modules only)*	The channels allocated for the physical port.
MAC Address *(Fast Ethernet only)*	The user-configured MAC address, if one is needed. In most cases, the burned-in MAC address in the module's ROM is sufficient. The Oper MAC Address field displays the burned-in MAC address. If the burned-in MAC address is in use, the MAC Address field displays a MAC address of all zeros.

Table 2-21. View (or Show) Physical Port Attributes Fields (Continued)

Field	Displays...
Port Capability *(Fast Ethernet only)*	One of the following options: *100M Full Duplex* – The port supports 100 Mbps full-duplex communication. *100M Half Duplex* – The port supports 100 Mbps half-duplex communication. *10M Full Duplex* – The port supports 10 Mbps full-duplex communication. *10M Half Duplex* – The port supports 10 Mbps half-duplex communication.
Port Connection Type *(Fast Ethernet only)*	The type of Ethernet connector: either RJ-45 Connector or MII Connector.
Oper MAC Address *(Fast Ethernet only)*	The MAC address that is burned into the module's ROM.
Oper Clock Speed *(Fast Ethernet only)*	The physical port's data rate in kilobits per second. (Note that 1000 Kbps equals 1 Mbps.)

Viewing DS1 Channel Attributes

You can view the attributes of DS1 channels on channelized DS3 and channelized DS3-1-0 physical ports. To access these attributes:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Double-click the Channelized DS3 or DS3-1-0 physical port. The Show Physical Port Attributes dialog box appears.
4. Select a channel button ID and choose Chann Attr. The Channel Attributes dialog box appears (see Figure 2-22).

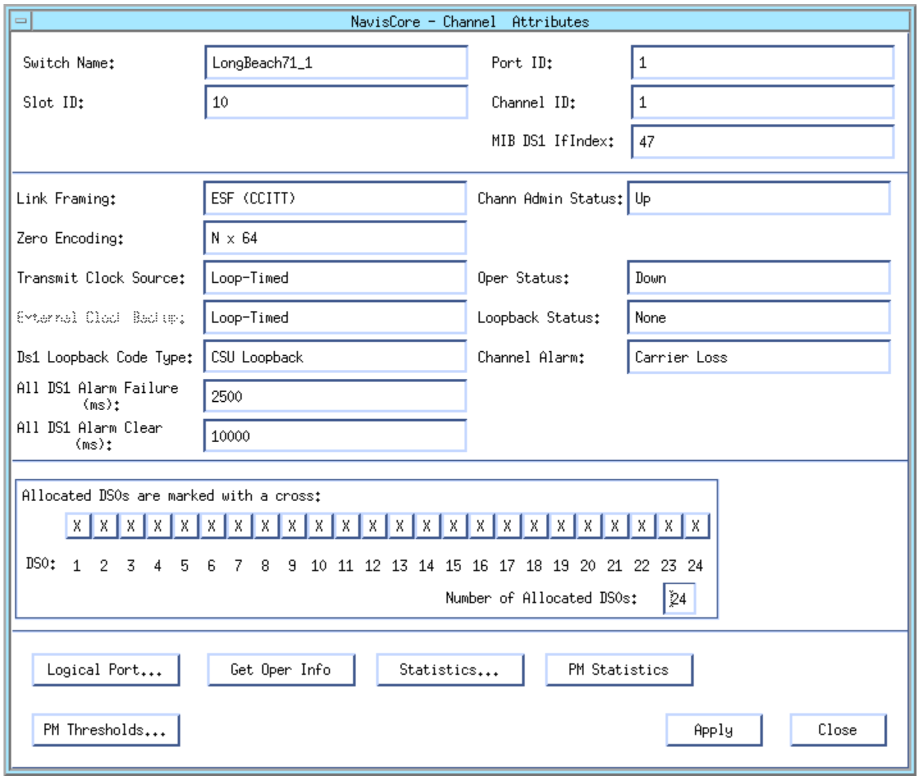


Figure 2-22. Channel Attributes Dialog Box

Table 2-22 describes the Channel Attributes buttons.

Table 2-22. Channel Attributes Buttons

Button	Function
Logical Port	Access the Show All Logical Ports in PPort dialog box.
Get Oper Info	Displays a status message in the Oper Status field that provides a brief status for the selected channel.
Statistics	Displays the summary statistics for the selected channel. See “Viewing DS1 Channel Statistics” on page 3-12 for details.
PM Threshold	Displays configured performance monitoring threshold attributes.
PM Statistics	Access performance monitoring statistics. See “Viewing Performance-Monitoring Data” on page 4-4 for details.
Close	Exit the dialog box and return to the network map.

Table 2-23 describes the Channel Attributes fields.

Table 2-23. Channel Attributes Fields

Field	Displays...
Switch Name	The name of the switch.
Slot ID	The number of the slot.
Port ID	The number of the port.
Channel ID	The number of the channel.
MIB DS1 IfIndex	The interface number used for link performance.
Link Framing	The configured framing format. The T1 interface is configured for a particular framing specification, enabling you to distinguish between individual channels. It is accomplished by adding one additional bit to each frame. Options include: *ESF (CCITT) (default)* – Extended Superframe. Extends the D4 framing format from 12 frames to 24 frames, and uses modified framing bits to provide a cyclic redundancy check (CRC), secondary channel, and data link. The advantage of ESF framing over D4 framing is that it enables Ascend's equipment to monitor and respond to a maintenance message from the network. Facility Data Link (FDL) for CCITT is the European standard. *D4 Framing* – Consists of 12 frames (also called "Superframe"). It provides end-to-end synchronization and signaling associated with a particular channel. ***Note**: The customer premise equipment (CPE) must use the same framing specification as the Ascend physical port.*
Transmit Clock Source	The configured transmit clock source for the DS1. Options include: *Loop Timed (default)* – The clock source is derived from the timing received. *Internal* – The internal timing generator provides the clock source. *External* – An external connection provides the clock source. If you select this option, you should also set an external clock backup.
External Clock Backup	Either loop-timed or internal clock source.
DS1 Loopback Code Type	The loopback code type. Options include: *CSU Loopback* – Specifies that the DS1 loopback loops back the CSU at the CPE. *NI Loopback* – Specifies that the DS1 loopback loops back the Network Interface (NI) at the CPE.

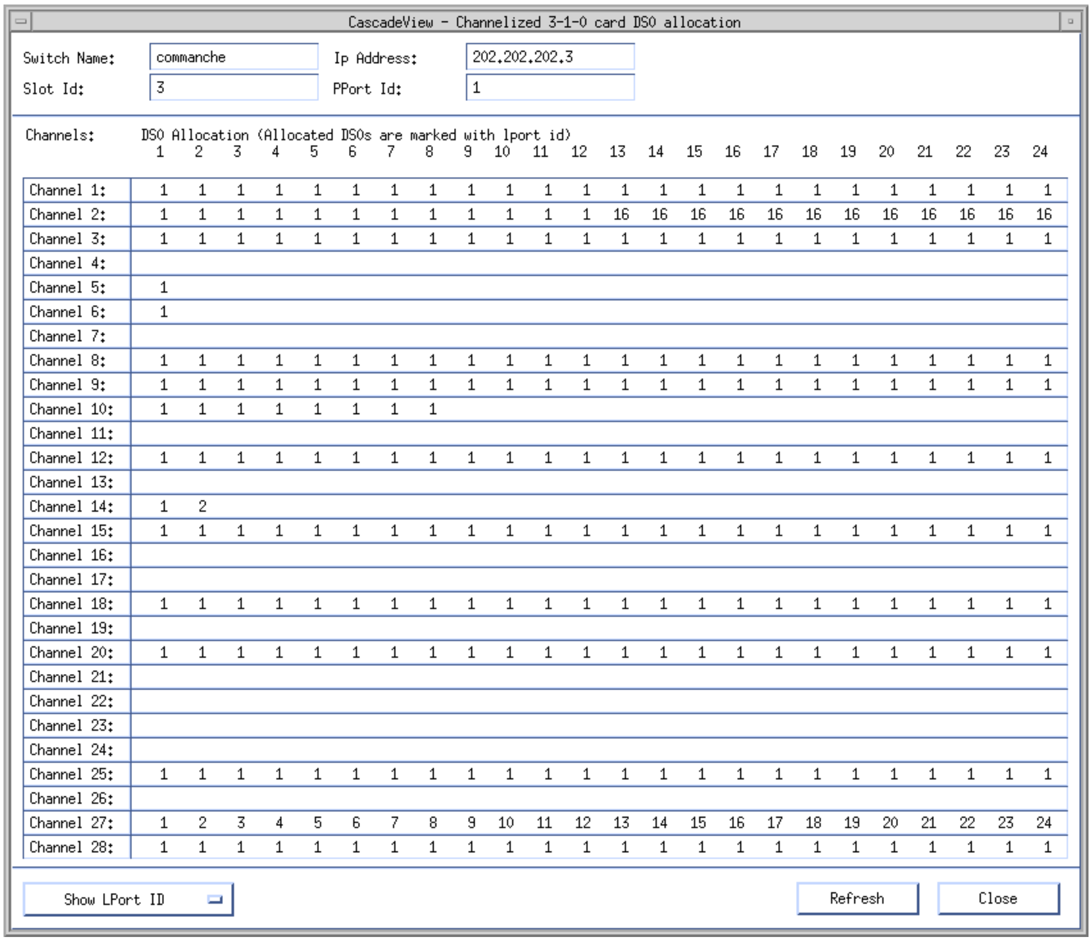
Table 2-23. Channel Attributes Fields (Continued)

Field	Displays...
All DS1 Alarm Failure (ms)	A value from 0 to 65535 ms that specifies how long the switch waits before declaring a DS1 interface problem (i.e., loss of signal) a real failure. The default value of 2500 ms (2.5 seconds) means the switch “soaks” the DS1 interface alarm for 2.5 seconds before declaring the DS1 interface down. A value of 0 ms means the physical port goes down immediately following any physical layer failure. If you set the value lower than the default of 2.5 seconds, the switch takes the DS1 interface down due to any transient failure in the transmission path. For a DS1 interface that provides trunk connectivity, this may cause unnecessary rerouting of circuits.
All DS1 Alarm Clear (ms)	A value from 0 to 65535 ms that specifies how long the switch waits once a failure is cleared before declaring a DS1 interface problem (i.e., loss of signal) resolved. The default value of 10000 ms (10 seconds) means the switch waits 10 seconds after the alarm clears before declaring the DS1 interface up. A value of 0 ms means the DS1 interface comes back up as soon as the DS1 interface failure alarm clears. If you set the value lower than the default of 10 seconds, the switch may declare the DS1 interface up before the transmission path is stabilized.
Chan Admin Status	The Channel Admin Status. Options include: *Up* – Enables immediate access to the channel. *Down* – Saves the configuration in the database without activating the port or takes the port off-line to run diagnostics.
Oper Status	The card’s current operational state.
Loopback Status	The card’s current loopback status.
Channel Alarm	The channel’s alarm status. For more information, see “Viewing DS1 Channel Alarms” on page 3-10.

Viewing DS0 Channel Allocation

You can view DS0 allocation on DS3-1-0 physical ports as follows:

1. On the network map, double-click the switch object. The system displays the Switch Back Panel dialog box.
2. Double-click the physical port on the DS3-1-0 module. The Show Physical Port Attributes dialog box appears.
3. Choose DS0s. The DS0 allocation dialog box appears. The example in Figure 2-23 shows allocated DS0s marked with the logical port ID.



Channels:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Channel 1:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 2:	1	1	1	1	1	1	1	1	1	1	1	1	16	16	16	16	16	16	16	16	16	16	16	16
Channel 3:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 4:																								
Channel 5:	1																							
Channel 6:	1																							
Channel 7:																								
Channel 8:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 9:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 10:	1	1	1	1	1	1	1	1																
Channel 11:																								
Channel 12:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 13:																								
Channel 14:	1	2																						
Channel 15:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 16:																								
Channel 17:																								
Channel 18:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 19:																								
Channel 20:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 21:																								
Channel 22:																								
Channel 23:																								
Channel 24:																								
Channel 25:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Channel 26:																								
Channel 27:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Channel 28:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Figure 2-23. Channelized 3-1-0 card DS0 Allocation

4. Select one of the following options:

   Show LPort ID — Displays allocated DS0s marked with the LPort ID.

   Show Interface Number — Displays allocated DS0s marked with the Interface Number.

5. To refresh the dialog box, choose Refresh.
6. Choose Close to exit.

You can also view DS0 channel allocation by viewing the logical port attributes for a DS1 channel. To view these attributes:

1. On the network map, double-click the switch object. The system displays the Switch Back Panel dialog box.
2. Double-click the physical port on the DS3-1-0 module. The Show Physical Port Attributes dialog box appears.
3. Select a DS1 channel button ID and choose Channel Attr. The Channel Attributes dialog box appears (see Figure 2-22 on page 2-53).
4. Choose Logical Port. The Show All Logical Ports in PPort dialog box appears, displaying the DS0 channels. See "Viewing All Logical Ports in a Physical Port" on page 6-19 for more information on this dialog box.

Monitoring VP Shaping

VP shaping is a technique that ATM modules use to control the transmission rate of cells in an ATM network. Both B-STDX 9000 switches and CBX 500 switches support VP shaping. This section describes how to monitor VP shaping on both platforms.

Monitoring VP Shaping on a B-STDX 9000 Switch

On B-STDX 9000 switches, VP shaping is supported by the ATM IWU module and the ATM CS module. The chip in each module contains 15 user-configurable shapers. Each shaper is responsible for controlling the transmission rate of cells across the circuits assigned to it.

You can configure each shaper to perform the following type of shaping:

VC — Shaping is performed on a circuit-by-circuit basis for each circuit assigned to the shaper.

VP — Shaping is performed on an aggregate (that is, virtual path) basis for all of the circuits assigned to the shaper.

To monitor VP shaping on B-STDX 9000 switches:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (Figure 2-5 on page 2-9).
3. Double-click on a physical port on an ATM IWU module or an ATM CS module. The View Physical Attributes dialog box appears. Figure 2-24 shows the View Physical Port Attributes dialog box for an ATM IWU module. The View Physical Port Attributes dialog box for an ATM CS module is similar in appearance.

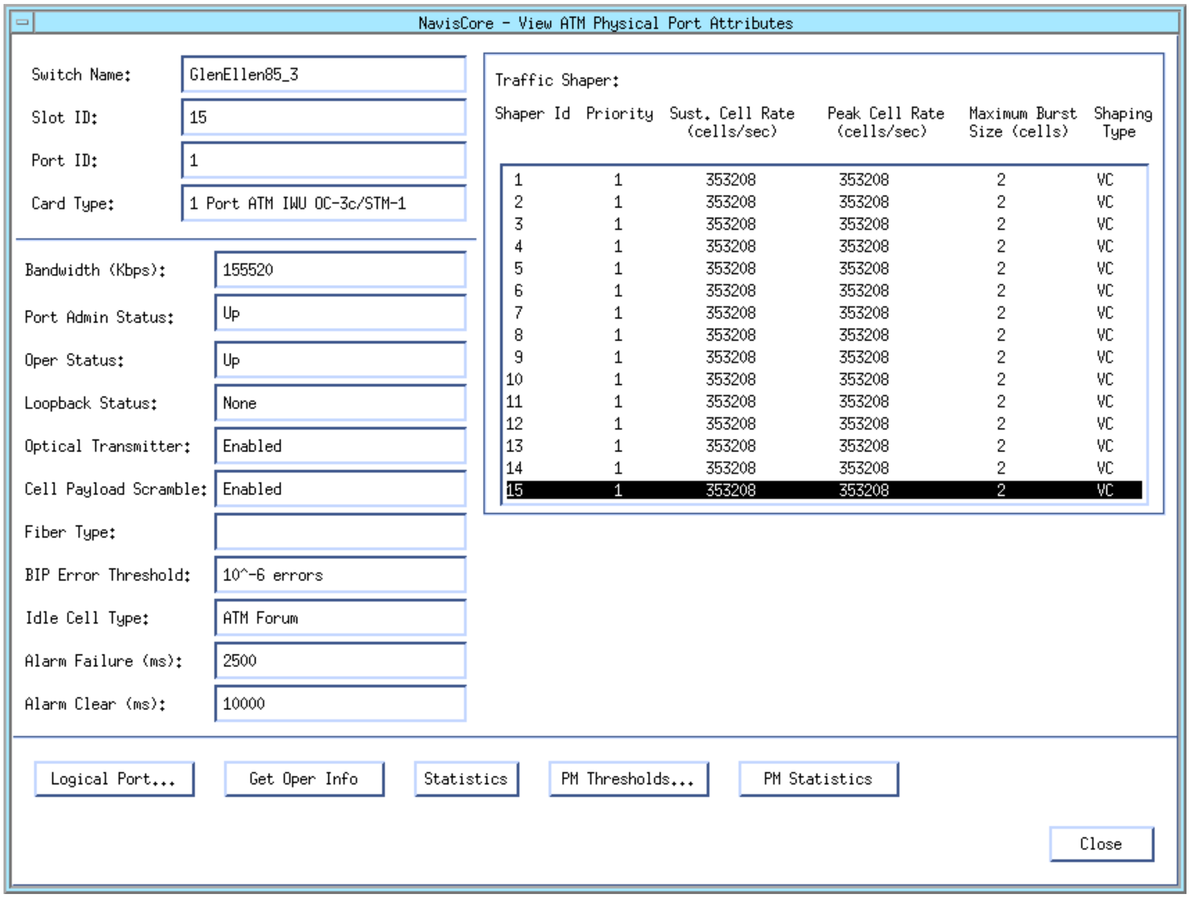


Figure 2-24. View Physical Port Attributes Dialog Box with VP Shaping Parameters

The dialog box displays a set of parameters for each shaper on the ATM IWU module or the ATM CS module. Table 2-24 describes the VP shaping parameters on this dialog box. For descriptions of the other fields on the dialog box, see Table 2-20 on page 2-45.

Table 2-24. VP Shaping Parameters

Parameter	Displays...
Shaper Id	The shaper identifier.
Priority	The priority assigned to the shaper. The switch services a shaper's circuits only if no higher priority shapers are waiting to be served. Priority ranges from 0 (the highest priority) to 15 (the lowest priority).

Table 2-24. VP Shaping Parameters (Continued)

Parameter	Displays...
Sust. Cell Rate (cells/sec)	The sustainable cell rate (SCR). The SCR defines the average rate, in cells per second, at which the shaper transmits cells. The SCR must be less than or equal to the peak cell rate (PCR) for the shaper. If the SCR is less than the PCR, the shaping algorithm will use the maximum burst size (MBS) value as a credit mechanism to allow cells to be transmitted at the PCR.
Peak Cell Rate (cells/sec)	The peak cell rate (PCR). The PCR defines the maximum rate, in cells per second, at which the shaper transmits cells. The PCR must be greater than or equal to the SCR for the shaper. If the PCR is greater than the SCR, then the shaping algorithm will use the maximum burst size (MBS) value as a credit mechanism to allow cells to be transmitted at the PCR.
Maximum Burst Size (cells)	The maximum burst size (MBS) for the shaper, in number of cells. This value determines the maximum number of cells that can be transmitted at the PCR.
Shaping Type	The type of shaping that the shaper implements. Possible values are: *VC* – Shaping is performed on a circuit-by-circuit basis for each circuit assigned to the shaper. *VP* – Shaping is performed on an aggregate (that is, virtual path) basis for all of the circuits assigned to the shaper.

In addition to monitoring VP shaping on the physical port level, you can monitor various types of logical ports associated with ATM IWU IOMs and ATM CS IOMs. VP shaping parameters appear when you monitor the administrative attributes for the following types of logical ports:

- ATM Direct Trunk
- ATM OPTimum Cell Trunk
- ATM OPTimum Frame Trunk
- ATM Network Internetworking for FR NNI

See Table 6-5 on page 6-7 for more information on monitoring logical port administrative attributes.

There are no VP shaping parameters to monitor for ATM UNI DTE/DCE logical ports associated with ATM IWU modules and ATM CS modules. Instead, shapers are assigned to PVCs that use these logical ports. See Table 13-10 on page 13-17 for more information.

Monitoring VP Shaping on a CBX 500 Switch

On a CBX 500 switch, VP shaping is supported by the ATM Flow-Control Processor (ATM FCP) for ATM OPTimum trunks.

> VC shaping applies to the B-STDX 9000 switch only and is not supported on the CBX 500.

Each shaped VP has four transmission queues, one for each QoS class:

- Constant Bit Rate (CBR)
- Variable Bit Rate (VBR) Real Time
- Variable Bit Rate Non-Real Time
- Available/Unspecified Bit Rate (ABR/UBR)

VCCs associated with a shaped VP are mapped to the queues according to their QoS class.

To monitor VP shaping on CBX 500 switches:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (Figure 2-6 on page 2-10).
3. Double-click on the IOM connected to the ATM OPTimum trunk.
4. Choose VP Shaping. The Set VP Shaping Thresholds dialog box appears (see Figure 2-25).

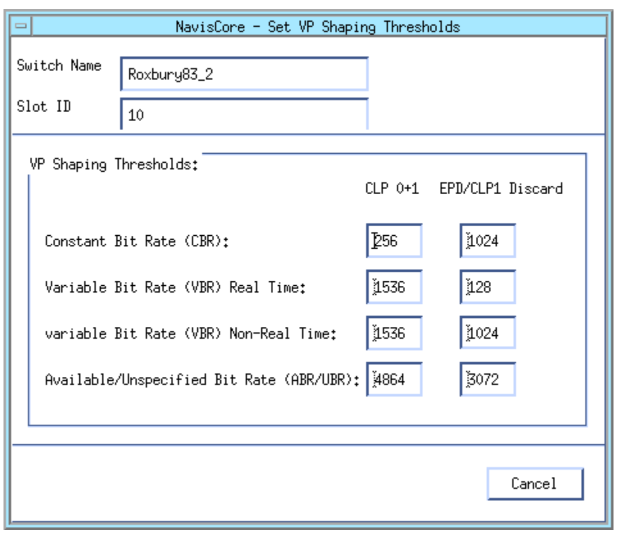


Figure 2-25. Set VP Shaping Thresholds Dialog Box

This dialog box displays the CLP 0+1 (cell loss priority 0+1) and EPD/CLP1 discard (early packet discard/cell loss priority 1 discard) thresholds for each queue in the shaped virtual path (VP).

The CLP 0+1 threshold enables you to reserve buffers before the maximum buffer capacity is reached. The EPD/CLP1 discard threshold is the threshold for both EPD and CLP1 discard.

EPD discard occurs when a cell causes the queue to exceed the threshold. The cells in the current packet are admitted to the queue. However when the end of the current packet is detected, all of the cells in the next packet are discarded.

CLP1 discard occurs when a cell that has the CLP bit set to 1 causes the queue to exceed the threshold. In this case, EPD is not performed, and the cell is discarded.

Table 2-25 describes the fields on the Set VP Shaping Thresholds dialog box.

Table 2-25. Set VP Shaping Thresholds Fields

Field	Displays...
Constant Bit Rate (CBR)	The CLP 0+1 threshold and EPD/CLP1 discard threshold for the CBR queue.
Variable Bit Rate (VBR) Real Time	The CLP 0+1 threshold and EPD/CLP1 discard threshold for the VBR Real Time queue.
Variable Bit Rate (VBR) Non-Real Time	The CLP 0+1 threshold and EPD/CLP1 discard threshold for the VBR Non-Real Time queue.
Available/Unspecified Bit Rate (ABR/UBR)	The CLP 0+1 threshold and EPD/CLP1 discard threshold for the ABR/UBR queue.

In addition to monitoring VP shaping on the physical port level, you can also monitor various types of logical ports associated with ATM OPTimum trunks on the CBX 500. VP shaping parameters appear when you monitor the administrative attributes of these logical ports. See Table 6-5 on page 6-7 for more information on monitoring logical port administrative attributes.

Displaying FDL Information for a T1 Port

If you configured a T1 physical port with Extended Superframe as its circuit type, you can view the facility data link (FDL) parameters, which provide information about the equipment connected to this T1 port.

To display the FDL information:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Select the T1 physical port for which you want to display FDL information. The View Physical Port Attributes dialog box appears.
4. Choose FDL. The system displays the Show ATM T1 Physical Port FDL Parameters dialog box (see Figure 2-26).

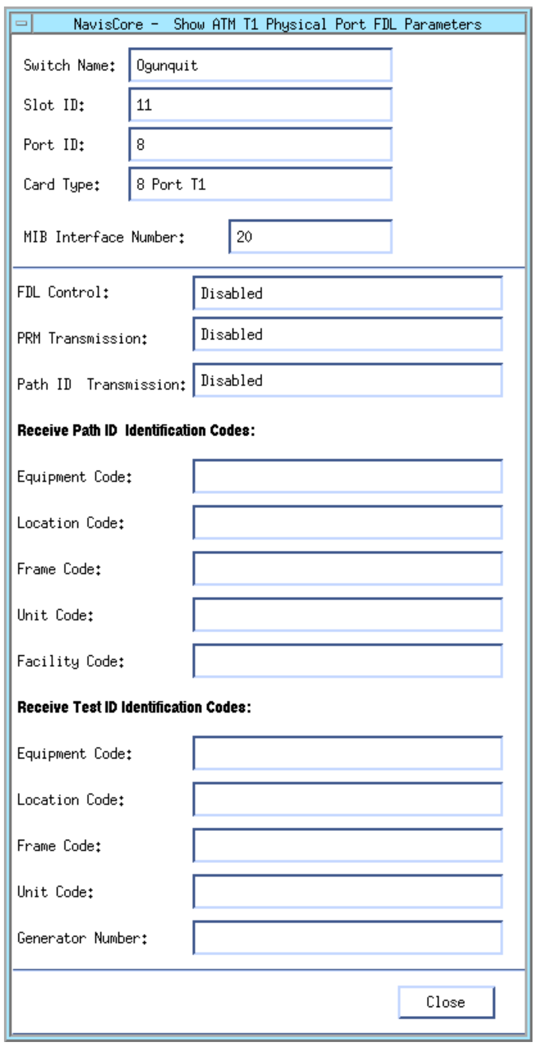


Figure 2-26. Show ATM T1 Physical Port FDL Parameters Dialog Box

Table 2-26 describes these dialog box fields.

Table 2-26. Show ATM T1 Physical Port FDL Parameters Fields

Field	Displays...
Switch Name	The name of the switch.
Slot ID	The number of the slot in which the T1 port's IOM resides.
Port ID	The T1 port number.
Card Type	The T1 IOM type (for example, "8 port T1").
MIB Interface Number	The MIB interface number for the T1 port. The software assigns a unique number to each physical port on the switch.
FDL Control	Enabled if this port uses the FDL control parameters; displays Disabled if the carrier does not use them.
PRM Transmission	Enabled if this port transmits a performance report message (PRM) signal; displays Disabled if it does not transmit this signal. (You can disable PRM transmission if the equipment connected to this port does not process PRM signals.) The T1 module processes incoming PRMs that provide error count information for far-end equipment.
Path ID Transmission	Enabled if this port transmits a Path ID signal; displays Disabled if it does not transmit this signal. (You can disable path ID transmission if the equipment connected to this port does not process path ID information.) The T1 module processes path ID messages it receives from other equipment.
Receive Path ID Identification Codes	The following information about the equipment connected to this T1 physical port: *Equipment Code* – The type of hardware connected to this port. *Location Code* – The location of this hardware. *Frame Code* – The location (within a building) of this hardware. *Unit Code* – The location of this equipment within a bay. *Facility Code* – The specific DS1 path the signal uses.
Receive Test ID Identification Codes	The following information about the test-signal-generating equipment connected to this physical port: *Equipment Code* – The type of test signal hardware connected to this port. *Location Code* – The location of this hardware. *Frame Code* – The location (within a building) of this hardware. *Unit Code* – The location of this equipment within a bay. *Generator Number* – Identifies the signal generator (for testing only).

Viewing ATM TCA Parameters

You can view Threshold Crossing Alarm (TCA) parameters for physical ports that handle ATM traffic. When TCA is enabled, threshold crossing provides support for traps that are generated during a variety of error conditions. This feature prevents the trap message log from receiving too many messages for the same trap condition.

When one of these conditions occurs, a trap is generated. When you enable threshold crossing, a timer is set to monitor specified conditions for a configured time period. No additional traps are generated unless the condition reoccurs more than *x* number of times, where *x* equals the threshold value.

When you configure threshold crossing, you specify a monitor period and threshold value for each physical port. See the *NavisCore Physical Interface Configuration Guide* for more information on configuring these parameters. If you disable threshold crossing, no trap message is generated.

To display TCA parameters:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Select the physical port that supports ATM traffic. The View Physical Port Attributes dialog box appears.
4. Select the ATM TCA button. The Threshold Crossing Alarm dialog box appears (see Figure 2-27).

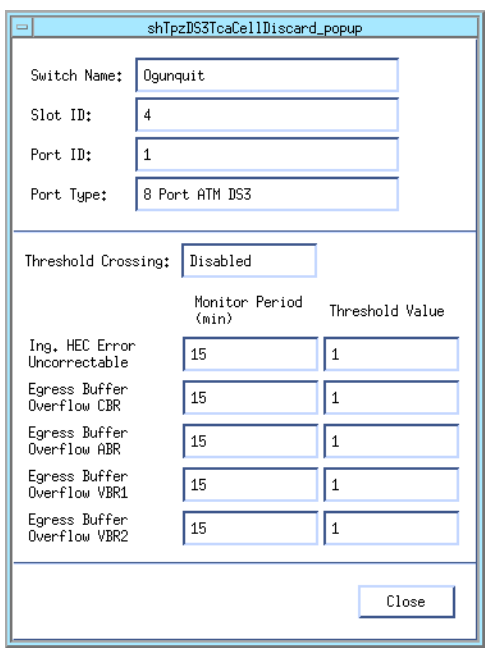


Figure 2-27. Threshold Crossing Alarm Dialog Box

Table 2-27 lists and describes the fields on the dialog box.

Table 2-27. TCA Parameters Fields

Field	Displays...
Switch Name	The name of the switch.
Slot ID	The number of the slot in which the physical port's IOM is installed.
Port ID	The number of the physical port.
Port Type	The physical port type.
Threshold Crossing	Enabled if TCA is enabled for the logical port; Disabled if TCA is disabled for the logical port.
Monitor Period (min.)	The TCA monitor period for each of the TCA parameters.
Threshold Value	The threshold value for each of the TCA parameters.
Ing. HEC Error Uncorrectable	The monitor period and threshold value for uncorrectable ingress header error control (HEC) conditions.
Egress Buffer Overflow CBR	The monitor period and threshold value for the CBR queue's egress buffer for overflow conditions.
Egress Buffer Overflow ABR	The monitor period and threshold value for the ABR queue's egress buffer for overflow conditions.
Egress Buffer Overflow VBR1	The monitor period and threshold value for the VBR1 queue's egress buffer for overflow conditions.
Egress Buffer Overflow VBR2	The monitor period and threshold value for the VBR2 queue's egress buffer for overflow conditions.

Viewing Physical Port Redundancy

On CBX 500 and GX 550 switches, you can view redundant pairs of OC-n/STM-n physical ports. These ports use SONET Automatic Protection Switching (APS) to switch from the working port to the protection (or backup) port during line outages. The Ascend implementation of APS is based on the Bellcore GR-253-CORE, 1994 standard.

Ascend supports physical port redundancy on the 4-port OC-3c/STM-1 module and single-port OC-12c/STM-4 module.

You can configure redundant physical port pairs, using the following APS implementations:

Intracard APS 1+1 — Both ports in the redundant pair are on the same IOM. On 4-port OC-3c/STM-1 IOMs, any two physical ports can be designated a redundant pair. Remaining physical ports can function as normal physical ports. On single-port OC-12c/STM-4 IOMs, you can have redundant physical ports even though only one physical port is on the IOM. The physical port pair does not map to two distinct physical ports. The physical port pair is really a single physical port that acts as two physical ports and is represented as such by NavisCore.

APS Resilient UNI — The ports in the redundant pair may reside on different IOMs, and the ports use resilient UNI to reroute traffic. You must configure a UNI logical port for each physical port in the pair. When you configure the UNI logical port for the protection physical port, you must enable the Can Backup Service Names parameter. See Table 6-5 on page 6-7 for a description of this parameter.

APS Trunk Backup — The ports in the redundant pair may reside on different IOMs, and the switch uses APS to move traffic from a primary trunk (working port) to a backup trunk (protection port). You must configure a trunk logical port for both the working port and protection port. You must designate the trunk associated with the working port as the primary trunk and the trunk associated with the protection port as the backup trunk. See Table 12-2 on page 12-4 for more information on primary trunks and backup trunks.

For information on how to configure APS, see the *NavisCore Physical Interface Configuration Guide* and the *NavisCore ATM Configuration Guide*.

Viewing Physical Port Pairs

On the Switch Back Panel dialog box, when you select a physical port in a redundant port pair, two arrowheads appear next to each port in the pair. For example, in Figure 2-28, ports 1 and 2 on the IOM in slot 14 make up an Intracard APS 1+1 redundant physical port pair.

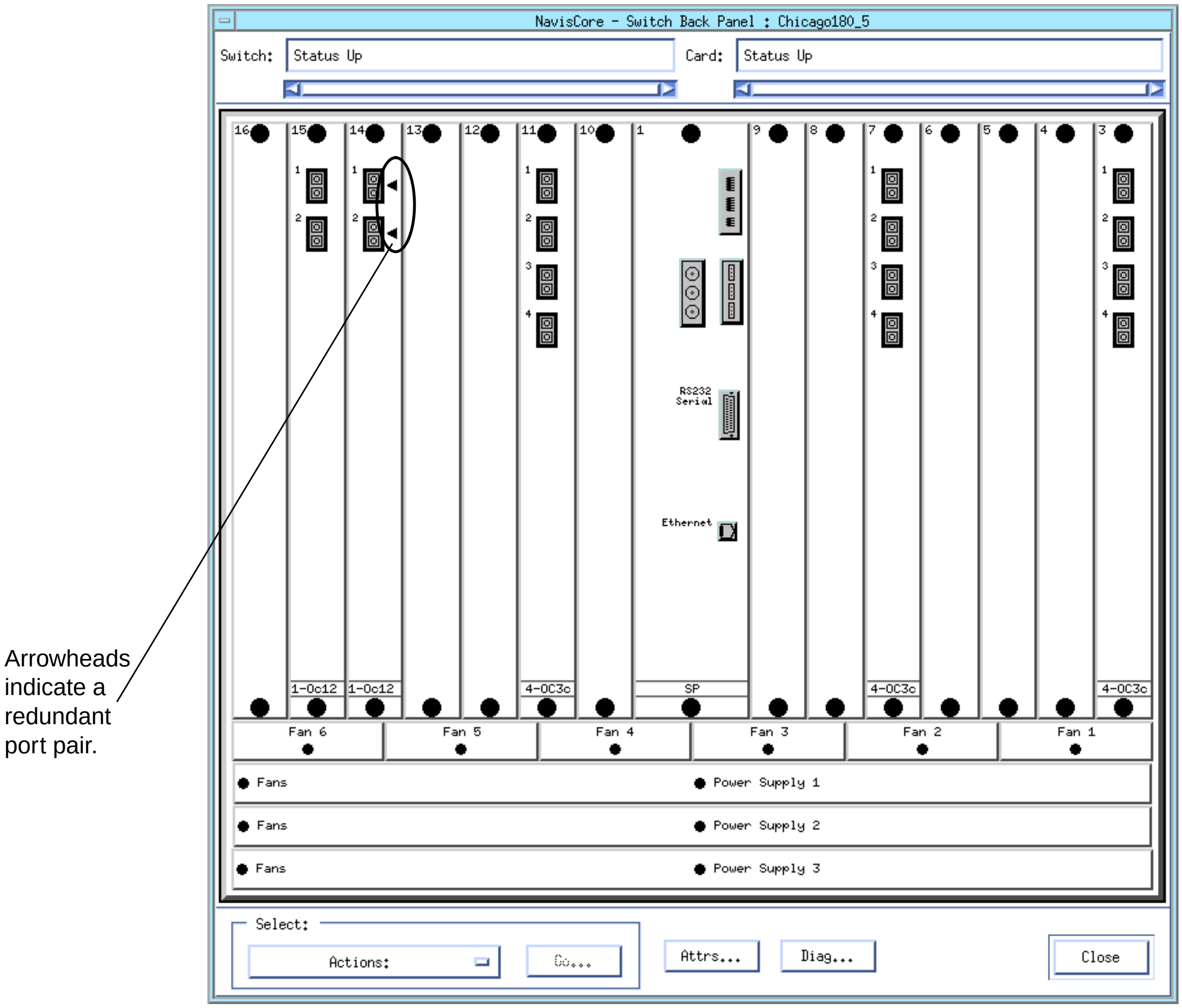


Figure 2-28. Redundant Physical Ports

Notice that the physical port pair resides on a single-port OC-12 IOM. In reality, there is only one distinct physical port on the IOM, but NavisCore represents it as two distinct physical ports.

To view all of the redundant physical port pairs on a CBX 500 or GX 550 switch:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 2-6 on page 2-10 or Figure 2-7 on page 2-11).
3. Select Actions.
4. Select View Port Redundancy from the Actions option menu.
5. Choose Go. The Physical Port Redundancy Pairings dialog box appears (see Figure 2-29).

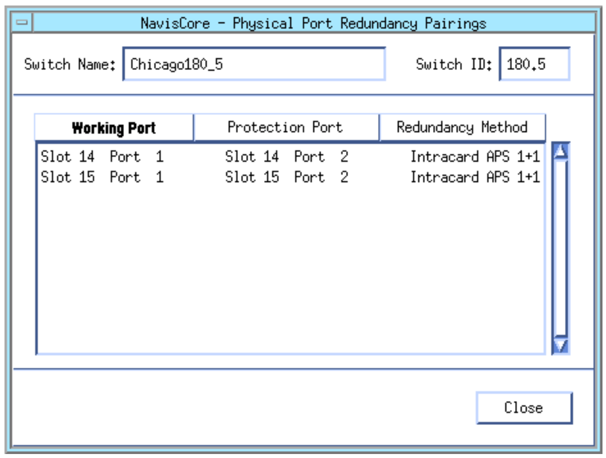


Figure 2-29. Physical Port Redundancy Pairings Dialog Box

The Physical Port Redundancy Pairings dialog box lists all the configured redundant port pairs. You can click on each column heading to sort by working port, protection port or redundancy method. The selected sort criteria is in bold.

For each pair, the dialog box lists:

- The port number of the working port.
- The port number of the protection (or backup) port.
- The redundancy method used to switch between ports. The method can be one of the following:
  - Intracard APS 1+1 (both ports are on the same IOM)
  - APS Resilient UNI (the ports use resilient UNI to re-route traffic)
  - APS Trunk Backup (the switch uses APS to move traffic to a backup trunk)

Viewing APS Attributes

To view APS attributes for each member of a redundant physical port pair:

1. On the network map, double-click the appropriate switch object. The system displays the Switch Back Panel dialog box.
2. Double-click an OC-n/STM-n physical port that is part of a redundant port pair. The Physical Port Attributes dialog box appears.
3. Choose APS. The Show APS Attributes dialog box appears for the selected port. Figure 2-30 shows the attributes for an ATM OC-12c/STM-4 physical port.

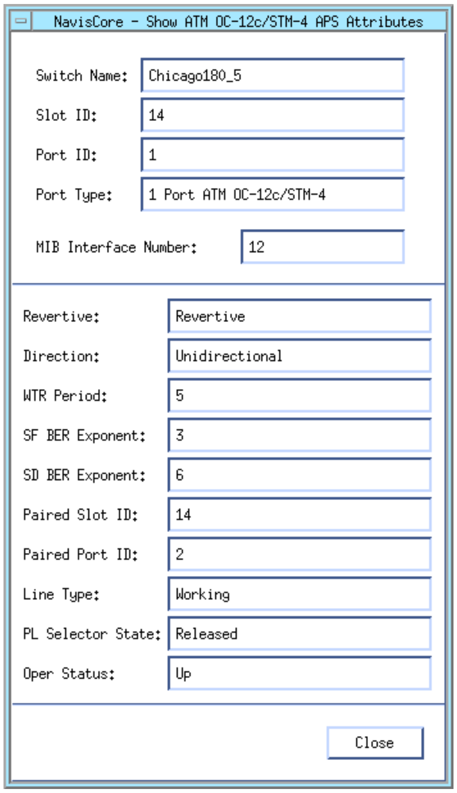


Figure 2-30. Show APS Attributes Dialog Box (OC12c/STM-4)

Table 2-28 lists and describes the fields on the dialog box.

Table 2-28. Show APS Attributes Fields

Field	Displays...
Switch Name	The name of the switch you are monitoring.
Slot ID	The number of the slot that contains this IOM and port.
Port ID	The number of the selected physical port.
Port Type	The selected physical port's type.
MIB Interface Number	The MIB interface number for the physical port. The software assigns a unique interface number to each physical port on the switch.
Revertive	The revertive mode: Revertive or Non-Revertive. When a Signal Fail (SF) condition or a Signal Degrade (SD) condition occurs on the working port, the switch selects the protection port to send and receive data. If the physical port is configured for revertive mode, the Ascend switch will revert back to the working port after the SF or SD condition clears. Following the clearing of the condition, the switch waits the "Wait-to-Restore" period before reverting back to the working port. If the physical port is in non-revertive mode, the switch does not automatically revert back to the working port. Instead, you must issue an APS command to switch back to the working port. See "Issuing APS Commands" on page 2-71 for details.
Direction	The directional mode: Unidirectional or Bidirectional. If the mode is unidirectional, protection-switching decisions are based on local requests only. This means that each end of the SONET line can make switching decisions independently. One end may receive data on the protection port while the other end may receive data on the working port. If the mode is bidirectional, protection-switching decisions are based on both local requests and remote requests. Both ends always transmit data and receive data on the same pair of fibers.
WTR Period	The Wait-to-Restore period, in minutes.
SF BER Exponent	The exponent that the switch uses to calculate the SF BER condition threshold. If this threshold is exceeded, the switch generates an SF BER condition that can trigger APS protection switching. The switch clears the condition when the SF BER threshold drops below 10^-7. The SF BER condition threshold granularity is expressed as a power of 10. For example, if 3 appears in this field, the SF BER condition threshold is 10^-3.
SD BER Exponent	The exponent that the Ascend switch uses to calculate the SD BER condition threshold. If this threshold is exceeded, an SD condition is generated that can trigger APS protection switching. The condition is cleared when the SD BER threshold drops below 10^-(n + 1) where n is the exponent you specify. The SD BER threshold granularity is a power of ten. For example, if 6 appears in this field, the SD failure threshold is 10^-6.

Table 2-28. Show APS Attributes Fields (Continued)

Field	Displays...
Paired Slot ID	The number of the slot that contains the paired port's IOM.
Paired Port ID	The port number of the paired port.
Line Type	"Working" indicates that the selected physical port is the working port. "Protection" indicates that the selected physical port is the protection port.
PL Selector State	The state of the protection line selector. "Released" indicates that network traffic is sent and received on the working port. "Selected" indicates that network traffic is sent and received on the protection port.
Oper Status	The port's operational status (Up or Down).

Issuing APS Commands

APS commands allow you to manually clear signal fail (SF) and signal degrade (SD) conditions and to switch network traffic from the working port to the protection port and vice versa.

To issue APS commands:

> ► To issue APS commands, you must log on to NavisCore.

1. On the network map, select the appropriate switch.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters.
3. Double-click on a port in a redundant port pair. The Set Physical Port Attributes dialog box appears (see Figure 2-31).

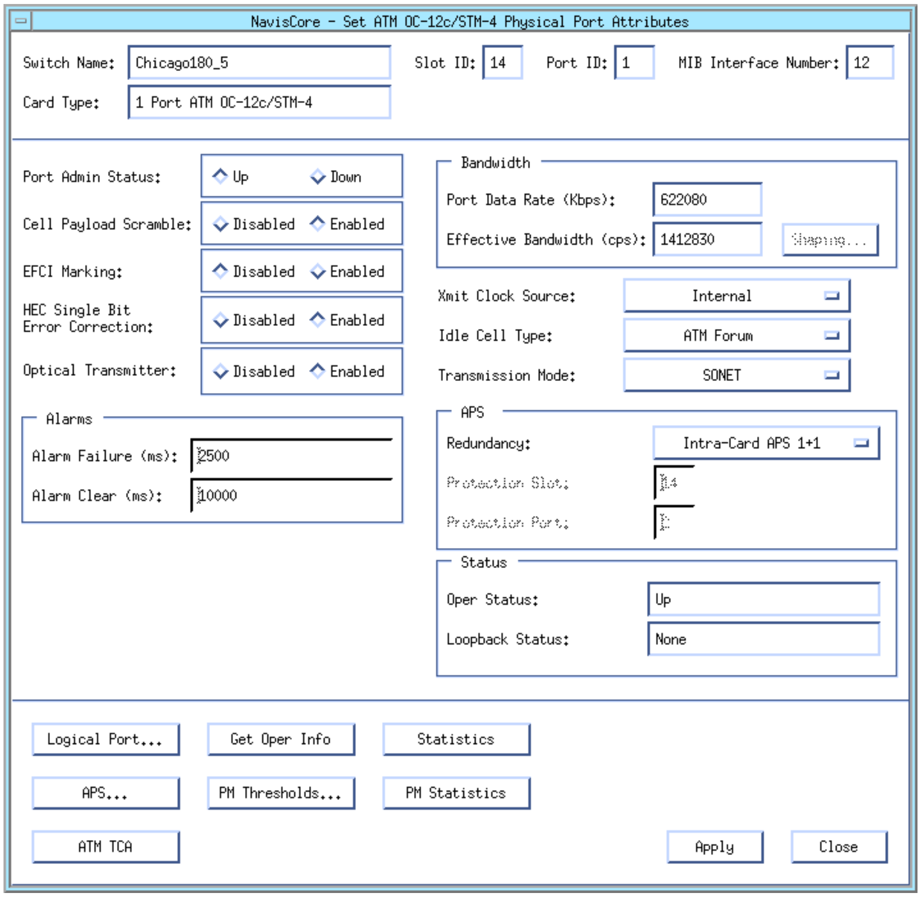


Figure 2-31. Set Physical Port Attributes Dialog Box (OC-12c/STM-4)

4. Choose APS. The Set APS Attributes dialog box appears (see Figure 2-32).

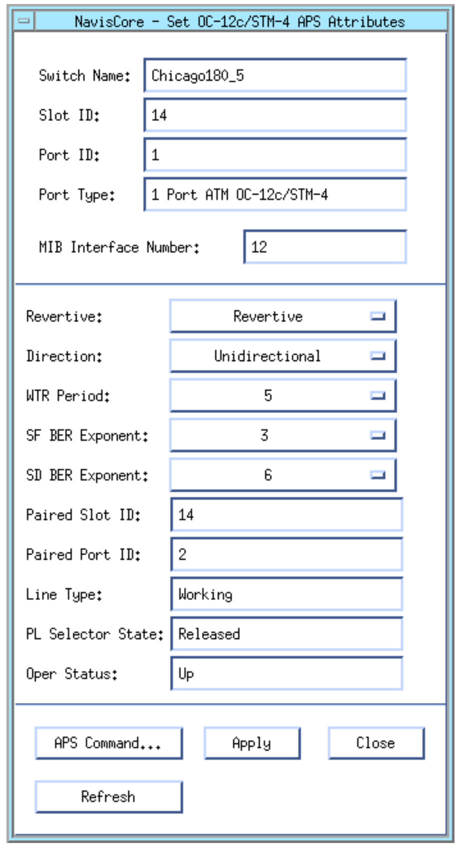


Figure 2-32. Set APS Attributes Dialog Box

5. Choose APS Command. The Send APS Command dialog box appears (see Figure 2-33).

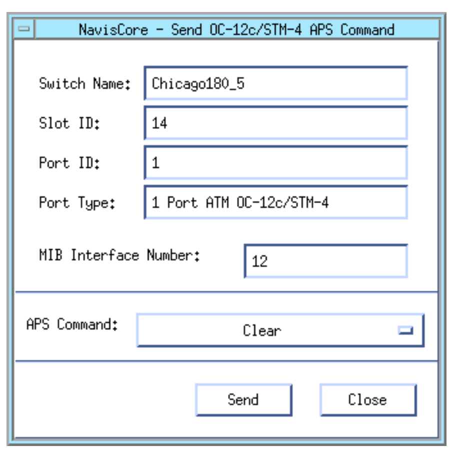


Figure 2-33. Send APS Command Dialog Box

The APS Command option menu enables you to issue APS commands. The specific commands that you can issue depend on your port selection (working port or protection port). Table 2-29 describes working port commands. Table 2-30 describes protection port commands.

6. Select the APS command you want to use.
7. Choose Send.
8. Choose OK when prompted.

Table 2-29. Working Port APS Commands

Command	Function
Clear	Clears all previously issued APS commands. If you cannot issue a command because one of equal or higher priority is in effect, issue the Clear command to cancel the previously issued command. Then, issue the new command. From highest priority to lowest priority, the order is as follows: 1. Lockout of Protection 2. Forced Switch 3. Automatic Switch (due to line outages) 4. Manual Switch 5. Exercise
Forced Switch (Work->Protect)	Switches network traffic to the protection port unless a command of equal or higher priority is in effect.
Manual Switch (Work->Protect)	Switches network traffic to the protection port unless a command of equal or higher priority is in effect.

Table 2-30. Protection Port APS Commands

Command	Function
Clear	Clears all previously issued APS commands. If you cannot issue a command because one of equal or higher priority is in effect, issue the Clear command to cancel the previously issued command. Then, issue the new command. See Table 2-29 for details on command priority.
Lockout of Protection	Protects the working port from switching network traffic to the protection port. If a working port has already switched traffic to the protection port, the traffic is switched back to the working port.
Forced Switch (Protect->Work)	Switches network traffic to the working port unless a command of equal or higher priority is in effect.
Manual Switch (Protect->Work)	Switches network traffic to the working port unless a command of equal or higher priority is in effect.
Exercise	Tests the protocol for protection switching unless a command of equal or higher priority is in effect. The switch-over is not actually completed.

3

Generating Physical Port Statistics

This chapter describes how to generate and view real-time physical port statistics to monitor and troubleshoot an Ascend switch network. You use NavisCore to set the polling interval to retrieve summary statistics and to view statistics for a physical port.

Supported Statistics

This section describes the types of available physical port statistics.

Physical port summary statistics are available for all I/O modules (IOMs). See the section "Viewing Physical Port Summary Statistics" on page 3-2 for details.

Along with physical port summary statistics, the following IOMs provide additional statistics on physical port activity:

Channelized IOMs — Alarms and statistics specific to DS1/E1 channel activity on channelized IOMs. See the section "Viewing DS1 Channel Alarms and Statistics" on page 3-10 for details.

4-Port Unchannelized E1, E1 PRI and Channelized E1 IOMs — ITU G.826 statistics. See the section "Viewing G.826 Statistics for 4-Port E1, E1 PRI, and Channelized E1 Modules" on page 3-14 for details.

12-Port E1 IOMs — RFC 1406 statistics and G.826 statistics.

For some IOMs, you can also view performance monitoring statistics. See Chapter 4, "Monitoring Physical Port Performance" for details.

Setting the Polling Interval

The Polling function sets the time interval for collecting and retrieving statistical data during the current session of NavisCore.

To modify the default time interval (five seconds):

1. From the Misc menu, select Ascend Time Intervals ⇒ Set Statistics Time Interval. The following Change Statistics Polling Interval dialog box appears, displaying the current time interval (see Figure 3-1).

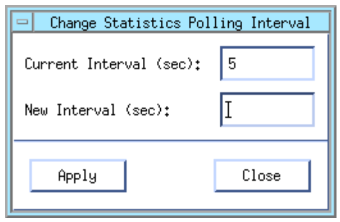


Figure 3-1. Change Statistics Polling Interval Dialog Box

2. Enter a new value in seconds.

3. Choose Apply to save the changes.

4. Choose Close to exit the dialog box.

Viewing Physical Port Summary Statistics

You can view physical port summary statistics, which show the data a physical port has sent and received.

To view physical port summary statistics:

1. Select the appropriate switch object on the network map.

2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears for the selected switch type:

- Figure 3-2 shows the Switch Back Panel dialog box for a B-STDX 8000/9000 switch.
- Figure 3-3 shows the Switch Back Panel dialog box for a CBX 500 switch.
- Figure 3-4 shows the Switch Back Panel dialog box for a GX 550 switch.

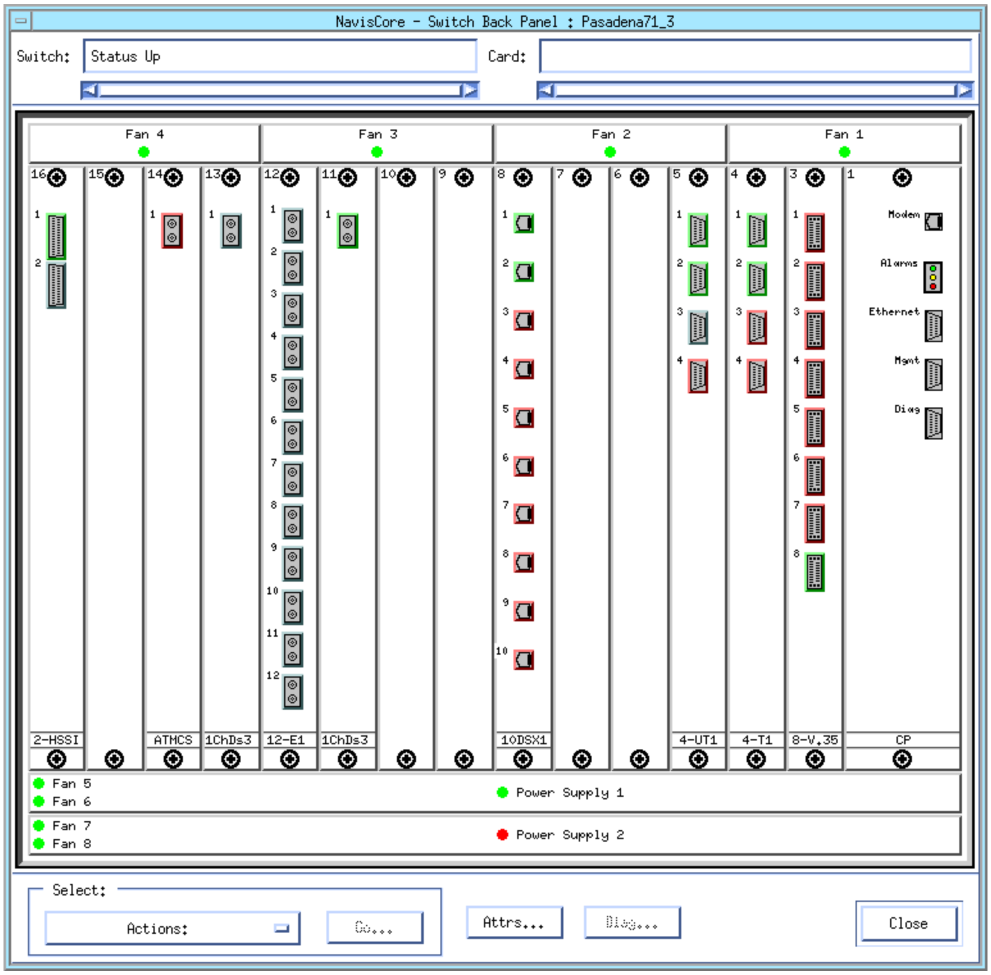


Figure 3-2. Switch Back Panel Dialog Box (B-STDX 8000/9000)

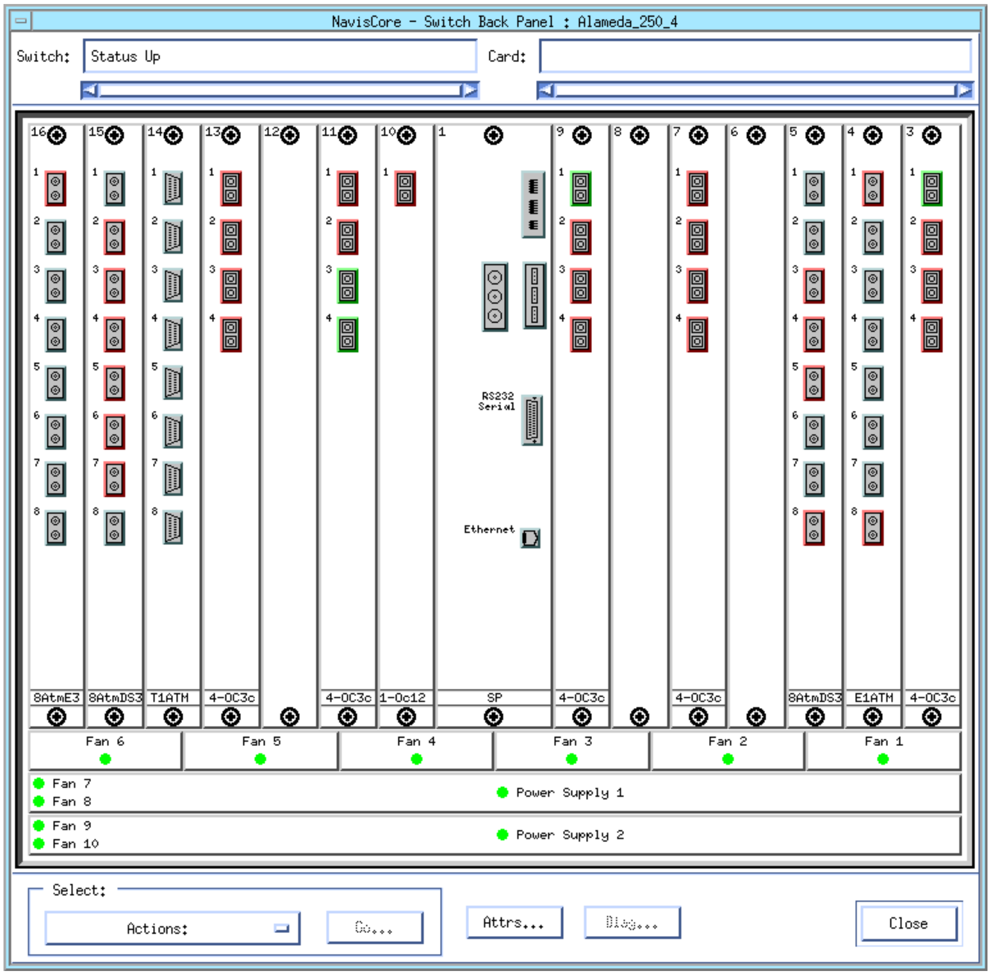


Figure 3-3. Switch Back Panel Dialog Box (CBX 500)

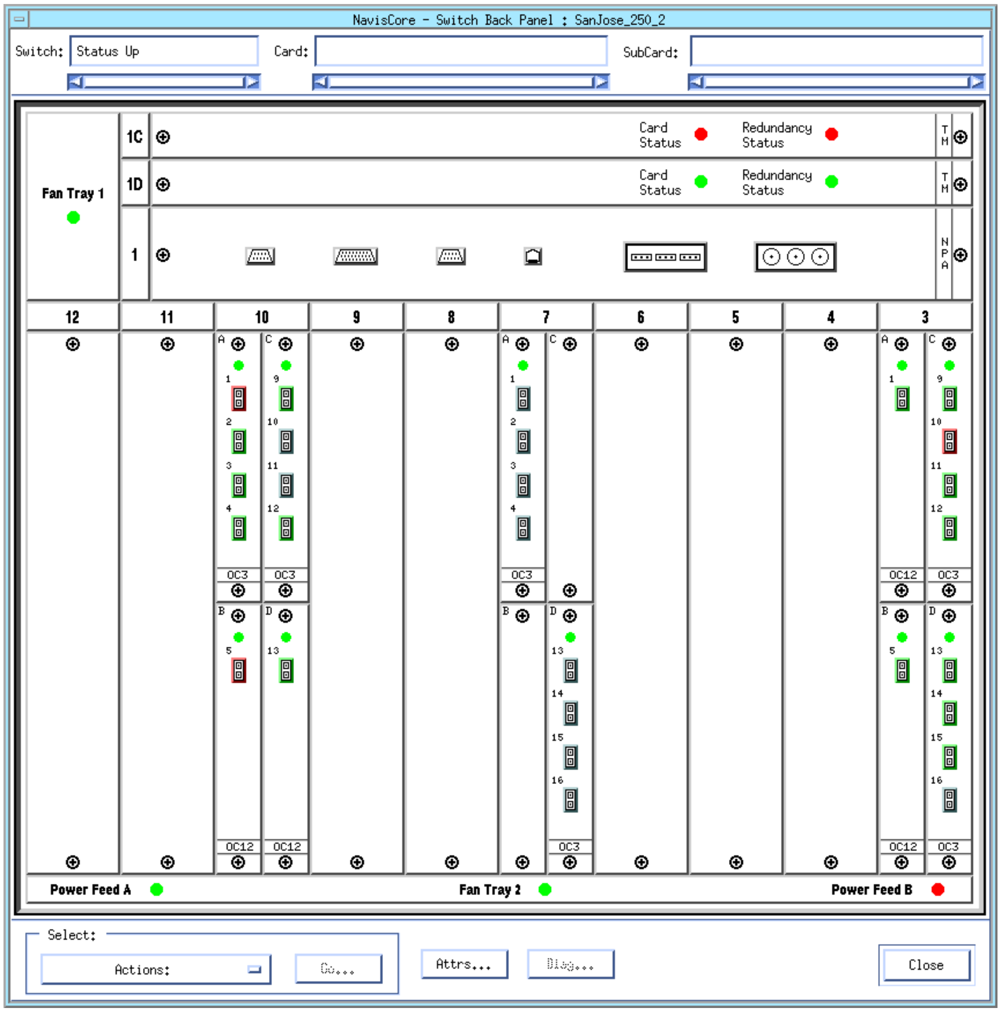


Figure 3-4. Switch Back Panel Dialog Box (GX 550)

3. Double-click on the physical port. The View Physical Port Attributes dialog box appears for the selected physical port. Figure 3-5 shows a sample View Physical Port Attributes dialog box (for an OC-3c/STM-1 physical port). The specific fields that appear on the dialog box vary depending on the type of IOM.

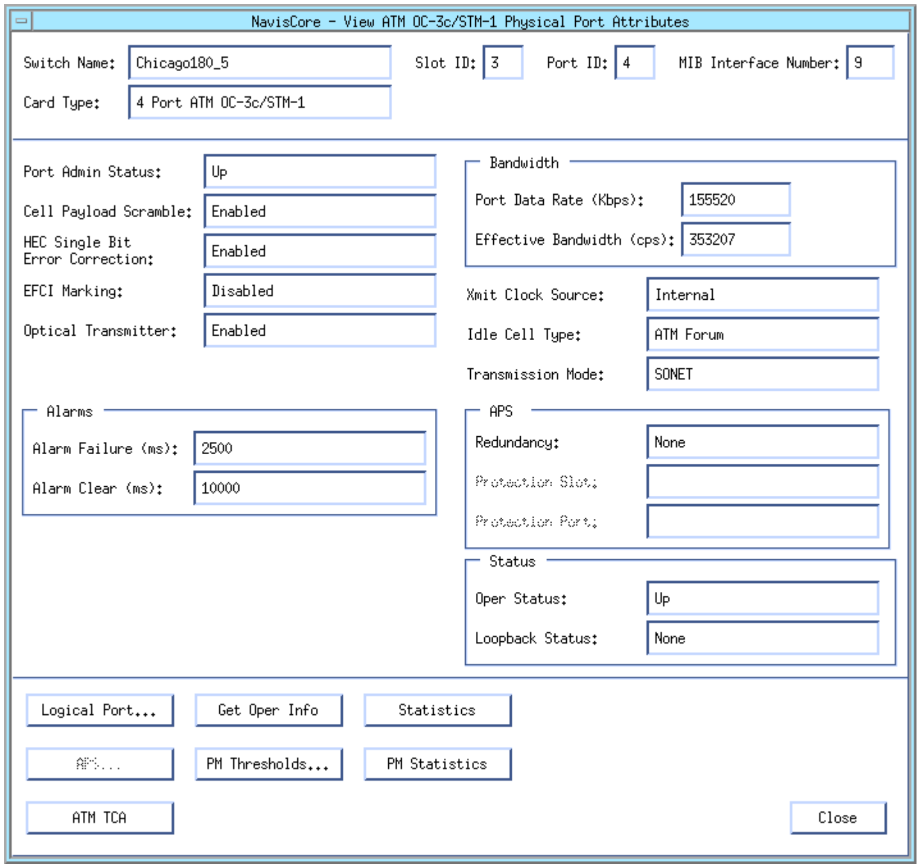


Figure 3-5. View Physical Port Attributes Dialog Box (OC-3c/STM-1)

4. Choose Statistics. The Physical Port Summary Statistics dialog box appears. The type of statistics that appear depend on the type of IOM and physical port:

   - Figure 3-6 shows statistics on ATM traffic for an OC-3c/STM-1 physical port.
   - Figure 3-7 shows statistics on Frame Relay traffic for a T1 physical port.
   - Figure 3-8 shows statistics on both ATM and Frame Relay traffic for an ATM CS E3 physical port that is used for Frame-to-ATM internetworking.

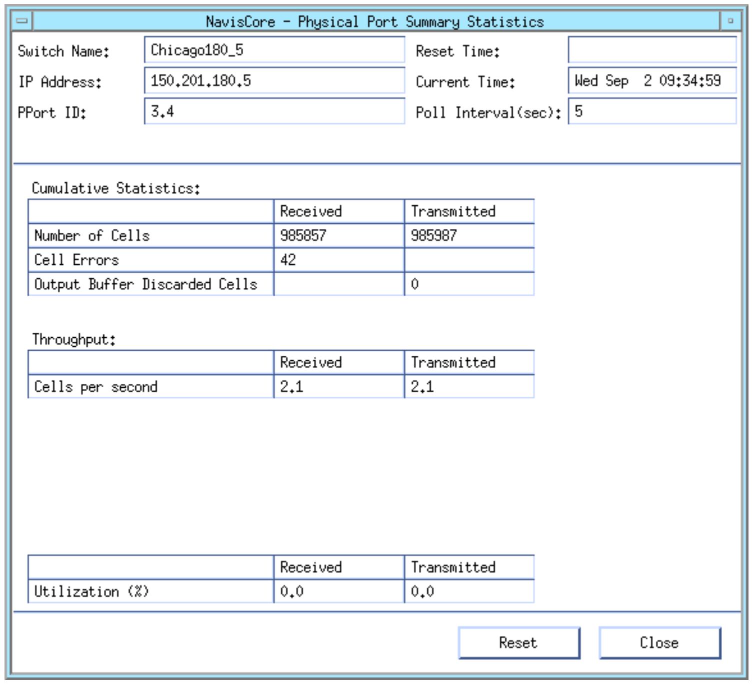


Figure 3-6. Physical Port Summary Statistics Dialog Box (OC3c/STM-1)

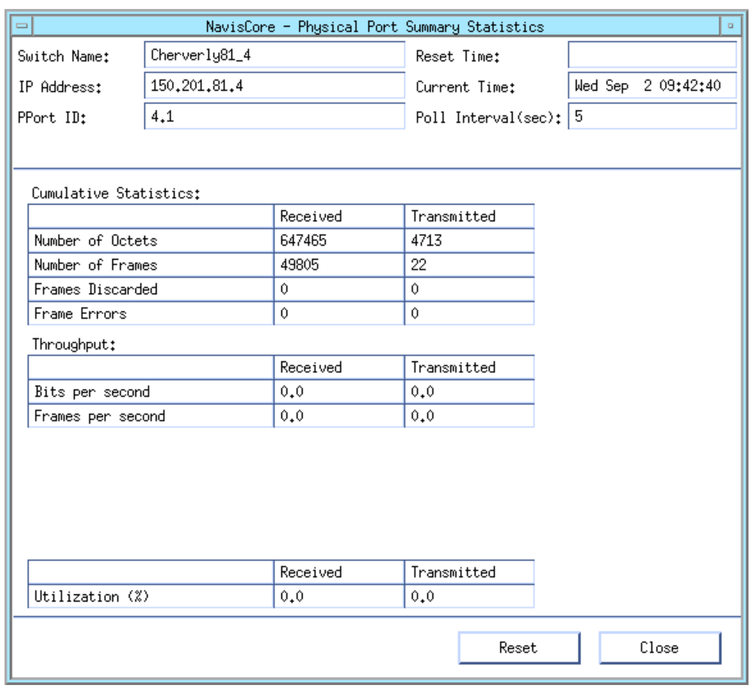


Figure 3-7. Physical Port Summary Statistics Dialog Box (T1)

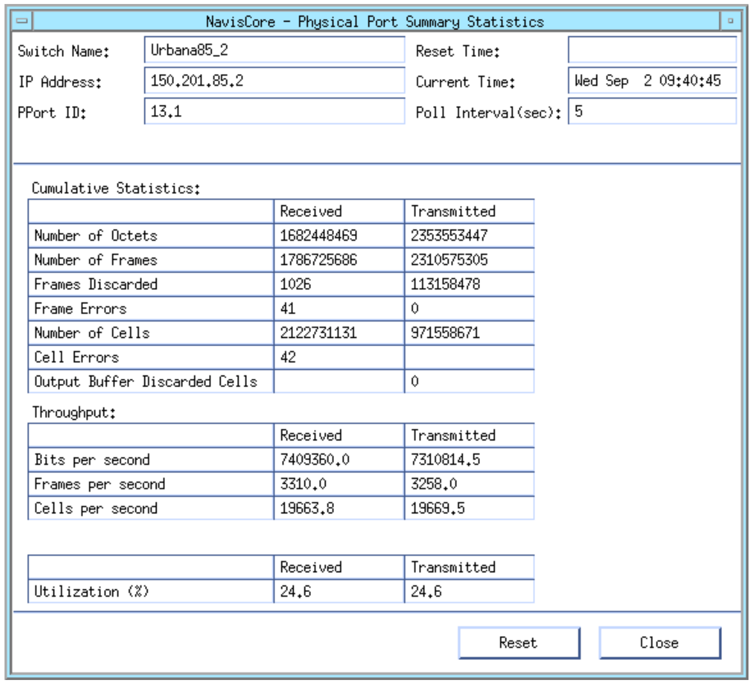


Figure 3-8. Physical Port Summary Statistics Dialog Box (CS E3)

The Physical Port Summary Statistics dialog box displays cumulative statistics and throughput data that reflects the transmission and receipt of data on the physical port.

Table 3-1 describes each of the fields on the Physical Port Summary Statistics dialog box. The specific fields will vary, depending on the type of traffic that the physical port supports. For example, if the physical port supports ATM traffic only, you will only see cumulative statistics for cell traffic. However, if the physical port supports both ATM and Frame Relay traffic, you will see cumulative statistics for both cell and frame traffic.

5. (*Optional*) Use the Reset button to clear the current statistics and update the time in the Reset Time field.

6. When you finish viewing the statistics, choose Close to exit.

Table 3-1. Physical Port Summary Statistics Fields

Statistic	Description
Switch Name	The name of the switch.
IP Address	The internal IP address of the switch.
PPort	The physical port number.
Reset Time	The time that the Reset button was last selected to reset counters.
Current Time	The current system time.
Poll Interval (sec)	The time interval for the collection of statistical data.
Cumulative Statistics	
Number of Octets	The total number of octets (bytes) received and transmitted since the last reset.
Number of Frames	The total number of frames received and transmitted since the last reset.
Frames Discarded	The total number of frames discarded since the last reset. If the system is discarding frames, graceful discard is set to OFF. The switch does not discard frames if graceful discard is set to ON. The graceful discard option is set during the configuration of a circuit.
Frame Errors	The total number of frame errors. This value includes all green, amber, and red frame errors.
Number of Cells	The total number of cells received and transmitted by the port since the last reset.
Cell Errors	The total number of cells that were received with a Header Error Control (HEC) error. A HEC error indicates a discrepancy between what the port expected in the header and what was actually received. The number of cell errors is indicated in the Received column. The Transmitted column does not apply.
Output Buffer Discarded Cells	The number of discarded cells.
Throughput Statistics	
Bits per Second	The total number of bits received and transmitted each second.
Frames per Second	The total number of frames received and transmitted each second.
Cells per Second	The total number of cells received and transmitted each second.
Utilization Statistic	
Physical Port Utilization (%)	The amount of traffic queued for transmission on a physical port, measured as a percentage of the physical port speed. This value does not measure the amount of bandwidth of the physical port in use. For this reason, the value can exceed 100%.

Viewing DS1 Channel Alarms and Statistics

This section describes how to view alarm status and statistics for DS1 channels on channelized DS3 and DS3-1-0 IOMs. These IOMs are supported on B-STDX switches.

Viewing DS1 Channel Alarms

The Channel Alarm Status dialog box displays the alarm status of all DS1 channels.

To view the alarm status:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 3-2 on page 3-3).
3. Double-click on the channelized DS3 or DS3-1-0 physical port. The View Physical Port Attributes dialog box appears.
4. Choose Chan Alarm Status. The Channel Alarm Status dialog box (see Figure 3-9).

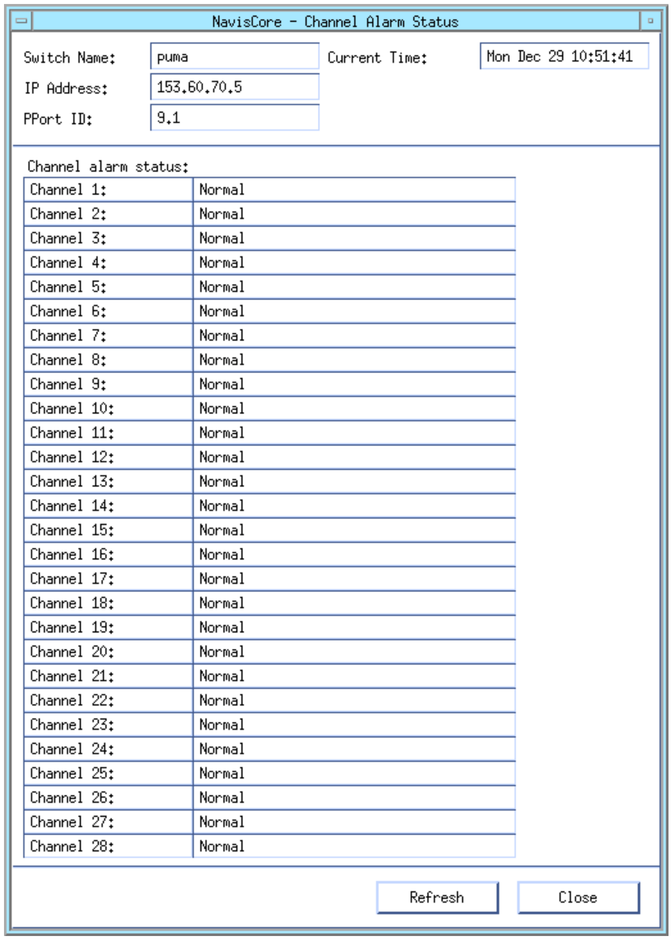


Figure 3-9. DS1 Channel Alarm Status Dialog Box

Table 3-2 lists and describes the possible alarm states.

Table 3-2. DS1 Channel Alarm States

Alarm State	Description
Normal	Normal operating state
Red	Loss of frame or loss of signal
Yellow	Far end is in a red alarm state
Blue	Downstream equipment failure

5. Choose Refresh to clear the alarm status.
6. Choose Close to exit and return to the View Physical Port Attributes dialog box.

Viewing DS1 Channel Statistics

This section describes how to view summary statistics for selected DS1 channels on channelized DS3 or DS3-1-0 modules. For information on viewing detailed performance statistics, see "Viewing DS1 Channel Data" on page 4-29.

To view channel summary statistics:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 3-3 on page 3-4).
3. Double-click on the channelized DS3 or DS3-1-0 physical port. The View Physical Port Attributes dialog box appears.
4. Double-click on the channel button for the DS1 channel whose summary statistics you want to view. The Channel Attributes dialog box appears (see Figure 3-10).

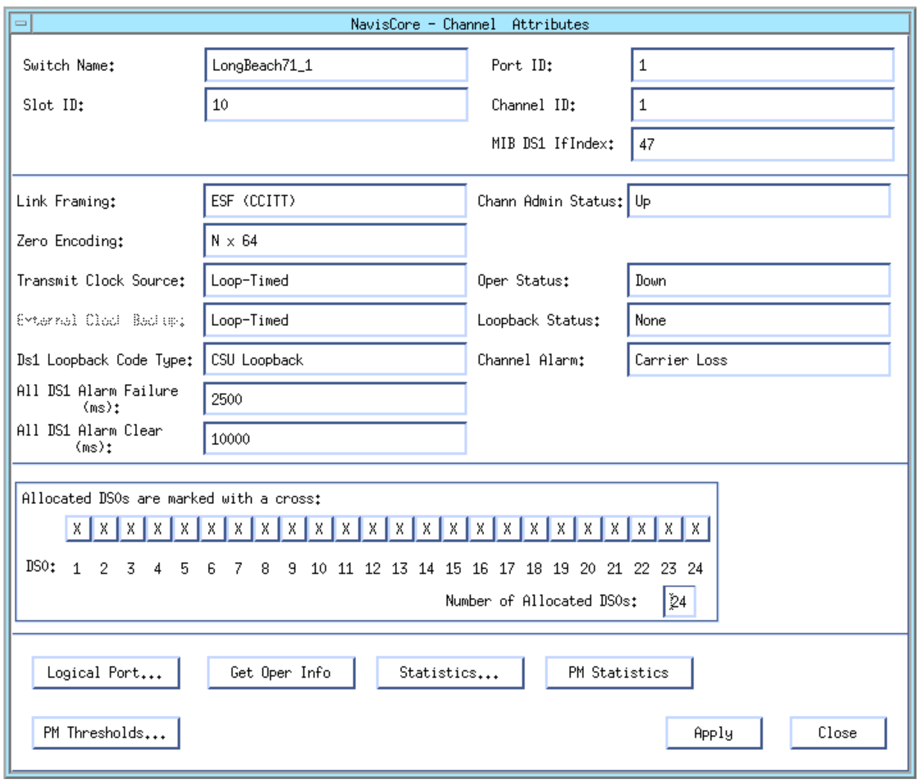


Figure 3-10. Channel Attributes Dialog Box

See Table 2-23 on page 2-54 for descriptions of the fields on this dialog box.

5. Choose Statistics. The Channel Summary Statistics dialog box appears (see Figure 3-11.

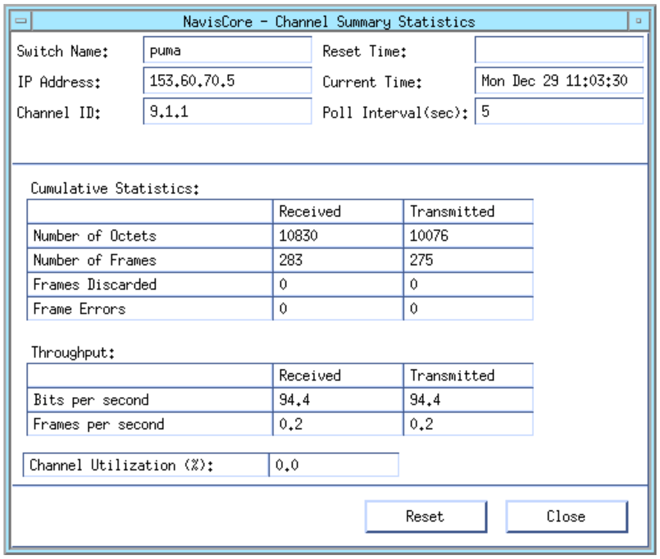


Figure 3-11. Channel Summary Statistics Dialog Box

Table 3-3 describes the Channel Summary Statistics fields.

Table 3-3. Channel Summary Statistics Fields

Statistic	Description
Switch Name	Name of the switch in which the module resides.
IP Address	IP address of the switch.
Channel ID	Channel number of the selected channel.
Reset Time	Time that a reset occurred.
Current Time	Current time.
Poll Interval (sec)	Number of seconds between polling intervals.
Cumulative Statistics	
Number of Octets	The total number of octets (bytes) received and transmitted since the last reset.
Number of Frames	The total number of frames received and transmitted since the last reset.
Frames Discarded	The total number of frames discarded since the last reset.
Frame Errors	The total number of frame errors. This value includes all green, amber, and red frame errors.
Throughput Statistics	
Bits per Second	The total number of bits received and transmitted each second.

Table 3-3. Channel Summary Statistics Fields (Continued)

Statistic	Description
Frames per Second	The total number of frames received and transmitted each second.
Utilization Statistic	
Channel Utilization (%)	The amount of traffic queued for transmission on a channel measured, as a percentage of the channel speed. This value does not measure the amount of bandwidth of the channel in use. For this reason, the value can exceed 100%.

Viewing G.826 Statistics for 4-Port E1, E1 PRI, and Channelized E1 Modules

This section describes how to view G.826 statistics for physical ports on 4-port E1, E1 PRI, and channelized E1 I/O modules, which are supported on B-STDX switches. These statistics provide you with performance information on digital transmission paths.

For information on viewing G.826 statistics for 12-port E1 modules, see "Viewing Additional Physical Port Statistics for 12-Port E1 Modules" on page 3-16.

To view G.826 statistics for E1 IOMs:

1. Select the B-STDX switch that contains the 4-port E1, E1 PRI, or channelized E1 module on the network map.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The back panel dialog box for the switch appears.
3. Select the physical port. The View Physical Port Attributes dialog box for the selected physical port appears.
4. Select G.826 Statistics. A dialog box appears that displays the G.826 statistics. Table 3-4 describes these statistics.

Table 3-4. G.826 Statistics

Statistic	Description
Switch Name	The name of the switch.
IP Address	The IP address of the selected switch.
Pport ID	The physical port number.
Refresh Time	The time at which the statistics were last refreshed.
E1 Current Statistics	
Errored Blocks	A count of detected block errors within a 15-minute interval. Block errors occur in frames that have cyclic redundancy check (CRC) or framing errors.
Errored Seconds	A count of one-second intervals with one or more errored blocks or at least one defect within a 15-minute interval.
Severely Errored Seconds	A count of one-second periods with either 30% errored blocks or at least one defect within a 15-minute interval.
Background Block Errors	A count of block errors that were detected but did not occur as part of a severely errored second within a 15-minute interval.
Errored Seconds Ratio	A ratio of accumulated errored seconds to total seconds in the available time.
Severely Errored Seconds Ratio	A ratio of accumulated severely errored seconds to total seconds in the available time.
Background Block Error Ratio	A ratio of background block errors to total received blocks (E1 frames) in the available time.

Viewing Additional Physical Port Statistics for 12-Port E1 Modules

For each physical port on a 12-port E1 module, you can view statistics that are based on the following standards:

- RFC 1406
- ITU G.826

The 12-port E1 module is supported on B-STDX switches. You access these statistics through the E1 Statistics button on the View Physical Port Attributes dialog box. Then, after specifying the appropriate standard (RFC 1406 or ITU G.826), you can access the following information:

Configuration — View the E1 configuration statistics.

Current — View up-to-date statistics. The counter tracks errors encountered by the E1 interface during the previous 15-minute interval.

Interval — View statistics for the previous 24 hours based on a specified number of 15-minute intervals.

Total — View statistics for the sum of all intervals and the current interval. The counter tracks errors encountered by the E1 interface during the previous 24-hour interval.

Accessing E1 Statistics

To access RFC 1406 or G.826 statistics:

1. Select the B-STDX switch that contains the 12-port E1 module on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 3-3 on page 3-4).
3. Select the physical port on the 12-port E1 IOM. The View Physical Port Attributes dialog box appears.
4. Choose E1 Statistics. The E1 Statistics dialog box appears (see Figure 3-12).

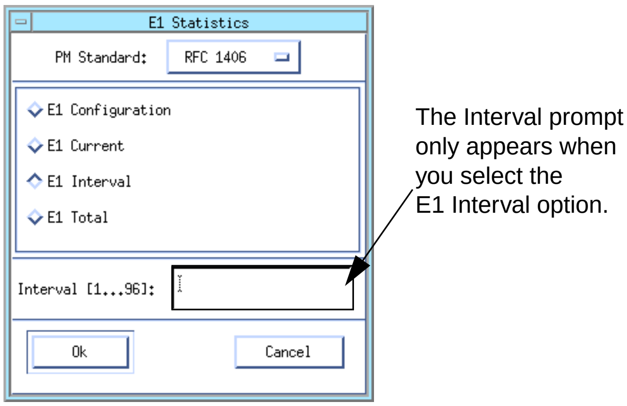


Figure 3-12. E1 Statistics Dialog Box

5. Select RFC 1406 or ITU G.826 from the PM Standard option menu.
6. Select from the following types of statistics and choose OK.

   E1 Configuration — View configuration statistics, including error and performance statistics. See "Viewing E1 Configuration Statistics" on page 3-18.

   E1 Current — View statistics accumulating in the present interval. See "Viewing E1 Current, Interval, and Total Statistics" on page 3-20.

   E1 Interval — View statistics that were collected during previous, user-specified 15-minute intervals. If you select this option, you must specify a polling interval. The Interval [1...96] function sets the time interval for collecting statistical data during the current session of NavisCore. Specify a number between 1 and 96 in the Interval [1...96] field. (For example, interval 4 displays statistics from the previous hour.) See "Viewing E1 Current, Interval, and Total Statistics" on page 3-20.

   E1 Total — View statistics for the sum of all intervals and the current interval. See "Viewing E1 Current, Interval, and Total Statistics" on page 3-20.

   An E1 Statistics dialog box appears depending on your selection. Table 3-5 describes the fields that are common to all E1 dialog boxes.

Table 3-5. E1 Fields (All Dialog Boxes)

Field	Displays...
Switch Name	Name of the switch containing the channelized E1 module.
IP Address	IP address of the switch in which the module resides.
PPort ID	The number of the selected E1 physical port.
Current Time	Current time.
PM Standard	The selected standard: RFC 1406 or ITU G.826.

Viewing E1 Configuration Statistics

The E1 Statistics dialog box lists the E1 configuration statistics, including error and performance event statistics.

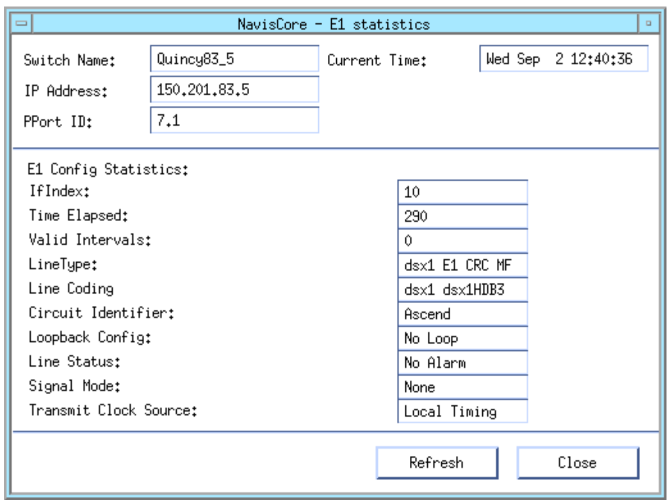


Figure 3-13. E1 Statistics Dialog Box (Configuration Statistics)

Table 3-6 lists and describes the E1 configuration statistics.

Table 3-6. E1 Configuration Statistics (RFC 1406 and G.826)

Statistic	Description
IfIndex	The unique interface number for this interface on the switch.
Time Elapsed	The number of elapsed seconds since the beginning of the current error-measurement period.
Valid Intervals	The number of previous intervals for which valid data was collected.
LineType	The E1 link framing method implemented on this circuit (e.g., E1 CRC MF, which is the same as TS16 enabled and CRC4 enabled).
Line Coding	The type of zero code suppression used on the link. The E1 link uses High Density Bipolar of Order 3 (HDB3).
Circuit Identifier	The transmission vendor’s circuit identifier (Ascend).
Loopback Config	The current loopback status of the E1 interface (e.g., No Loop).
Line Status	The interface line status (e.g., No Alarm).
Signal Mode	The E1 signal mode, which indicates the method used to reserve bits for signaling. “None” means that no bits are reserved for signaling.
Transmit Clock Source	The source of transmit clock (e.g., Local Timing, which is the same as Internal).

Viewing E1 Current, Interval, and Total Statistics

E1 Current Statistics provide up-to-date statistical information for the current 15-minute interval. Table 3-7 and Table 3-8 list and describe the E1 Current statistics.

E1 Interval Statistics provide statistical information on a user-specified period of operation during the current NavisCore session. You specify this period in 15-minute intervals, from 1 to 96 intervals (15 minutes to 24 hours). For example, if you specify an interval of 4, NavisCore will display statistics on activity over the past hour of your NavisCore session. Table 3-9 and Table 3-10 list and describe the E1 Interval statistics.

E1 Total Statistics provide statistical information for the sum of all intervals and the current interval. Table 3-11 and Table 3-12 list and describe the E1 Total statistics.

Table 3-7. E1 Current Statistics (RFC 1406)

Statistic	Description
Current Errored Seconds	The number of errored seconds encountered by the E1 interface in the current 15-minute interval.
Current Severely Errored Seconds	The number of p-bit severely errored seconds encountered by the E1 interface in the current 15-minute interval.
Current Severely Errored Framing Seconds	The number of severely errored framing seconds encountered by the E1 interface in the current 15-minute interval.
Current Unavailable Seconds	The number of unavailable seconds encountered by the E1 interface in the current 15-minute interval.
Current Controlled Slip Seconds	The number of controlled slip seconds encountered by the E1 interface in the current 15-minute interval.
Current Path Coding Violations	The number of path coding violations encountered by the E1 interface in the current 15-minute interval.
Current Line Errored Seconds	The number of line errored seconds encountered by the E1 interface in the current 15-minute interval.
Current Bursty Errored Seconds	The number of bursty errored seconds encountered by the E1 interface in the current 15-minute interval.
Current Degraded Minutes	The number of degraded minutes encountered by the E1 interface in the current 15-minute interval.
Current Line Code Violations	The number of line code violations encountered by the E1 interface in the current 15-minute interval.

Table 3-8. E1 Current Statistics (G.826)

Statistic	Description
Errored Seconds Count	A count of one-second intervals with one or more errored blocks or at least one defect within the current 15-minute interval.
Severely Errored Seconds Count	A count of one-second periods with either 30% errored blocks or at least one defect within the current 15-minute interval.
Errored Block Count	The number of block errors encountered by the E1 interface in the current 15-minute interval. Block errors occur in frames that have cyclic redundancy check (CRC) or framing errors.
Background Block Errors Count	A count of block errors that were detected but did not occur as part of a severely errored second within the current 15-minute interval.
Errored Seconds Ratio	A ratio of accumulated errored seconds to total seconds within the current 15-minute interval.
Severely Errored Seconds Ratio	A ratio of accumulated severely errored seconds to total seconds within the current 15-minute interval.
Background Block Errors Ratio	A ratio of background block errors to total received blocks (E1 frames) within the current 15-minute interval.

Table 3-9. E1 Interval Statistics (RFC 1406)

Statistic	Description
Interval Number	The specified interval number.
Interval Errored Seconds	The number of errored seconds encountered by the E1 interface over the user-specified interval.
Interval Severely Errored Seconds	The number of severely errored seconds encountered by the E1 interface over the user-specified interval.
Interval Severely Errored Framing Seconds	The number of severely errored framing seconds encountered by the E1 interface over the user-specified interval.
Interval Unavailable Seconds	The number of unavailable seconds encountered by the E1 interface over the user-specified interval.
Interval Controlled Slip Seconds	The number of controlled slip seconds encountered by the E1 interface over the user-specified interval.
Interval Path Coding Violations	The number of path coding violations encountered by the E1 interface over the user-specified interval.
Interval Line Errored Seconds	The number of line errored seconds encountered by the E1 interface over the user-specified interval.

Table 3-9. E1 Interval Statistics (RFC 1406) (Continued)

Statistic	Description
Interval Bursty Errored Seconds	The number of bursty errored seconds encountered by the E1 interface over the user-specified interval.
Interval Degraded Minutes	The number of degraded minutes encountered by the E1 interface over the user-specified interval.
Interval Line Code Violations	The number of line code violations encountered by the E1 interface over the user-specified interval.

Table 3-10. E1 Interval Statistics (G.826)

Statistic	Description
Interval Number	The specified interval number.
Errored Seconds Count	A count of one-second intervals with one or more errored blocks or at least one defect within the user-specified interval.
Severely Errored Seconds Count	A count of one-second periods with either 30% errored blocks or at least one defect within the user-specified interval.
Errored Block Count	The number of block errors encountered by the E1 interface within the user-specified interval. Block errors occur in frames that have cyclic redundancy check (CRC) or framing errors.
Background Block Errors Count	A count of block errors that were detected but did not occur as part of a severely errored second within the user-specified interval.

Table 3-11. E1 Total Statistics (RFC 1406)

Statistic	Description
Total Errored Seconds	The number of errored seconds encountered by the E1 interface for the sum of all intervals.
Total Severely Errored Seconds	The number of severely errored seconds encountered by the E1 interface for the sum of all intervals.
Total Severely Errored Framing Seconds	The number of severely errored framing seconds encountered by the E1 interface for the sum of all intervals.
Total Unavailable Seconds	The number of unavailable seconds encountered by the E1 interface for the sum of all intervals.
Total Controlled Slip Seconds	The number of controlled slip seconds encountered by the E1 interface for the sum of all intervals.

Table 3-11. E1 Total Statistics (RFC 1406) (Continued)

Statistic	Description
Total Path Coding Violations	The number of path coding violations encountered by the E1 interface for the sum of all intervals.
Total Line Errored Seconds	The number of line errored seconds encountered by the E1 interface for the sum of all intervals.
Total Bursty Errored Seconds	The number of bursty errored seconds encountered by the E1 interface for the sum of all intervals.
Total Degraded Minutes	The number of degraded minutes encountered by the E1 interface for the sum of all intervals.
Total Line Code Violations	The number of line code violations encountered by the E1 interface for the sum of all intervals.

Table 3-12. E1 Total Statistics (G.826)

Statistic	Description
Errored Seconds Count	A count of one-second intervals with one or more errored blocks or at least one defect for the sum of all intervals.
Severely Errored Seconds Count	A count of one-second periods with either 30% errored blocks or at least one defect for the sum of all intervals.
Errored Block Count	The number of block errors encountered by the E1 interface for the sum of all intervals. Block errors occur in frames that have cyclic redundancy check (CRC) or framing errors.
Background Block Errors Count	A count of block errors that were detected but did not occur as part of a severely errored second for the sum of all intervals.

4

Monitoring Physical Port Performance

This chapter describes how to retrieve and view performance-monitoring (PM) data (parameters, thresholds, and statistics) from physical ports on Ascend switches. See the next section "Performance-Monitoring Support on Physical Ports" for information on how to tell whether performance monitoring data is available for a physical port.

NavisCore provides scheduled periodic PM reports for current data based on a configured interval from 1-900 seconds. You specify this interval when you set the polling interval for performance statistics (see "Setting the Polling Interval for Performance Statistics" on page 4-3).

The PM function enables you to create a report for the current day or previous one or two days. You can view the total performance statistics for a day or for a specified interval.

For a complete discussion of performance monitoring, see the *American National Standard for Telecommunications - Digital Hierarchy – Layer 1 In-Service Digital Transmission Performance Monitoring Specification (ANSI T1.231-1993)*.

Performance-Monitoring Support on Physical Ports

You need to verify which physical ports provide PM data. To verify that a particular physical port supports PM data, access PM data as described in "Viewing Performance-Monitoring Data" on page 4-4. If the PM Thresholds and PM Statistics buttons are either grayed out or not visible, the physical port does not support PM data.

Examples of IOMs and BIO cards with physical ports that provide PM data include:

- GX 550 BIO cards
- CBX 500 ATM OC-n/STM-n
- B-STDX ATM IWU
- B-STDX ATM CS
- DS3/E3 (except for 1-port ATM DS3/E3 IOMs)
- Channelized DS3 and DS3-1-0 ports and each of their DS1 channels
- 4-port 24-Channel Fractional T1
- 8-port T1/E1 ATM

Setting Performance-Monitoring Thresholds

You can set PM thresholds to generate traps whenever the thresholds are exceeded. PM statistics are measured in 15-minute and one-day thresholds. These thresholds do not have to be set in order to view PM statistics. See the *NavisCore Physical Interface Configuration Guide* for more information on setting these thresholds.

Setting the Polling Interval for Performance Statistics

The *Polling* function sets the time interval for collecting and retrieving PM statistics during the current session of NavisCore.

To set the time interval for the current session of NavisCore:

1. From the Misc menu, select Ascend Time Intervals ⇒ Set Performance Statistics Time Interval. The Change Performance Statistics Polling dialog box appears (see Figure 4-1), displaying the current time interval.

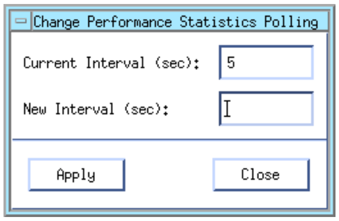


Figure 4-1. Change Performance Statistics Polling Dialog Box

2. Enter a value, in seconds, from 1-900. This polling interval is used for all physical port performance statistics (Current) reports.
3. Choose Apply to save changes.
4. Choose Close to return to the network map.

Viewing Performance-Monitoring Data

You can view performance-monitoring parameters, thresholds, and statistics for either a physical port or a DS1/E1 channel on a channelized DS3/E3 or DS3-1-0 physical port.

For a Physical Port

To view PM data for a physical port:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Double-click on the desired physical port. The View Physical Port Attributes dialog box appears.
4. Choose PM Statistics to display the Performance Monitoring Statistics dialog box.

For a DS1/E1 Channel

To view PM data for a DS1/E1 channel:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Double-click on the desired channelized physical port. The View Physical Port Attributes dialog box appears.
4. Select the DS1/E1 channel and choose Channel Attr. The Channel Attributes dialog box appears (see Figure 3-10 on page 3-12).
5. Choose PM Statistics to display the Performance Monitoring Statistics dialog box.

See the following sections for detailed information on PM data by port type:

- "Viewing OC-n/STM-n Data" on page 4-5.
- "Viewing DS3/E3 Data" on page 4-12.
- "Viewing T1/E1 Data" on page 4-24.
- "Viewing DS1 Channel Data" on page 4-29

> In the PM dialog boxes, a PM parameter, threshold, or statistic field is grayed out whenever it does not apply to a specific physical port.

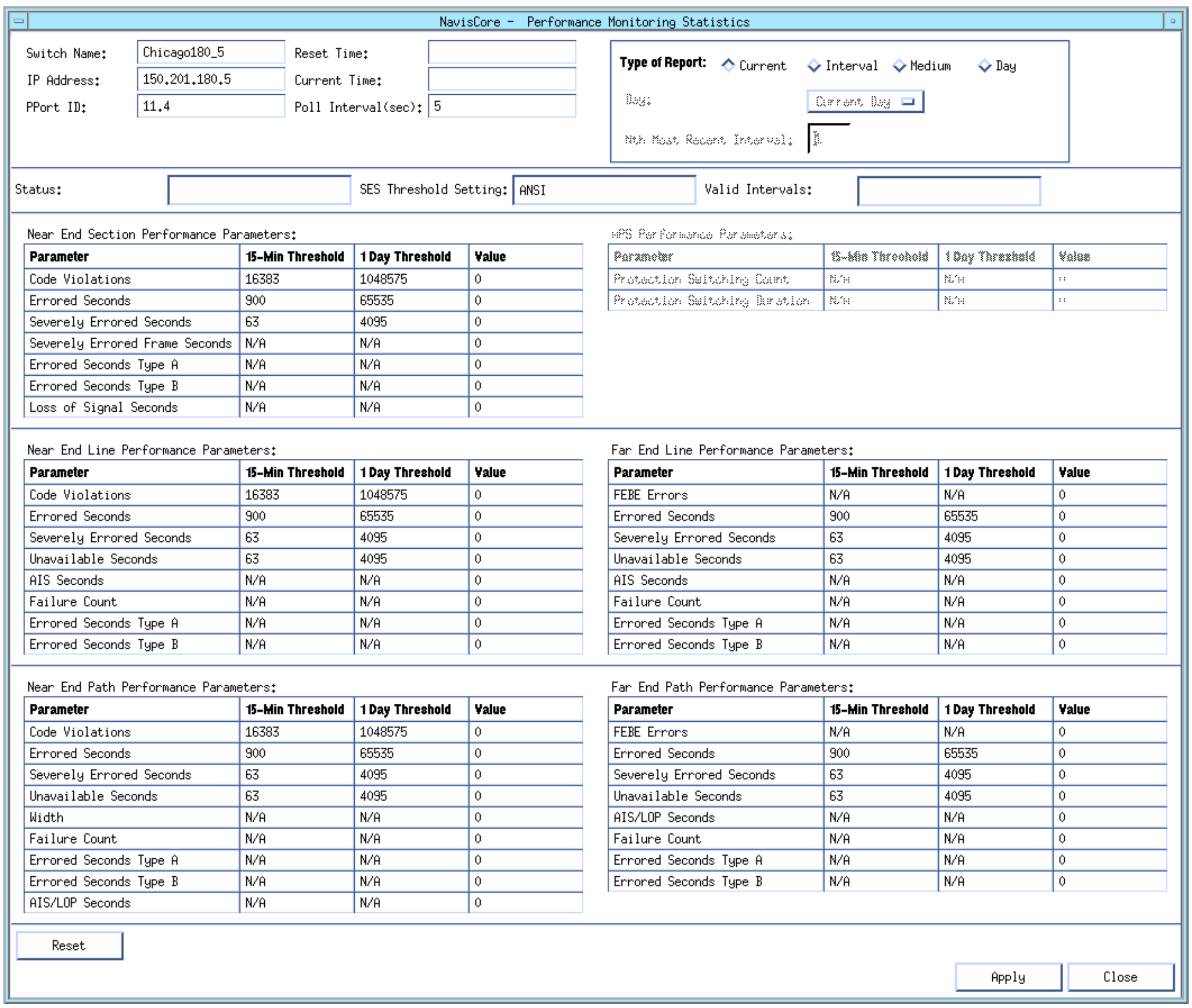
Viewing OC-n/STM-n Data

Before you retrieve OC-n/STM-n PM data, verify that the port supports this data. See "Performance-Monitoring Support on Physical Ports" on page 4-2 for more information.

Examples of cards that support OC-n/STM-n PM data include:

- GX 550 BIO cards
- CBX 500 ATM OC-n/STM-n IOMs
- B-STDX ATM IWU IOMs

The Performance Monitoring Statistics dialog box displays the Current statistics by default. Figure 4-2 shows a sample OC-n/STM-n Performance Monitoring Statistics dialog box.



Near End Section Performance Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
Code Violations	16383	1048575	0
Errored Seconds	900	65535	0
Severely Errored Seconds	63	4095	0
Severely Errored Frame Seconds	N/A	N/A	0
Errored Seconds Type A	N/A	N/A	0
Errored Seconds Type B	N/A	N/A	0
Loss of Signal Seconds	N/A	N/A	0

HPS Performance Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
Protection Switching Count	N/A	N/A	::
Protection Switching Duration	N/A	N/A	::

Near End Line Performance Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
Code Violations	16383	1048575	0
Errored Seconds	900	65535	0
Severely Errored Seconds	63	4095	0
Unavailable Seconds	63	4095	0
AIS Seconds	N/A	N/A	0
Failure Count	N/A	N/A	0
Errored Seconds Type A	N/A	N/A	0
Errored Seconds Type B	N/A	N/A	0

Far End Line Performance Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
FEBE Errors	N/A	N/A	0
Errored Seconds	900	65535	0
Severely Errored Seconds	63	4095	0
Unavailable Seconds	63	4095	0
AIS Seconds	N/A	N/A	0
Failure Count	N/A	N/A	0
Errored Seconds Type A	N/A	N/A	0
Errored Seconds Type B	N/A	N/A	0

Near End Path Performance Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
Code Violations	16383	1048575	0
Errored Seconds	900	65535	0
Severely Errored Seconds	63	4095	0
Unavailable Seconds	63	4095	0
Width	N/A	N/A	0
Failure Count	N/A	N/A	0
Errored Seconds Type A	N/A	N/A	0
Errored Seconds Type B	N/A	N/A	0
AIS/LOP Seconds	N/A	N/A	0

Far End Path Performance Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
FEBE Errors	N/A	N/A	0
Errored Seconds	900	65535	0
Severely Errored Seconds	63	4095	0
Unavailable Seconds	63	4095	0
AIS/LOP Seconds	N/A	N/A	0
Failure Count	N/A	N/A	0
Errored Seconds Type A	N/A	N/A	0
Errored Seconds Type B	N/A	N/A	0

Figure 4-2. Performance Monitoring Statistics Dialog Box (OC-n/STM-n)

To view OC-n/STM-n PM data:

1. Select one of the following reports:

   Current (*default*) — To view real-time current interval data updated at the specified polling frequency. (Figure 4-2 shows a Current statistics example.)

   Interval — To view an interval report based on an interval value from 1-96 you specify in the Nth Most Recent Interval field, with 1 indicating the most recent.

   Medium — To view a dialog box for viewing Sonet/SDH medium statistics. If you choose this option, proceed to "Sonet/SDH Medium Statistics" on page 4-11 for more information.

   Day — To view a report based on the option you specify:
   Current Day (default), Previous Day, or Recent Day (two days ago).

2. If you selected Interval, specify an interval value (from 1 to 96) in the Nth Most Recent Interval field.

   If you selected Day, choose one of the following options: Current Day, Previous Day, or Recent Day.

3. If you chose Current, Interval, or Day, choose Apply to view the data.
4. Choose Reset to update these statistics.
5. Choose Close to exit.

Table 4-1 describes the informational fields at the top of the dialog box, and Table 4-2 describes the performance-monitoring parameters (and associated thresholds and statistics).

Table 4-1. OC-n/STM-n Performance Monitoring Informational Fields

Field	Displays...
Switch Name	The name of the switch you are monitoring.
IP Address	The internal IP address of the switch.
PPort ID	The selected physical port number.
Reset Time	The time statistics were last reset.
Current Time	The current time.
Poll Interval (sec)	The poll interval you set. See "Setting the Polling Interval for Performance Statistics" on page 4-3 for more information.
Status	"Data Valid" if these statistics are valid; displays "Data Invalid" if there is no valid data for the specified time period; displays all zeroes when there is no valid data.

Table 4-1. OC-n/STM-n Performance Monitoring Informational Fields (Continued)

Field	Displays...
SES Threshold Settings	A read-only field that indicates the standard (ANSI or Bellcore) used to calculate the SES values. This is the option you selected when you configured the performance thresholds.
Valid Intervals (*Interval reports only*)	The number of intervals for which data is available.

Table 4-2. OC-n/STM-n Performance Monitoring Statistics

Parameter	Threshold	Description
Near-End Section Performance Parameters		
Code Violations	CV-S	A count of BIP-8 (bit interleaved parity) errors that are detected at the section layer of the incoming signal. Section CV counters increment for each BIP-8 error detected. That is, each BIP-8 can detect up to eight errors per STS-N (synchronous transport signal level N) frame with each error incrementing the CV counter. CVs for the section layer are collected using the BIP-8 in the B1 byte located in the section overhead of STS-1 number 1.
Errored Seconds	ES-S	A count of 1-second intervals in which one or more BIP-8 errors (B1 byte) occurred, one or more severely errored frame (SEF) defects were detected, or one or more loss of signal (LOS) defects were detected.
Severely Errored Seconds	SES-S	A count of 1-second intervals in which x or more BIP-8 errors (B1 byte) occurred, one or more SEF defects were detected, or one or more LOS defects were detected. ***Note:*** *The SES Threshold standard sets the value of x for SES-S. For ANSI standards, this value is 8800; for Bellcore standards, this value is 63; for Sonet, this value is 32.*
Severely Errored Frame Seconds	SESF-S	A count of 1-second intervals in which one or more SEF defects were detected.
Errored Seconds Type A	ESA-S	A count of 1-second intervals in which one BIP-8 (B1 byte) error occurred, and no SEF or LOS condition was detected.
Errored Seconds Type B	ESB-S	A count of 1-second intervals in which two or more BIP-8 (B1 byte) errors occurred, and no SEF or LOS condition was detected.
Loss of Signal Seconds	LOSS-S	A count of 1-second intervals in which one or more loss of signal section conditions were detected.

Table 4-2. OC-n/STM-n Performance Monitoring Statistics (Continued)

Parameter	Threshold	Description
Near-End Line Performance Parameters		
Code Violations	CV-L	A count of the BIP-8 errors detected at the line layer of the incoming signal. The line CV counter increments for each BIP-8 error detected. Each line BIP-8 can detect up to eight errors per STS-1 frame with each error incrementing the CV counter. Line layer CVs are collected using the BIP-8s in the B2 byte located in the line overhead of each STS-1.
Errored Seconds	ES-L	A count of 1-second intervals in which one or more BIP-8 errors (B2 byte) occurred, or one or more alarm indication signal (AIS) defects were detected.
Severely Errored Seconds	SES-L	A count of 1-second intervals in which x or more BIP-8 errors (B2 byte) occurred, or one or more AIS defects were detected. ***Note:*** *The SES Threshold standard sets the value of x for SES-L. For ANSI, this value is 10000; for Bellcore, this value is 124.*
Unavailable Seconds	UAS-L	A count of 1-second intervals for which the SONET/SDH line is unavailable, which begins at the onset of 10 contiguous SES-Ls. The unavailable time period includes the 10 SES-Ls. Once the SONET line is unavailable, it becomes available at the onset of 10 contiguous seconds with no SES-Ls. The 10 seconds with no SES-Ls are excluded from the unavailable time period.
AIS Seconds	AISS-L	A count of 1-second intervals in which one or more AIS defects were detected.
Failure Count	FC-L	A count of near-end line failure (AIS-L) events.
Errored Seconds Type A	ESA-L	A count of 1-second intervals in which one line BIP-8 (B2 byte) error occurred, and no alarm indication signal (AIS-L) defects were detected.
Errored Seconds Type B	ESB-L	A count of 1-second intervals in which two or more BIP-8 (B2 byte) errors occurred, and no alarm indication signal (AIS-L) defects were detected.
Near-End Path Performance Parameters		
Code Violations	CV-P	A count of BIP-8 errors that are detected at the STS path layer of the incoming signal. The CV counters increment for each BIP-8 error detected. CVs for the STS path layer are collected using the BIP-8 in the B3 byte located in the STS path overhead.
Errored Seconds	ES-P	A count of 1-second intervals in which one or more BIP-8 path errors (B3 byte) occurred, one or more AIS-P (alarm indication signal path) defects were detected, or one or more LOP-P (loss of pointer path) defects were detected.

Table 4-2. OC-n/STM-n Performance Monitoring Statistics (Continued)

Parameter	Threshold	Description
Severely Errored Seconds	SES-P	A count of 1-second intervals in which x or more BIP-8 path errors (B3 byte) occurred, one or more LOP-P defects were detected, or one or more AIS-P defects were detected. The default value of x for the STS-1 and STS-3c synchronous payload envelope (SPE) is 2400. ***Note:*** *The SES Threshold standard sets the value of x for SES-P. For ANSI standards, this value is 8800; for Bellcore standards, this value is 63.*
Unavailable Seconds	UAS-P	A count of 1-second intervals for which the SONET STS path is unavailable, which begins at the onset of 10 contiguous severely errored seconds. The unavailable time period includes the 10 SESs. Once the SONET STS-path is unavailable, it becomes available at the onset of 10 contiguous seconds with no SESs. The 10 seconds with no SESs are excluded from the unavailable time period.
Width	N/A	A value that indicates the type of Sonet/SDH path. For Sonet, the assigned types are the STS-Nc SPEs, where N equals one of the following values: 1, 3, 12, 24, and 48. STS-1 is equal to 51.84 Mbps; STS-3 is equal to 51.84*3 or 155.52 Mbps; STS-12 is equal to 622.08 Mbps, and so on. For SDH, the assigned types are the STM-Nc VCs, where N equals one of the following values: 1, 4, and 16.
Failure Count	FC-P	A count of near-end STS path failure (LOP-P or AIS-P) events.
Errored Seconds Type A	ESA-P	A count of 1-second intervals in which one BIP-8 (B3 byte) error occurred, and no AIS-P or LOP defects were detected.
Errored Seconds Type B	ESB-P	A count of 1-second intervals in which two or more BIP-8 (B3 byte) errors occurred, and no AIS-P or LOP defects were detected.
AIS/LOP Seconds	ALS-P	A count of 1-second intervals in which one or more AIS-P or LOP path conditions were detected.
APS Performance Parameters		
Protection Switching Count	PSC	The number of switching events on the working line and the protection line.
Protection Switching Duration	PSD	The length of time, in seconds, when a working line is out of service due to a protection-switching event, or the length of time a protection line is in service due to a protection-switching event.
Far-End Line Performance Parameters		
FEBE errors	CV-LFE	Far-end block line errors.

Table 4-2. OC-n/STM-n Performance Monitoring Statistics (Continued)

Parameter	Threshold	Description
Errored Seconds	ES-LFE	A count of 1-second intervals in which one or more far-end line BIP errors occurred, or one or more RDI-L conditions were detected.
Severely Errored Seconds	SES-LFE	A count of 1-second intervals in which the far-end line BIP errors exceed the SES-LFE threshold, or RDI-L conditions were detected.
Unavailable Seconds	UAS-LFE	A count of far-end line unavailable seconds. Each far-end line unavailable second begins at the onset of 10 consecutive far-end severely errored seconds (SES-LFE seconds).
AIS Seconds	AISS-LFE	A count of 1-second intervals in which one or more RDI-L conditions were detected.
Failure Count	FC-LFE	A number of far-end line failure (RFI-L) events.
Errored Seconds Type A	ESA-LFE	A count of 1-second intervals in which one far-end line BIP error occurred, and no RDI-L conditions were detected.
Errored Seconds Type B	ESB-LFE	A count of 1-second intervals in which two or more far-end line BIP errors occurred, the far-end line BIP errors were less than the SES-LFE threshold x, and no RDI-L conditions were detected.
Far-End Path Performance Parameters		
FEBE errors	CV-PFE	Far-end block path errors.
Errored Seconds	ES-PFE	A count of 1-second intervals in which one or more far-end BIP errors occurred, or one or more RDI-P conditions were detected.
Severely Errored Seconds	SES-PFE	A count of 1-second intervals in which the number of far-end path BIP errors exceed the SES-PFE threshold x, or RDI-P conditions were detected.
Unavailable Seconds	UAS-PFE	A count of far-end path unavailable seconds. A far-end path unavailable second begins at the onset of 10 consecutive far-end severely errored seconds.
AIS/LOP Seconds	ALS-PFE	A count of 1-second intervals in which one or more RDI path conditions were detected.
Failure Count	FC-PFE	A count of far-end STS path failure (RFI-P) events.
Errored Seconds Type A	ESA-PFE	A count of 1-second intervals in which one far-end path BIP error occurred, and no RDI-P condition was detected.
Errored Seconds Type B	ESB-PFE	A count of 1-second intervals in which two or more far-end BIP errors occurred, the far-end path BIP errors were less than the SES-PFE threshold x, and no RDI-P conditions were detected.

Sonet/SDH Medium Statistics

When you choose the Medium report type on the Performance Monitoring Statistics (OC-n/STM-n) dialog box (Figure 4-2 on page 4-5), the Sonet/SDH Medium Statistics dialog box appears (see Figure 4-3).

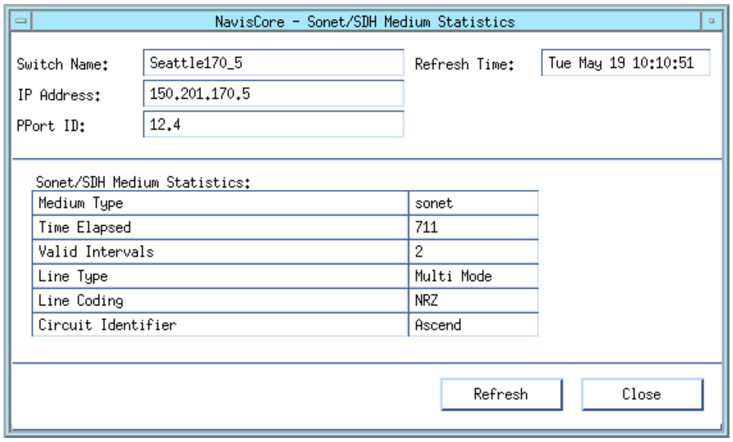


Figure 4-3. Sonet/SDH Medium Statistics Dialog Box

Table 4-3 describes the fields on the Sonet/SDH Medium Statistics dialog box.

Table 4-3. Sonet/SDH Medium Statistics Fields

Statistic	Description
Medium Type	Whether a SONET or an SDH signal is used across this interface. Values may be "Sonet" or "SDH."
Time Elapsed	The number of seconds, including partial seconds, that have elapsed since the beginning of the current error-measurement period.
Valid Intervals	The number of previous intervals for which valid data has been stored.
Line Type	The line type for the interface. Values are: Short Single Mode, Long Single Mode, MultiMode, Coax, UTP, Other.
Line Coding	The line coding for this interface. Values are: Other, B3ZA, CMI, NRZ, RZ.
Circuit Identifier	The transmission vendor's company name or ID, which you can use for troubleshooting.

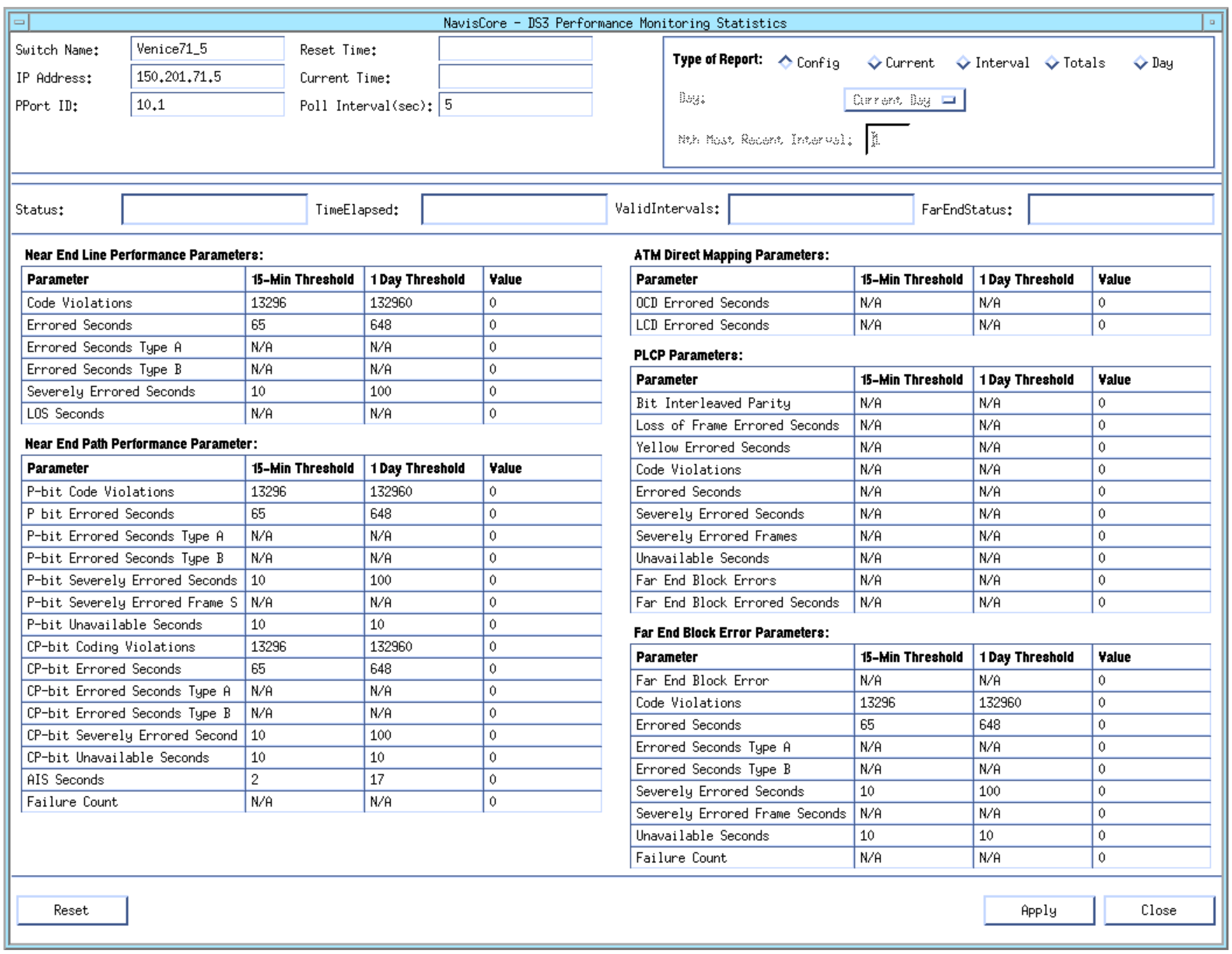
Viewing DS3/E3 Data

Before you retrieve DS3/E3 PM data, verify that the port supports this data. See "Performance-Monitoring Support on Physical Ports" on page 4-2 for more information.

Examples of IOMs that support DS3/E3 PM data include:

- ATM CS IOMs
- Most DS3/E3 IOMs (except for 1-port ATM DS3/E3 IOMs)
- Channelized DS3 and DS3-1-0 IOMs

The DS3/E3 Performance Monitoring Statistics dialog box displays the Current statistics by default. Figure 4-4 shows a sample DS3/E3 Performance Monitoring Statistics dialog box.



NavisCore - DS3 Performance Monitoring Statistics

Switch Name: Venice71_5
IP Address: 150.201.71.5
PPort ID: 10.1
Reset Time:
Current Time:
Poll Interval(sec): 5

Type of Report: Config Current Interval Totals Day
Day: Current Day
Nth Most Recent Interval: 1

Status: TimeElapsed: ValidIntervals: FarEndStatus:

Near End Line Performance Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
Code Violations	13296	132960	0
Errored Seconds	65	648	0
Errored Seconds Type A	N/A	N/A	0
Errored Seconds Type B	N/A	N/A	0
Severely Errored Seconds	10	100	0
LOS Seconds	N/A	N/A	0

Near End Path Performance Parameter:

Parameter	15-Min Threshold	1 Day Threshold	Value
P-bit Code Violations	13296	132960	0
P bit Errored Seconds	65	648	0
P-bit Errored Seconds Type A	N/A	N/A	0
P-bit Errored Seconds Type B	N/A	N/A	0
P-bit Severely Errored Seconds	10	100	0
P-bit Severely Errored Frame S	N/A	N/A	0
P-bit Unavailable Seconds	10	10	0
CP-bit Coding Violations	13296	132960	0
CP-bit Errored Seconds	65	648	0
CP-bit Errored Seconds Type A	N/A	N/A	0
CP-bit Errored Seconds Type B	N/A	N/A	0
CP-bit Severely Errored Second	10	100	0
CP-bit Unavailable Seconds	10	10	0
AIS Seconds	2	17	0
Failure Count	N/A	N/A	0

ATM Direct Mapping Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
OCD Errored Seconds	N/A	N/A	0
LCD Errored Seconds	N/A	N/A	0

PLCP Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
Bit Interleaved Parity	N/A	N/A	0
Loss of Frame Errored Seconds	N/A	N/A	0
Yellow Errored Seconds	N/A	N/A	0
Code Violations	N/A	N/A	0
Errored Seconds	N/A	N/A	0
Severely Errored Seconds	N/A	N/A	0
Severely Errored Frames	N/A	N/A	0
Unavailable Seconds	N/A	N/A	0
Far End Block Errors	N/A	N/A	0
Far End Block Errored Seconds	N/A	N/A	0

Far End Block Error Parameters:

Parameter	15-Min Threshold	1 Day Threshold	Value
Far End Block Error	N/A	N/A	0
Code Violations	13296	132960	0
Errored Seconds	65	648	0
Errored Seconds Type A	N/A	N/A	0
Errored Seconds Type B	N/A	N/A	0
Severely Errored Seconds	10	100	0
Severely Errored Frame Seconds	N/A	N/A	0
Unavailable Seconds	10	10	0
Failure Count	N/A	N/A	0

Reset Apply Close

Figure 4-4. Performance Monitoring Statistics Dialog Box (DS3/E3)

> If you are monitoring performance statistics for a physical port on a channelized DS3/E3 or DS3-1-0 IOM, the ATM Direct Mapping Parameters, PLCP Parameters, and Far-End Block Error Parameters are grayed out.

To view DS3/E3 PM data:

1. Select one of the following reports:

   Config — To view the current configuration information. See "Viewing DS3/E3 Statistics Configuration" on page 4-18 for more information.

   Current (*default*) — To view real-time current 15-minute interval counters, updated at the specified polling frequency. (Figure 4-4 shows a Current statistics example.)

   Interval — To view counters for a previous 15-minute interval, based on the interval value from 1-96 you specify in the Nth Most Recent Interval field, with 1 indicating the most recent.

   Totals — To view the rolling total count of all the counters in the last 24-hour period. Effectively, it is the total count of the past 96 15-minute interval counters. These are updated at 15-minute intervals, starting from the current interval.

   Day — To view a report based on the option you specify: Current Day (default), Previous Day, or Recent Day (two days ago). The Day report contains a snapshot of each counter's totals for a 24-hour period (per ANSI T1.231). These reports are updated every 24 hours by totaling all 15 intervals from the previous 24 hours.

2. If you selected Interval, specify an interval value (from 1 to 96) in the Nth Most Recent Interval field.

   If you selected Day, choose one of the following options: Current Day, Previous Day, or Recent Day.

3. Choose Apply to view the data.
4. Choose Reset to update these statistics.
5. Choose Close to exit.

Table 4-4 describes the informational fields at the top of the dialog box, and Table 4-5 describes the performance-monitoring parameters (and associated thresholds and statistics).

Table 4-4. DS3/E3 Performance Monitoring Informational Fields

Field	Displays...
Switch Name	The name of the switch you are monitoring.
IP Address	The internal IP address of the switch.
PPort ID	The selected physical port number.
Reset Time	The time statistics were last reset.
Current Time	The current time.
Poll Interval (sec)	The poll interval you set. See “Setting the Polling Interval for Performance Statistics” on page 4-3 for more information.
Status	“Data Valid” if these statistics are valid; displays “Data Invalid” if there is no valid data for the specified time period; displays all zeroes when there is no valid data.
Time Elapsed	The time elapsed in the current time period.
Valid Intervals (*Interval reports only*)	The number of intervals for which data is available.
Far End Status	Indicates any problems with remote/far-end equipment that could affect the accuracy of this data.

Table 4-5. DS3/E3 Performance Monitoring Statistics

Parameter	Threshold	Description
Near-End Line Performance Parameters		
Code Violations	CV-L	A count of both BPVs and EXZs occurring over the accumulation period.
Errored Seconds	ES-L	A count of 1-second intervals containing one or more BPVs, one or more EXZs, or one or more LOS defects.
Errored Seconds Type A	ESA-L	A count of 1-second intervals containing one BPV or EXZ and no LOS defects.
Error Seconds Type B	ESB-L	A count of 1-second intervals containing more than one, but less than x BPVs plus EXZs, and no LOS defects.
Severely Errored Seconds	SES-L	A count of 1-second intervals with more than x BPVs plus EXZs, or one or more LOS defects.

Table 4-5. DS3/E3 Performance Monitoring Statistics (Continued)

Parameter	Threshold	Description
LOS Seconds	LOS-L	A count of 1-second intervals containing one or more LOS defects.
Near-End Path Performance Parameters		
P-bit Code Violations	CVP-P	A count of error events occurring in the accumulation period.
P-bit Errored Seconds	ESP-P	A count of 1-second intervals containing the occurrence of one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects.
P-bit Errored Seconds Type A	ESAP-P	The count of 1-second intervals containing exactly one P-bit parity error and no SEF or AIS defects.
P-bit Errored Seconds Type B	ESBP-P	The count of 1-second intervals containing more than one, but less than x P-bit parity errors, and no SEF or AIS defects.
P-bit Severely Errored Seconds	SESP-P	A count of 1-second intervals containing more than x P-bit parity errors, one or more SEF defects, or one or more AIS defects.
P-bit Severely Errored Frames	SEFP-P	A count of 1-second intervals containing one or more SEF defects or one or more AIS defects.
P-bit Unavailable Seconds	UASP-P	A count of 1-second intervals for which the DS3 path is unavailable. The DS3/E3 path becomes unavailable at the onset of 10 contiguous SESP-Ps.
CP-bit Coding Violations	CVCP-P	A count of error events occurring in the accumulation period.
CP-bit Errored Seconds	ESCP-P	A count of 1-second intervals containing one or more M-frames with the three FEBE bits not all set to ONE or one or more far-end SEF/AIS defects.
CP-bit Errored Seconds Type A	ESCPA-P	The count of 1-second intervals containing one CP-bit parity error and no SEF or AIS defects.
CP-bit Errored Seconds Type B	ESCPB-P	The count of 1-second intervals containing more than one, but less than x CVCP-Ps, and no SEF or AIS defects.
CP-bit Severely Errored Seconds	SESCPP	A count of 1-second intervals containing more than x CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
CP-bit Unavailable Seconds	UASCP-P	A count of 1-second intervals for which the DS3 path is unavailable. The DS3 path becomes unavailable at the onset of 10 contiguous SESCP-Ps.
AIS Seconds	AISS-P	A count of 1-second intervals containing one or more AIS defects.

Table 4-5. DS3/E3 Performance Monitoring Statistics (Continued)

Parameter	Threshold	Description
Failure Count	FC-P	A count of the number of occurrences of near-end path failure events, with the failure event defined as follows: • A near-end path failure event begins when either a LOF or AIS failure is declared. • A near-end path failure event ends when both LOF and AIS failures are cleared.
ATM Direct-Mapping Parameters		
OCD Errored Seconds	OCD	Count of 1-second intervals containing Out of Cell Delineation (OCD).
LCD Errored Seconds	LCD	Count of 1-second intervals containing Loss of Cell Delineation (LCD).
PLCP Parameters		
Bit Interleaved Parity	PLCP-BIP	The number of PLCP-BIP errors in the current 15-minute interval.
Loss of Frame Errored Seconds	PLCP-LOF	The number of PLCP-LOF errors in the current 15-minute interval.
Yellow Errored Seconds	PLCP-YEL	The number of PLCP-YEL errors in the current 15-minute interval.
Code Violations	PLCP-CV	The number of PLCP-CV errors in the current 15-minute interval.
Errored Seconds	PLCP-ES	The number of PLCP-ES errors in the current 15-minute interval.
Severely Errored Seconds	PLCP-SES	The number of PLCP-SES errors in the current 15-minute interval.
Severely Errored Frames	PLCP-SEF	The number of PLCP-SEF errors in the current 15-minute interval.
Unavailable Seconds	PLCP-UAS	The number of PLCP-UAS errors in the current 15-minute interval.
Far End Block Errors	PLCP-FEBE	The number of PLCP-FEBE errors in the current 15-minute interval.
Far End Block Errored Seconds	PLCP-FEBE-ES	The number of PLCP-FEBE errors in the current 15-minute interval.
Far-End Block Error Parameters		
Far End Block Error	FEBE-P	The number of FEBE errors in the current 15-minute interval.

Table 4-5. DS3/E3 Performance Monitoring Statistics (Continued)

Parameter	Threshold	Description
Code Violations	CVCP-P	The number of FEBE-CV errors in the current 15-minute interval.
Errored Seconds	ESCP-P	The number of FEBE-ES errors in the current 15-minute interval.
Errored Seconds Type A	ESACP-P	The number of FEBE-ESA errors in the current 15-minute interval.
Errored Seconds Type B	ESBCP-P	The number of FEBE-ESB errors in the current 15-minute interval.
Severely Errored Seconds	SESCP-P	The number of FEBE-SES errors in the current 15-minute interval.
Severely Errored Frame Seconds	SEFSCP-P	The number of FEBE-SEFS errors in the current 15-minute interval.
Unavailable Seconds	UASCP-P	The number of FEBE-UAS errors in the current 15-minute interval.
Failure Count	FCCP-P	The number of FEBE-FC errors in the current 15-minute interval.

Viewing DS3/E3 Statistics Configuration

The DS3/E3 Statistics Configuration dialog box appears when you select Config from the DS3/E3 Performance Monitoring Statistics dialog box (Figure 4-4 on page 4-12). Figure 4-5 shows the DS3/E3 Statistics Configuration dialog box.

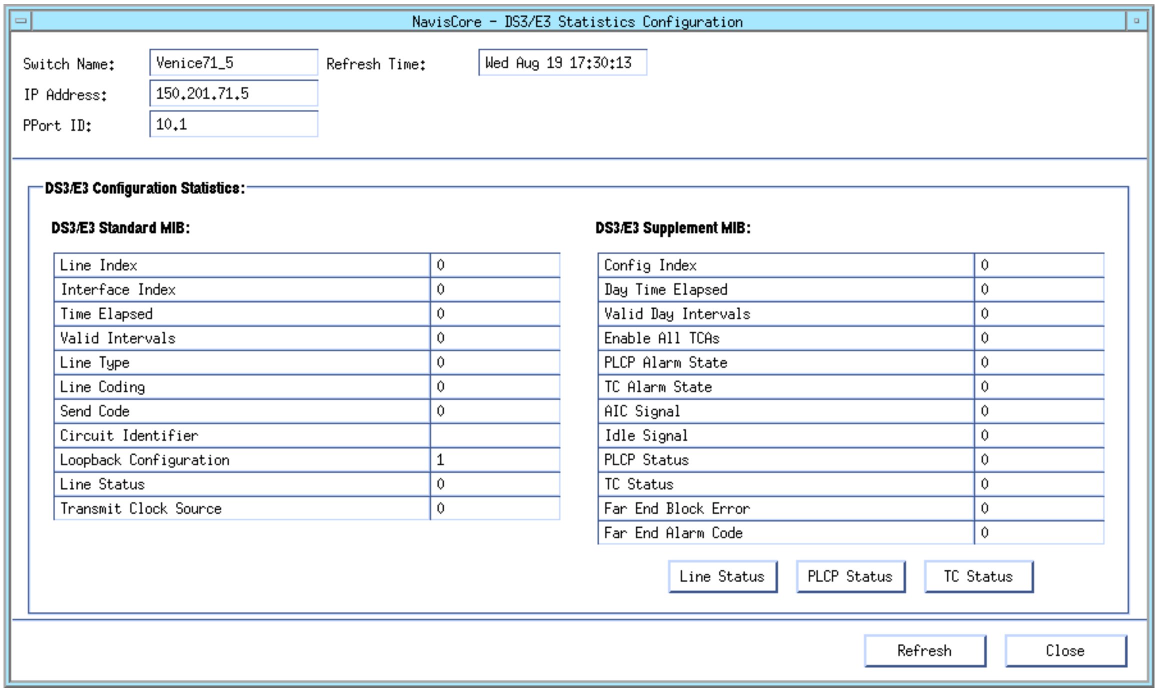


Figure 4-5. DS3/E3 Statistics Configuration Dialog Box

Use the Refresh button to update the DS3/E3 statistics configuration. See Table 4-6 for descriptions of the statistics configuration parameters.

Table 4-6. DS3/E3 Statistics Configuration Parameters

Parameter	Description
DS3/E3 Standard MIB	
Line Index	The DS3 or E3 interface index identifier on a managed device.
Interface Index	The value of ifIndex from the Interface table of MIB II.
Time Elapsed	The number of seconds elapsed since the beginning of the current error measurement period.
Valid Intervals	The number of previous near-end intervals for which valid data was collected.

Table 4-6. DS3/E3 Statistics Configuration Parameters (Continued)

Parameter	Description
Line Type	The DS3 C-bit or E3 applications implementing this interface. Possible values include: 1 – Other (undefined) DS3 interface 2 – M23 (defined in ANSI T1.107-1988) 3 – SYNTRAN (defined in ANSI T1.107-1988) 4 – C-bit Parity (defined in ANSI T1.107a-1989) 5 – Clear Channel (defined in ANSI T1.102-1987) 6 – Other (undefined) E3 interface 7 – Framed (defined in CCITT G.751) 8 – PLCP (defined in ETSI T/NA (91) 18) Note that the Clear Channel value means that C-bits are not used except for sending and receiving AIS.
Line Coding	The type of Zero Code Suppression on this interface. Possible values include: 1 – Other (undefined) from of Zero Code Suppression 2 – B3ZS (for DS3 links) 3 – HDB3 (for E3 links) Note that B3ZS and HDB3 refer to the use of specified patterns of normal bits and bipolar violations which are used to replace sequences of zero bits of a specified length.
Send Code	The type of code the device sends across the DS3/E3 interface. Possible values include: 1 – Send no code (that is, send looped or normal data) 2 – Send line code (that is, send a request for a line loopback) 3 – Send payload code (that is, send a request for a payload loopback) 4 – Send reset code (that is, send a loopback deactivation request) 5 – Send DS1 loop code (that is, request to loopback to a particular DS1/E1 within a DS3/E3 frame 6 – Send test pattern (that is, send a test pattern)
Circuit Identifier	The transmission vendor's circuit identifier (Ascend).
Loopback Configuration	The loopback configuration of the DS3/E3 interface. Possible values include: 1 – No loop (that is, not in the loopback state) 2 – Payload loop (that is, the received signal is looped through the device) 3 – Line loop (that is, the received signal does not go through this interface but is looped back out) 4 – Other (undefined) loopback

Table 4-6. DS3/E3 Statistics Configuration Parameters (Continued)

Parameter	Description
Line Status	The line status of the interface. This field is a bit map that represents a sum and, therefore, can represent multiple failures and a loopback. The various bit positions (and their MIB variables and descriptions) include: 1 – No alarm (dsx3NoAlarm) 2 – Receiving indication of a yellow/remote alarm (dsx3RcvRAIFailure) 4 – Transmitting yellow/remote alarm indication (dsx3XmitRAIAlarm) 8 – Receiving AIS failure state (dsx3RcvAIS) 16 – Transmitting AIS (dsx3XmitAIS) 32 – Receiving LOF failure state (dsx3LOF) 64 – Receiving LOS failure state (dsx3LOS) 128 – Looping the received signal (dsx3LoopbackState) 256 – Receiving a test pattern (dsx3RcvTestCode) 512 – Undefined line status (dsx3OtherFailure)
Transmit Clock Source	The source of the transmit clock. Possible values include: 1 – Loop timing 2 – Local timing 3 – Through timing
DS3/E3 Supplement MIB	
Config Index	The DS3 or E3 interface index identifier on a managed device.
Day Time Elapsed	The number of seconds that have elapsed since the beginning of the measurement period.
Valid Day Intervals	The number of previous intervals for which valid data was collected. This value is 3 unless the interface was brought online within the last three days, in which case the value is equal to the number of complete one-day intervals since the interface has been online.
Enable All TCAs	Indicates whether Threshold Crossing Alerts (TCAs) can be sent across the interface. Possible values include: 1 – True (TCAs can be sent) 2 – False (TCAs cannot be sent)
PLCP Alarm State	The current PLCP alarm state.
TC Alarm State	The current TC alarm state.
AIC Signal	The type of application (C-bit or M23/SYNTRAN) based on the AIC signal received by the DS3 interface. Possible values include: 1 – C-bit 2 – M23/SYNTRAN

Table 4-6. DS3/E3 Statistics Configuration Parameters (Continued)

Parameter	Description
Idle Signal	Indicates whether an Idle signal is being received. Possible values include: 1 – No idle 2 – Receiving idle
PLCP Status	The current PLCP status. Possible values include: 1 – No status 2 – Receiving LOF 4 – Receiving YEL 8 – Receiving AIS 16 – Receiving FEBE
TC Status	The current TC status. Possible values include: 1 – No status 2 – Receiving OCD 4 – Receiving LCD
Far End Block Error	Indicates whether a FEBE is being received. Possible values include: 1 – No FEBE 2 – Receiving FEBE
Far End Alarm Code	Indicates whether a FEAC is being received. Possible values include: 1 – No FEAC 2 – Equipment failure 4 – LOS 8 – Out of frame 16 – AIS received. 32 – Idle received 64 – Non-service affecting equipment failure 128 – Common equipment failure 256 – Loopback received 512 – DS1 service affecting equipment failure 1024 – DS1 non-service affecting equipment failure 2048 – Single DS1 LOS 4096 – Multiple DS1 LOS

Use the following buttons to display additional configuration and status information:

Line Status — View the line status of the associated interface.

PLCP Status — View the PLCP status of the associated interface.

TC Status — View the TC status of the associated interface.

Line Status

The DS3/E3 Configuration Line Status dialog box appears (see Figure 4-6) when you use the Line Status button.

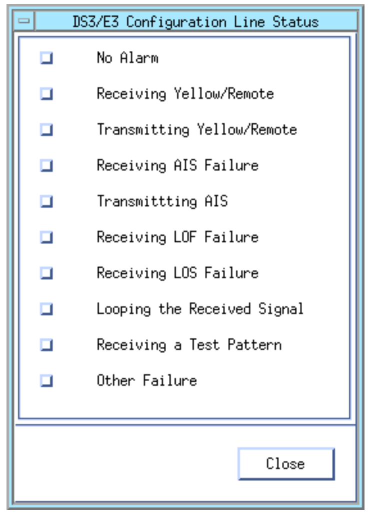


Figure 4-6. DS3/E3 Configuration Line Status Dialog Box

Table 4-7 describes the possible error conditions.

Table 4-7. DS3/E3 Line Status Conditions

Status	Description
No Alarm	No alarm present.
Receiving Yellow/Remote	Far-end SEF/AIS detected.
Transmitting Yellow/Remote	Transmitting a yellow/remote alarm.
Receiving AIS Failure	Near-end SEF/AIS detected.
Transmitting AIS	Transmitting an alarm indication signal.
Receiving LOF Failure	Receiving loss of frame condition.
Receiving LOS Failure	Receiving loss of signal. No signal detected.
Looping the Received Signal	Loopback enabled/disabled.
Receiving a Test Pattern	FEAC (Far end alarm code) signal received.
Other Failure	Any failures not covered by the above conditions.

PLCP Status

The DS3/E3 Configuration PLCP Status dialog box appears (see Figure 4-7) when you use the PLCP Status button.

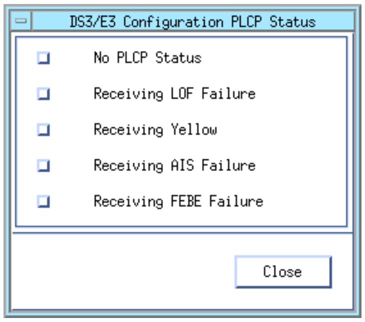


Figure 4-7. DS3/E3 Configuration PLCP Status Dialog Box

Table 4-8 describes the possible error conditions.

Table 4-8. DS3/E3 PLCP Status Conditions

Status	Description
No PLCP Status	No PLCP status condition is detected.
Receiving LOF Failure	Receiving notification of a loss of frame failure.
Receiving Yellow	Receiving a yellow alarm.
Receiving AIS Failure	Receiving notification of an AIS failure.
Receiving FEBE Failure	Receiving notification of a FEBE failure.

TC Status

The DS3/E3 Configuration TC Status dialog box appears (see Figure 4-8) when you use the TC Status button.

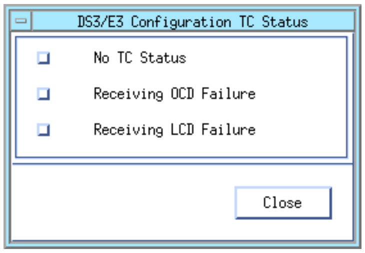


Figure 4-8. DS3/E3 Configuration TC Status Dialog Box

Table 4-9 describes the possible error conditions.

Table 4-9. DS3/E3 TC Status Conditions

Status	Description
No TC Status	No TC status condition is detected.
Receiving OCD Failure	Receiving notification of an OCD failure.
Receiving LCD Failure	Receiving notification of an LCD failure.

Viewing T1/E1 Data

Before you retrieve T1/E1 PM data, verify that the port supports this data. See "Performance-Monitoring Support on Physical Ports" on page 4-2 for more information.

Examples of IOMs that support T1/E1 PM data include:

- 4-port 24-channel Fractional T1 IOMs
- 8-port T1/E1 ATM IOMs

The T1/E1 Performance Monitoring Statistics dialog box displays the Current statistics by default. Figure 4-9 shows a sample T1/E1 Performance Monitoring Statistics dialog box.

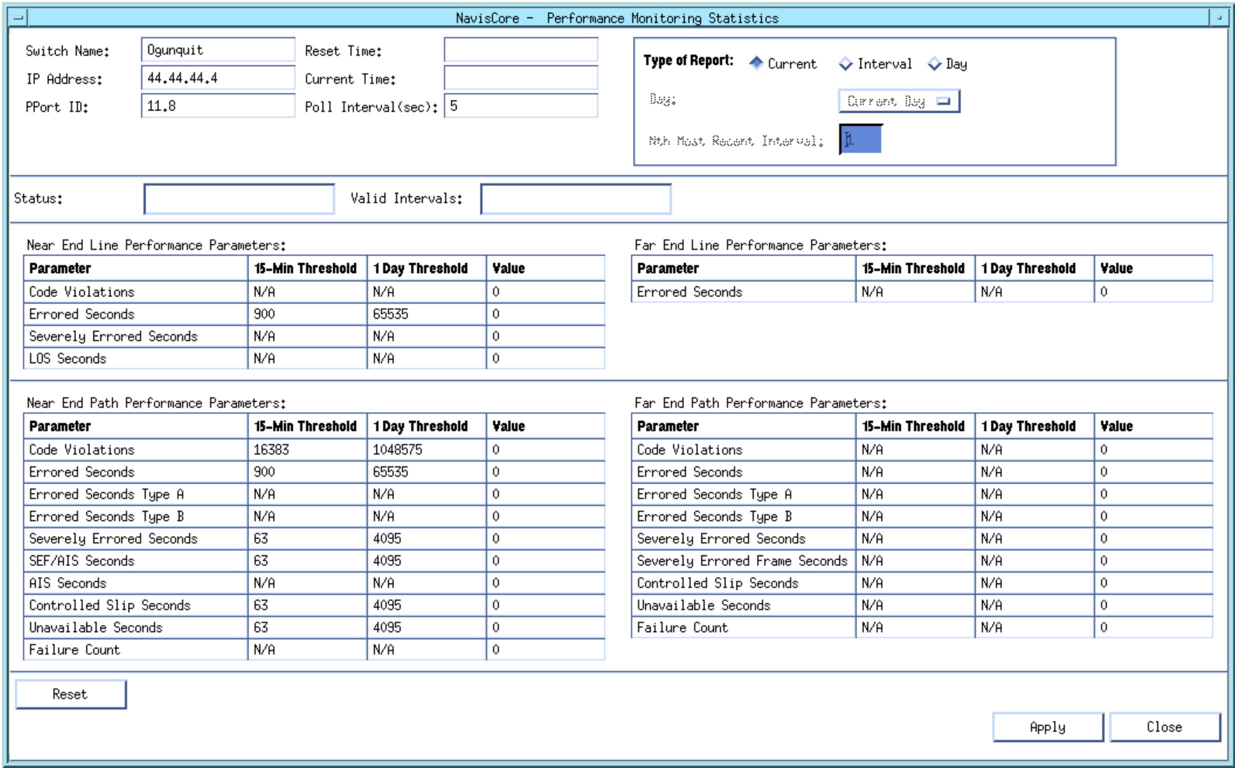


Figure 4-9. Performance Monitoring Statistics Dialog Box (T1/E1)

To view T1/E1 PM data:

1. Select one of the following reports:

   Current (*default*) — To view real-time current interval data updated at the specified polling frequency. (Figure 4-9 shows a Current statistics example.)

   Interval — To view an interval report based on the interval value from 1-96 you specify in the Nth Most Recent Interval field, with 1 indicating the most recent.

   Day — To view a Totals report from one of the three options: Current Day (default), Previous Day, or Recent Day (two days ago).

2. If you selected Interval, specify an interval value (from 1 to 96) in the Nth Most Recent Interval field.

   If you selected Day, choose one of the following options: Current Day, Previous Day, or Recent Day.

3. Choose Apply to view the data.
4. Choose Reset to update these statistics.
5. Chose Close to exit.

Table 4-10 describes the informational fields at the top of the dialog box, and Table 4-11 describes performance-monitoring parameters (and associated thresholds and statistics).

Table 4-10. T1/E1 Performance Monitoring Informational Fields

Field	Displays...
Switch Name	The name of the switch you are monitoring.
IP Address	The internal IP address of the switch.
PPort ID	The selected physical port.
Reset Time	The time statistics were last reset.
Current Time	The current time.
Poll Interval (sec)	The poll interval you set. See "Setting the Polling Interval for Performance Statistics" on page 4-3 for more information.
Status	"Data Valid" if these statistics are valid; displays "Data Invalid" if there is no valid data for the specified time period; displays all zeroes when there is no valid data.
Valid Intervals (*Interval reports only*)	The number of intervals for which data is available.

Table 4-11. T1/E1 Performance Monitoring Statistics

Parameter	Threshold	Description
Near-End Line Performance Parameters		
Code Violations	CV-L	A count of both BPVs (bipolar violations) and EXZs (excessive zeros) occurring over the accumulation period. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded from the count.
Errored Seconds	ES-L	A count of 1-second intervals with one or more BPVs, one or more EXZs, or one or more LOS (loss of signal) defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded.
Severely Errored Seconds	SES-L	A count of 1-second intervals with 1544 or more BPVs plus EXZs, or one or more LOS defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded.
LOS Seconds	LOSS-L	A count of 1-second intervals with one or more LOS defects.

Table 4-11. T1/E1 Performance Monitoring Statistics (Continued)

Parameter	Threshold	Description
Near-End Path Performance Parameters		
Code Violations	CV-P	A count of frame synchronization bit errors (FE) in the SF (Superframe) format, or a count of cyclic redundancy check (CRC)-6 errors in the ESF (Extended Superframe) format occurring during the accumulation period.
Errored Seconds	ES-P	In the case of DS1 ESF, a count of 1-second intervals containing one or more CRC-6 errors, one or more CS events, or one or more SEF or AIS defects. In the case of DS1 SF, this parameter is a count of 1-second intervals containing one or more FE events, one or more SEF or AIS defects, or one or more CS events.
Errored Seconds Type A	ESA-P	This parameter applies to DS1 ESF paths only. A count of 1-second intervals with exactly one CRC-6 error and no SEF or AIS defects.
Errored Seconds Type B	ESB-P	This parameter applies to DS1 ESF paths only. A count of 1-second intervals with no less than 2, and not more than 319 CRC-6 errors, no SEF defects, and no AIS defects.
Severely Errored Seconds	SES-P	This parameter applies to both SF and ESF frame formats of DS1. In the case of ESF, it is a count of 1-second intervals with 320 or more CRC-6 errors, or one or more SEF or AIS defects. In the case of SF, it is a count of 1-second intervals with eight or more FE events (if F_t and F_8 bits are measured) or four or more FE events (if F_t bits only are measured), or an SEF or AIS defect.
SEF/AIS Seconds	SAS-P	A count of 1-second intervals containing one or more SEF defects or one or more AIS defects.
AIS Seconds	AISS-P	A count of 1-second intervals containing one or more AIS defects.
Controlled Slip Seconds	CSS-P	A count of 1-second intervals containing one or more controlled slips. Counts of controlled slips can be made accurately only in the path-terminating network element of the DS1 signal, where the controlled slip takes place.
Unavailable Seconds	UAS-P	A count of 1-second intervals for which the DS1 path is unavailable. The DS1 path becomes unavailable at the onset of 10 contiguous SESs. The 10 SESs are included in the unavailable time period. Once it is unavailable, the DS1 path becomes available at the onset of 10 contiguous seconds with no SESs. The 10 seconds with no SESs are excluded from the unavailable time period.
Failure Count	FC-P	Count of Loss of Frame or AIS events within the accumulation period.

Table 4-11. T1/E1 Performance Monitoring Statistics (Continued)

Parameter	Threshold	Description
Far-End Line Performance Parameters		
Errored Seconds	ES-LFE	A count of one second PRM intervals containing an LV=1.
Far-End Path Performance Parameters		
Code Violations	CV-PFE	A count of the number of far end CVs occurring during the accumulation period.
Errored Seconds	ES-PFE	A count of one second PRM intervals containing a G1, G2, G3, G4, G5, or G6 or SE or SL=1, or an RAI signal.
Errored Seconds Type A	ESA-PFE	A count of one second PRM intervals containing a G1=1 and SE=0.
Errored Seconds Type B	ESB-PFE	A count of one second PRM intervals containing a G2, G3, G4, or G5=1, and SE=0.
Severely Errored Seconds	SES-PFE	A count of one second PRM intervals containing a G6 or SE=1, or an RAI signal.
Severely Errored Frame Seconds	SEFS-PFE	A count of one second PRM intervals containing an SE=1.
Controlled Slip Seconds	CSS-PFE	A count of one second PRM intervals containing an SL=1.
Unavailable Seconds	UAS-PFE	A count of 1-second intervals for which the DS1 path is unavailable.
Failure Count	FC-PFE	Count of RAI (yellow alarm) events within the accumulation period.

Viewing DS1 Channel Data

For DS1 channels on channelized DS3 and DS3-1-0 IOMs, you can display performance statistics on the channel's signal quality. The DS1 Channel Performance Monitoring Statistics dialog box displays the Current statistics by default. Figure 4-10 shows a sample DS1 Channel Performance Monitoring Statistics dialog box.

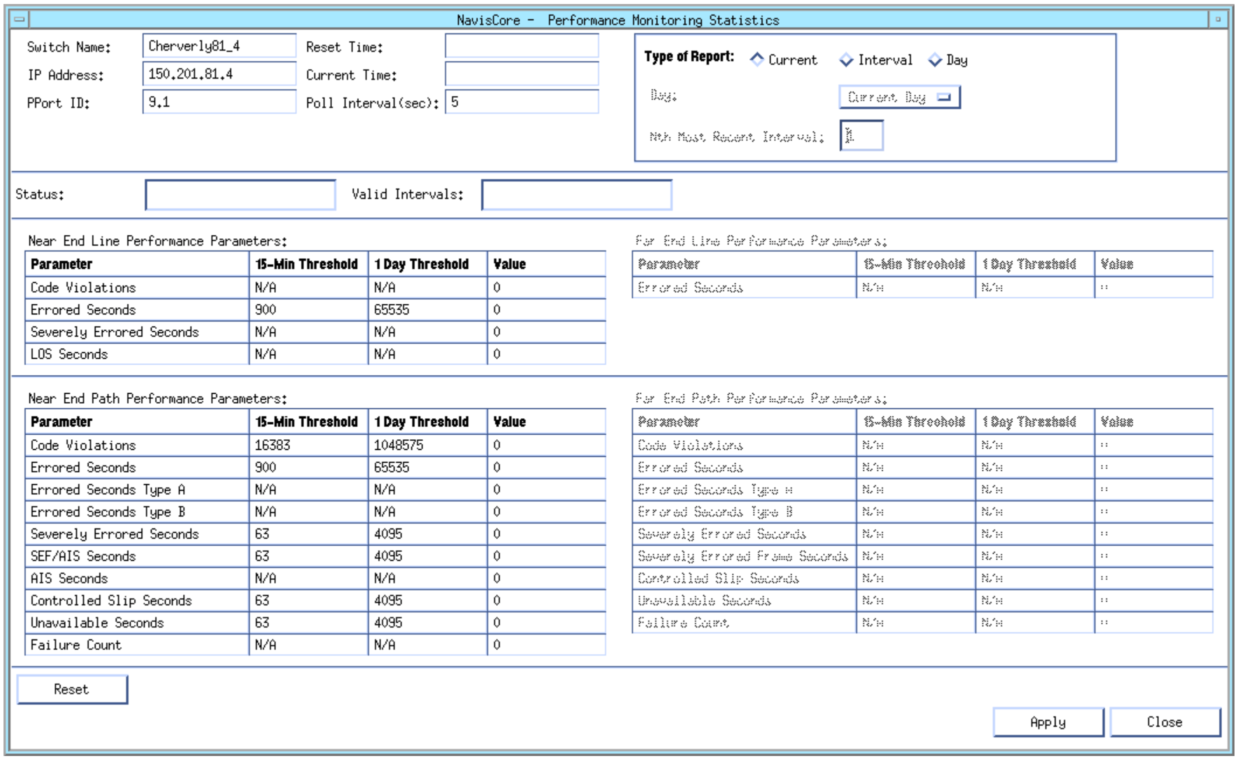


Figure 4-10. Performance Monitoring Statistics Dialog Box (DS1 Channel)

▶ For channels on channelized DS3/E3 and DS3-1-0 IOMs, the Far-End Line Performance Parameters and the Far-End Path Performance Parameters are grayed out.

To view DS1 channel PM data:

1. Select one of the following reports:

   Current (*default*) — To view real-time current interval data updated at the specified polling frequency. (Figure 4-10 shows a Current statistics example.)

   Interval — To view an interval report based on the interval value from 1-96 you specify in the Nth Most Recent Interval field, with 1 indicating the most recent.

   Day — To view a Totals report from one of the three options: Current Day (default), Previous Day, or Recent Day (two days ago).

2. If you selected Interval, specify an interval value (from 1 to 96) in the Nth Most Recent Interval field.

   If you selected Day, choose one of the following options: Current Day, Previous Day, or Recent Day.

3. Choose Apply to view the data.
4. Choose Reset to update these statistics.
5. Chose Close to exit.

Table 4-12 describes the informational fields at the top of the dialog box, and Table 4-13 describes performance-monitoring parameters (and associated thresholds and statistics).

Table 4-12. DS1 Channel Performance Monitoring Informational Fields

Field	Displays...
Switch Name	The name of the switch you are monitoring.
IP Address	The internal IP address of the switch.
PPort ID	The selected physical port.
Reset Time	The time statistics were last reset.
Current Time	The current time.
Poll Interval (sec)	The poll interval you set. See "Setting the Polling Interval for Performance Statistics" on page 4-3 for more information.
Status	"Data Valid" if these statistics are valid; displays "Data Invalid" if there is no valid data for the specified time period; displays all zeroes when there is no valid data.
Valid Intervals (*Interval reports only*)	The number of intervals for which data is available.

Table 4-13. DS1 Channel Performance Monitoring Statistics Fields

Parameter	Threshold	Description
Near-End Line Performance Parameters		
Code Violations	CV-L	A count of both BPVs (bipolar violations) and EXZs (excessive zeros) occurring over the accumulation period. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded from the count.
Errored Seconds	ES-L	A count of 1-second intervals with one or more BPVs, one or more EXZs, or one or more LOS (loss of signal) defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded.
Severely Errored Seconds	SES-L	A count of 1-second intervals with 1544 or more BPVs plus EXZs, or one or more LOS defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded.
LOS Seconds	LOSS-L	A count of 1-second intervals with one or more LOS defects.
Near-End Path Performance Parameters		
Code Violations	CV-P	A count of frame synchronization bit errors (FE) in the SF (Superframe) format, or a count of cyclic redundancy check (CRC)-6 errors in the ESF (Extended Superframe) format occurring during the accumulation period.
Errored Seconds	ES-P	In the case of DS1 ESF, a count of 1-second intervals containing one or more CRC-6 errors, one or more CS events, or one or more SEF or AIS defects. In the case of DS1 SF, this parameter is a count of 1-second intervals containing one or more FE events, one or more SEF or AIS defects, or one or more CS events.
Errored Seconds Type A	ESA-P	This parameter applies to DS1 ESF paths only. A count of 1-second intervals with exactly one CRC-6 error and no SEF or AIS defects.
Errored Seconds Type B	ESB-P	This parameter applies to DS1 ESF paths only. A count of 1-second intervals with no less than 2, and not more than 319 CRC-6 errors, no SEF defects, and no AIS defects.
Severely Errored Seconds	SES-P	This parameter applies to both SF and ESF frame formats of DS1. In the case of ESF, it is a count of 1-second intervals with 320 or more CRC-6 errors, or one or more SEF or AIS defects. In the case of SF, it is a count of 1-second intervals with eight or more FE events (if F_t and F_8 bits are measured) or four or more FE events (if F_t bits only are measured), or an SEF or AIS defect.

Table 4-13. DS1 Channel Performance Monitoring Statistics Fields (Continued)

Parameter	Threshold	Description
SEF/AIS Seconds	SAS-P	A count of 1-second intervals containing one or more SEF defects or one or more AIS defects.
AIS Seconds	AISS-P	A count of 1-second intervals containing one or more AIS defects.
Controlled Slip Seconds	CSS-P	A count of 1-second intervals containing one or more controlled slips. Counts of controlled slips can be made accurately only in the path-terminating network element of the DS1 signal, where the controlled slip takes place.
Unavailable Seconds	UAS-P	A count of 1-second intervals for which the DS1 path is unavailable. The DS1 path becomes unavailable at the onset of 10 contiguous SESs. The 10 SESs are included in the unavailable time period. Once it is unavailable, the DS1 path becomes available at the onset of 10 contiguous seconds with no SESs. The 10 seconds with no SESs are excluded from the unavailable time period.
Failure Count	FC-P	Count of Loss of Frame or AIS events within the accumulation period.

5

Testing Modules, Ports, and Channels

This chapter describes how to test hardware modules (including processor, I/O, and BIO modules), physical ports, and channels. NavisCore diagnostic and loopback tests help you to detect potential failures or problems with you switch hardware.

► All DS0, DS1, and DS3 loopback tests are latching loopback tests.

You can obtain node-level diagnostic information for a selected switch, as well as physical and logical port-level diagnostic information. NavisCore provides the following diagnostic programs:

Background Diagnostics — Run continuously in background to monitor the switches for potential failures or problems. Background diagnostics execute automatically and do not interfere with switch operations.

Foreground Diagnostics — Provide current status for all active switches and enable you to test physical and logical port integrity.

Accessing Diagnostics

When you access diagnostic tests through the Monitor menu, you do not have to log on to run them. The Administer menu allows you to access processor module, IOM, BIO card, and physical port diagnostic tests from the switch back panel without logging on. To proceed beyond the Switch Back Panel dialog box (e.g., double-click on a physical port), you must log on.

However, you must log on to change the admin status (up to down) of IOMs, physical ports, logical ports, and channels. You must disable (admin down) the network object before you run foreground diagnostic tests and loopbacks.

Background Diagnostics

This section describes the problems that background diagnostics detect and how to view background diagnostic information in NavisCore.

Problems Background Diagnostics Detect

Background diagnostics can alert you to the following types of problems that can occur on an active switch:

- Corruption of different data structures
- Corruption of code space

Background diagnostics provide real-time status information, categorized by fatal and non-fatal errors.

Fatal errors — Includes those conditions that cause the switch to fail and reboot and may also include user-initiated outages, such as a requested reboot, synchronization, or software download. Document and report any non-user initiated fatal errors to the Ascend Technical Assistance Center (TAC) by calling 1-800-DIAL-WAN (1-800-342-5926).

> This guide does not describe how to resolve a fatal error.

Non-fatal errors — Includes those conditions whereby system resources are strained by some event, either internally or externally. Non-fatal errors are also reported to the NMS via trap alarms and viewed through the Ascend Events browser. See Chapter 15, "Managing Traps" for information about trap alarms.

Viewing Background Diagnostics

The Background Diagnostics dialog box displays status information for an active switch. The procedure for viewing background diagnostics differs slightly, depending on the type of switch.

Viewing Background Diagnostics for GX 550 Switches

To run background diagnostics for a GX 550 switch:

1. On the network map, select the switch object for which you want to view diagnostic information.

2. Perform one of the following actions:

   – From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.

   – From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.

3. Select the BIO module or GX 550 node processor (NP).

> When you select a BIO module on a GX 550 switch, click on the top of the module where the slot number appears. You cannot run diagnostics if you click on any of the sub-cards.

4. Choose Diag. The Select Card Diagnostics dialog box appears. The appearance of the dialog box varies, depending on whether you selected an NP or a BIO module.

   – For NP modules, select either Active or Standby (see Figure 5-1). The diagnostics type defaults to background and cannot be selected.

   – For BIO modules, select Background (see Figure 5-2).

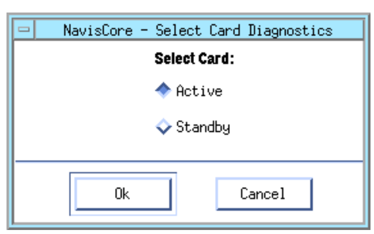


Figure 5-1. Select Card Diagnostics Dialog Box (GX 550 NPs)

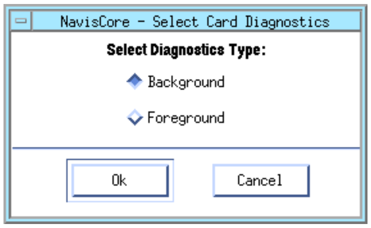


Figure 5-2. Select Card Diagnostics Dialog Box (GX 550 BIO Modules)

5. Choose OK. The Background Diagnostics dialog box appears (see Figure 5-3).

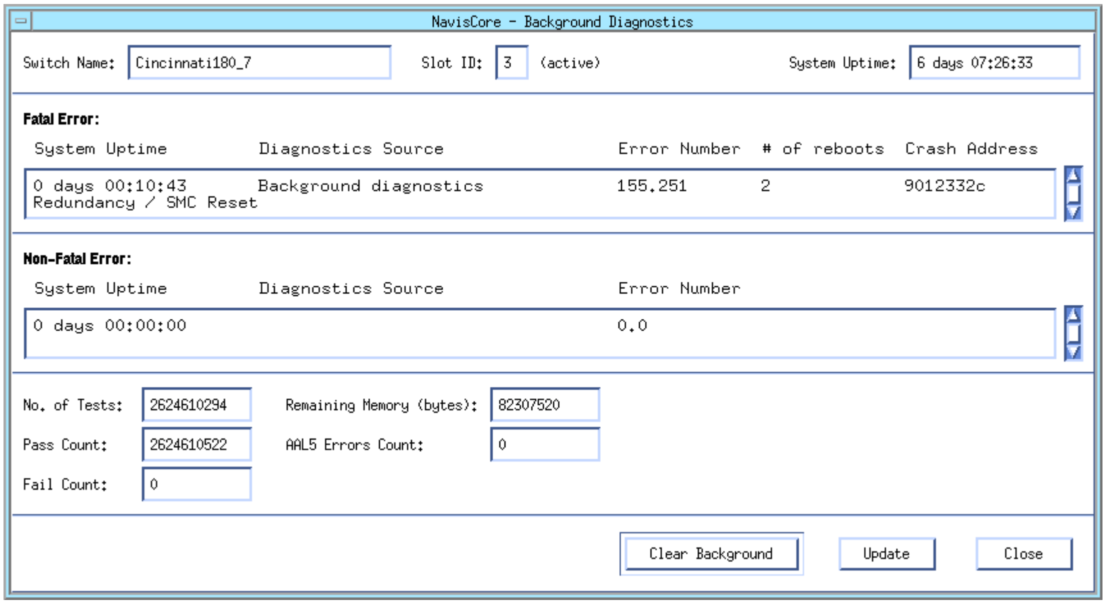


Figure 5-3. Background Diagnostics Dialog Box

The Background Diagnostics dialog box displays both fatal and non-fatal errors. Table 5-1 on page 5-6 describes the Background Diagnostics dialog box fields.

Optionally, you can choose the Clear Background button or the Update button to rerun the background diagnostic test.

6. Choose Close to return to the Switch Back Panel dialog box.

If it appears that a BIO module or NP is failing, consider switching to a redundant module or NP if one is available. See "Switching to a Redundant Unit" on page 5-7 for more information.

Viewing Background Diagnostics for B-STDX 8000/9000 and CBX 500 Switches

To run background diagnostics for a B-STDX 8000/9000 switch or a CBX 500 switch:

1. On the network map, select the switch object for which you want to view diagnostic information.

2. Perform one of the following actions:

– From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.

– From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.

3. Select the IOM, SP, or CP for which you want to obtain background diagnostic information.

4. Choose Diag.

The Select Card Diagnostics dialog box appears (see Figure 5-4). If you are viewing diagnostics for an SP or a CP, you can select either the active or standby card. For the diagnostics type, you can select Background only.

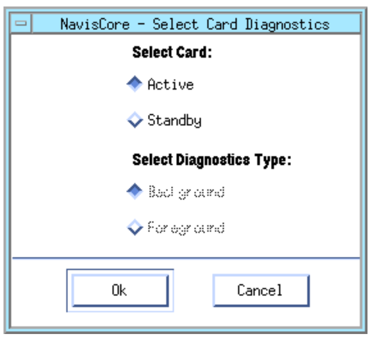


Figure 5-4. Select Card Diagnostics Dialog Box (B-STDX and CBX)

5. Choose OK. The Background Diagnostics dialog box appears (see Figure 5-3 on page 5-4).

The Background Diagnostics dialog box displays both fatal and non-fatal errors. Table 5-1 on page 5-6 describes the Background Diagnostics dialog box fields.

Optionally, you can choose the Clear Background button or the Update button to rerun the background diagnostic test.

6. Choose Close to return to the network map.

Background Diagnostics Fields

Table 5-1 describes the fields on the Background Diagnostics dialog box.

Table 5-1. Background Diagnostics Fields

Field	Displays...
Switch Name	The name of the switch for which you are viewing diagnostic information.
Slot ID	The I/O module slot number and specifies whether the diagnostics are for the active or standby card.
System Uptime	The amount of time that the module has been active since its last reboot. For example, if this field displays “7 days 22:31:01,” then 7 days, 22 hours, 31 minutes and 1 second have elapsed since the module’s last reboot.
Fatal Error	The following information about the conditions that caused the switch to fail and reboot. *System Uptime* – The System Uptime value at the time the error occurred. For example, if the System Uptime value was 0 days, 22 hours, 24 minutes, and 30 seconds when the error occurred, this field displays: 0 days 22:24:30. *Diagnostics Source* – The source from which NavisCore collected the error information. Options include: system level (NP/SP/CP), card level, redundancy manager, BD Heap (Frame-heap memory), power-on diagnostics, background diagnostics, Fault, and Device driver level. *Error Number* – The error number containing the major and minor error codes in the format of X.Y (X being the major code and Y being the minor code). See Table B-1 on page B-2 for a list of background diagnostics error codes. For error codes from other sources, contact the TAC. *# of Reboots* – The number of times this switch experienced a reboot condition since the last logged fatal error. If this value is greater than three (3), information displayed in the Background Diagnostics dialog box is outdated. ***Note**: Although the # of Reboots counter increments with each reboot, there are instances where the hardware reboots or resets but the screen information does not change. These instances include: the switch powers off and on; the hardware resets (for example, when you use the latch to reset a CBX 500 module); and the CP, SP, or NP continuously polls the modules for status. If a module does not respond, the CP, SP, or NP resets this module.* *Crash Address* – A crash address for certain types of fatal error conditions. The Ascend CS TAC uses this address for debugging purposes. If the background diagnostics indicate a crash address, make a note of the address and contact the TAC. This guide does not describe how to resolve a fatal error.
Non-Fatal Error	Information about those conditions that strain system resources. This information is the same as that described for a fatal error. See the “Fatal Error” field descriptions.
No. of Tests	The number of tests that have occurred on the selected switch.
Pass count	The number of background diagnostic tests that have passed without error.

Table 5-1. Background Diagnostics Fields (Continued)

Field	Displays...
Fail count	The number of tests that produced an error condition. The failed diagnostic(s) is displayed in the fatal or non-fatal area.
Remaining Memory (bytes)	The amount of available heap memory on the selected module.
AAL5 Errors Count (ATM modules only)	A count of ATM Adaptation Layer 5 (AAL5) errors.
Total Invalid ATM Cells Received (CBX ATM modules only)	The total number of invalid VPI/VCI ATM cells received on this module.
Last Received Invalid VPI/VCI (CBX ATM modules only)	The last invalid VPI/VCI cell received on a per-module basis. In this case, invalid cell traffic is defined as cells that are received on a physical port that does not have a corresponding PVC or SVC mapped to the received cell's VPI or VCI.

Switching to a Redundant Unit

If background diagnostics indicate that an IOM, NP (and accompanying switching fabric and timing module), SP, or CP is failing, consider switching to a redundant unit if one is available. You should also switch to a redundant unit before removing an active unit.

B-STDX 8000/9000 and CBX 500

To switch to a redundant unit on a B-STDX 8000/9000 or CBX 500 switch:

1. Select the switch object on the network map.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the redundant IOM, redundant SP (CBX 500), or redundant CP (B-STDX).
4. Select Actions ⇒ Switch to Redundant Unit.
5. Choose Go.
6. Choose OK to confirm your action.

GX 550

To switch to a redundant unit on a GX switch:

1. Select the switch object on the network map.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the redundant NP.
4. Select Actions ⇒ Switch to Redundant Unit.
5. Select Node Processor, Switching Fabric, or Timing Module, as appropriate.
6. Choose Go.
7. Choose OK to confirm your action.

> On GX 550 switches, only NPs support redundancy.

Foreground Diagnostics

You can run foreground diagnostics on an IOM, a physical port, a channel, or a logical port. You cannot run foreground diagnostics on a CP, SP, or NP.

You use foreground diagnostics to test for problems indicated by background diagnostics (non-fatal errors) or to collect statistical data. You can also run foreground diagnostics to verify that new equipment functions properly.

Problems Foreground Diagnostics Detect

Foreground diagnostics enable you to:

- Verify whether an IOM, physical port, channel, or logical port is transmitting data properly at the physical link level
- Isolate the cause of a transmission stall error (error codes 27.1 and 27.2)

Foreground diagnostics provide more information about non-fatal error conditions. The following foreground diagnostic tests are available depending on the component you are testing:

Internal — Tests the IOM hardware only. You can use this test on all IOMs. This checks the internal hardware of a specific physical port.

> The channelized DS3 IOM requires an external loopback connector to pass internal foreground diagnostic tests. All other IOMs (including the DS3-1-0 IOM) do not require an external loopback connector to pass internal foreground diagnostic tests.

External — Performs an external test that directs signals back toward the source along a communications path to test the ability to send and receive data. This test requires an external loopback connector, which you install on the physical port being tested.

Loopback — Tests the ability of physical ports, channels, and logical ports to send and receive data. See “Running Loopback Tests” on page 5-16 for more information.

Before You Begin

Before you run these tests, make sure you:

- Set the applicable IOM, physical port, channel, or logical port admin status to *Down*. You must be logged on to perform this task.
- When applicable, review the Transmit (Xmit) Clock Source on the Show Physical Port Attributes dialog box and make sure it is not set to Loop-Timed. The foreground diagnostic tests also require the physical port to provide clocking (set to Internal). If you need to change the Transmit (Xmit) Clock Source, you must log on to the NMS.

> It is recommended that you run foreground diagnostics on a physical port only if it appears red on the switch back panel.
>
> Do not run foreground diagnostics at the physical port level if individual DS1 or DS0 channels are malfunctioning, but other channels are functioning properly. Instead, run foreground diagnostics on the specific channels.

Review the following steps to modify the admin status and clock source selection for an IOM, a physical port, a channel (such as DS1 channel on a channelized DS3 IOM), or a logical port.

Changing an IOM's Admin Status

1. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
2. Select the IOM.
3. Choose Attrs. The Set Card Attributes dialog box appears.
4. Change admin status to *Down*.
5. Choose OK to save your changes.

Changing a Physical Port's Admin Status

1. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
2. Double-click on the port you need to disable. The Set Physical Port Attributes dialog box appears.
3. Set the port admin status to *Down*.
4. If the clock source selection on the Set Physical Port Attributes dialog box is set to Loop-Timed, change this field temporarily to *Internal*.
5. Choose Apply and then choose OK to save your changes.

Changing a Channel’s Admin Status

1. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
2. Double-click on the specific channelized DS3 or DS3-1-0 port you need to disable. The Set Physical Port Attributes dialog box appears.
3. Double-click on the channel that you need to disable. The Set Channel Attributes dialog box appears.
4. Set the chan admin status to *Down* (this temporarily sets the Transmit Clock Source to Internal).
5. Choose Apply. The system displays a confirmation message.
6. Choose OK to save your changes.
7. Choose Close.

Changing a Logical Port’s Admin Status

1. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
2. Double-click on the physical port associated with the logical port you need to disable. The Set Physical Port Attributes dialog box appears.
3. Perform one of the following actions:
   – For physical ports that are not channelized, choose Logical Port. The Set Logical Ports dialog box appears.
   – For physical ports that are channelized (such as channelized DS3 and DS3-1-0 ports), double-click on the channel associated with the logical port. The Set Channel Attributes dialog box appears. Then choose Logical Port. The Set Logical Ports dialog box appears.
4. Select a logical port and choose Modify to change the logical port settings. The Modify Logical Port Type dialog box appears.
5. Choose Ok. The Modify Logical Port dialog box appears.
6. Change the admin status to *Down*.
7. Choose OK to save your changes.

Viewing Foreground Diagnostics

You can display foreground diagnostics for IOMs, physical ports, channels on channelized IOMs, and logical ports. You cannot view foreground diagnostics for a CP, SP, or NP.

Testing an IOM

To test an IOM:

1. On the network map, select the switch object from which you want to obtain IOM diagnostic information.
2. Perform one of the following actions:
   – From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
   – From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Select the IOM you want to test.

> When you select a BIO module on a GX 550 switch, click on the top of the module where the slot number appears. You cannot run diagnostics if you click on any of the subcards.

4. Choose Diag. The Select Card Diagnostic dialog box appears.
   – For a GX 550 switch, choose Foreground. The Perform Foreground Diagnostic Test dialog box appears.
   – For all other switches, select either Active or Standby and then choose Foreground. The Perform Foreground Diagnostic Test dialog box appears.
5. Select the type of test:

   Internal – Performs an internal loopback test that checks the module's hardware only. You can use this test on all IOMs.

   External – Performs a test that directs signals back toward the source along a communications path to test the ability of the physical port(s) on the IOM to send and receive data. This test requires an external loopback connector, which you install on the physical ports you are testing. You can also install the external loopback connector on an external device such as a DSU or router.
6. Choose Start Test. The results appear in the Test Results window.
7. Set the IOM's admin status to Up.
8. When you are finished running foreground diagnostics, reset the IOM's admin status to *Up*.

Testing a Physical Port

To test a physical port:

1. On the network map, select the switch object from which you want to obtain physical port diagnostic information.
2. Perform one of the following actions:
   - From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
   - From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Select the physical port you want to test.
4. Choose Diag. The Perform Foreground Diagnostic Test dialog box appears.
5. Select the type of test:

   Internal – Performs an internal loopback test that checks the module's hardware only. You can use this test on all IOMs.

   External – Performs a test that directs signals back toward the source along a communications path to test the ability of the physical port to send and receive data. This test requires an external loopback connector, which you install on the physical port you are testing. You can also install the external loopback connector on an external device such as a DSU or router.

   Loopbacks – Various loopback tests are listed, depending on the type of physical port selected. See "Running Loopback Tests" on page 5-16 for more information. For some physical ports, such as Fast Ethernet physical ports, loopback tests are not available.
6. Choose Start Test. The results appear in the Test Results window.
7. When you are finished running foreground diagnostics, reset the port's admin status to *Up*.

Testing a Channel

To test a channel:

1. On the network map, select the switch object from which you want to obtain channel diagnostic information.
2. Perform one of the following actions:
   – From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
   – From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears.
3. Select the physical port on a channelized module.
4. Choose Attrs from the Switch Back Panel dialog box. The Physical Port Attributes dialog box appears.
5. Click once on the specific channel and choose Diagnose. The Perform Foreground Channel Diagnostic Test dialog box appears (see Figure 5-5).

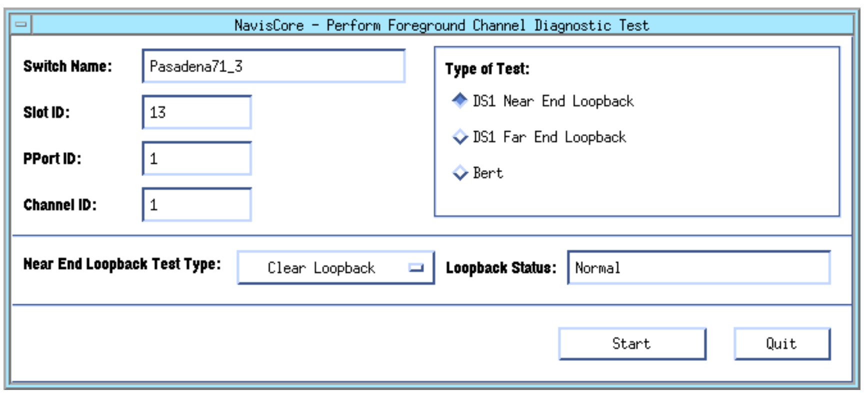


Figure 5-5. Perform Foreground Channel Diagnostic Test Dialog Box

6. Select one of the following channel diagnostic tests:
   - DS1 Near End Loopback
   - DS1 Far End Loopback
   - Bert

   For more information on these tests, see "Running Loopback Tests" on page 5-16.
7. Choose Start.
8. When you are finished running foreground diagnostics, reset the chan admin status to *Up*.

Testing a Logical Port

To test a logical port:

1. On the network map, select the switch object from which you want to obtain logical port diagnostic information.

2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.

3. Select the physical port that is used by the logical port you want to test.

4. Choose Attrs from the Switch Back Panel dialog box. The Set Physical Port Attributes dialog box appears.

5. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.

6. Choose Options ⇒ Diagnostics.

7. Choose View. The Perform Foreground Diagnostic Test dialog box appears.

8. Select the type of test:

   Internal – Performs an internal loopback test that checks the hardware of the IOM used by the logical port only. You can use this test on all modules.

   External – Performs an external test that enables you to direct signals back toward the source along a communications path to test the port's ability to send and receive data. This test requires an external loopback connector, which you install on the physical port that is used by the logical port you are testing. You can also install the external loopback connector on an external device such as a DSU or router.

9. Choose Start Test. The results appear in the Test Results window.

10. Choose Close to return to the network map.

11. When you are finished running foreground diagnostics, reset the logical port's admin status to *Up*.

Running Loopback Tests

This section describes how to initiate and monitor loopback diagnostic functions. Loopback testing can be used on physical ports and channels as a means of verifying data integrity and for general troubleshooting purposes. You can run a loopback test online or offline, depending on the loopback type.

Ascend switches support the following hardware loopback tests:

Physical Port Loopbacks — For each IOM type, the Ascend switches support a variety of physical line loopbacks. At a minimum, each physical port type supports basic internal and external loopback tests. Additional types of loopbacks specific to the individual media type are also available for each of the physical ports. The physical port loopback tests must be run *offline* (you must set the physical port's admin status to *Down*).

Channel Loopbacks — You can test the transmission path of a specific DS1 channel for channelized DS3 and DS3-1-0 IOMs. You can also test the transmission path of a specific DS0 channel for DS3-1-0, channelized T1, 4-port ISDN PRI, and 4-port DSX modules.

All DS0, DS1, and DS3 loopback tests are latching loopback tests.

Do not attempt to modify physical port or channel while they are undergoing loopback testing.

T1/E1 Loopback Tests

The type of loopback tests that are available for the T1 and E1 modules (including 10-port DSX modules) depends on the physical port's configured circuit type (Superframe or Extended Superframe) and the specific module on which it resides.

Table 5-2 describes the types of T1/E1 loopback tests.

> Some T1/E1 modules do not support all of the tests described in Table 5-2.

Table 5-2. T1/E1 Loopback Tests

Test	Circuit Type	Description
Metallic (ATM IOMs Only)	Both Superframe & Extended Superframe	Performs a cell loopback test that checks the IOM and IOA component of the module.
Payload loopback	Both Superframe & Extended Superframe	Similar to a near-end line loopback in that the incoming signal from the device attached to the physical port is looped back. However, with the payload loopback, the loopback is made after the physical port framer device such that the signal from the outside traverses the framer device and is then looped back. This (in some regards) is a more comprehensive test than the near-end line loopback, because when you verify the integrity of the signal passing through the loopback, the integrity of the switch framer is also verified. The physical port remains in this state until you stop the test.
Line	Both Superframe & Extended Superframe	A near-end loopback where the external data stream is looped back prior to clock recovery and framing. The external device therefore receives its own clocked signal back.
Framed inband line	Both Superframe & Extended Superframe	A static loopback command mode where the far-end equipment is commanded into line loopback via the previously selected in-band line loopback code CSU or Network Interface (NI). Using this command, framed loopback control commands are sent to the far end. • Choose Start Test to send loop-up code for 5 seconds; the far-end equipment responds by initiating a line loopback. • Choose Stop Test to send loop-down code for 5 seconds; the far-end equipment responds by terminating the line loopback mode.

Table 5-2. T1/E1 Loopback Tests (Continued)

Test	Circuit Type	Description
Unframed inband line	Both Superframe & Extended Superframe	A static loopback command mode where the far-end equipment is commanded into line loopback via the previously selected in-band line loopback code CSU or NI. Using this command, unframed loopback control commands are sent to the far end. • Choose Start Test to send loop-up code for 5 seconds; the far-end equipment responds by initiating a line loopback. • Choose Stop Test to send loop-down code for 5 seconds; the far-end equipment responds by terminating the line loopback mode.
ESF FDL line (ANSI)	Extended Superframe	A static loopback command mode where the far-end equipment is commanded into line loopback via the T1 ESF out-of-band FDL loopback control commands. This option is only available if you configure the physical port with Extended Superframe ESF and FDL *enabled*. • Choose Start Test to send loop-up code; the far-end equipment responds by initiating a line loopback. • Choose Stop Test to send loop-down code; the far-end equipment terminates the line loopback mode.
ESF FDL payload (ANSI)	Extended Superframe	A static loopback command mode where the far-end equipment is commanded into payload loopback via the T1 ESF out-of-band FDL loopback control commands. This option is only available if you configure the physical port with Extended Superframe ESF and FDL *enabled*. • Choose Start Test to send loop-up code; the far-end equipment responds by initiating a payload loopback. • Choose Stop Test to send loop-down code; the far-end equipment terminates the payload loopback mode.

Network Response to a T1/E1 Loopback

The following list outlines the network's response to a T1/E1 line or payload loopback.

> Ascend only supports a CSU type loopback code from the network.

1. The T1/E1 port receives a line or payload T1/E1 loop activate code from the network.
2. The framer detects the loop code and interrupts the processor.
3. The processor responds by activating the desired loopback.
4. The polling mechanism detects an active loopback status and the port operating status is changed to *Down*.
5. A trap is issued to the NMS indicating the change in loopback status. For more information about the type of trap that the NMS generates, see Appendix A, "Trap Alarm Condition Messages."
6. The loopback status is updated on the PPort Attributes dialog box and the PPort Foreground Diagnostics dialog box.
7. A user at the far-end can initiate tests to test the link that has just looped back.
8. After completion of tests, a loop deactivate code is sent to the near-end port.
9. The framer detects the loop code and interrupts the processor.
10. The processor responds by deactivating the specified loopback.
11. The polling mechanism detects the change to a Normal operating status and the port operating status changes to *Up*.
12. The system updates the loopback status on the PPort Attributes dialog box and PPort Foreground Diagnostics dialog box.

Activating and Ending a T1/E1 Loopback

To activate and end a T1/E1 loopback:

1. On the network map, select the switch object from which you want to obtain physical port diagnostic information.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears.
3. Select the physical port that you want to test. To do this, double-click on the physical port. The Set Physical Ports Attributes dialog box appears.
4. Disable the physical port as follows:
   - **a.** Change the port admin status value to *Down*.
   - **b.** Choose Apply. The system then prompts you to confirm the change.
   - **c.** Choose OK.
   - **d.** Choose Close. The system then redisplays the Set Switch Back Panel dialog box.
5. Verify that the physical port you want to test is still selected.
6. Choose Diag. The Perform Foreground Diagnostic Test dialog box appears (see Figure 5-6).

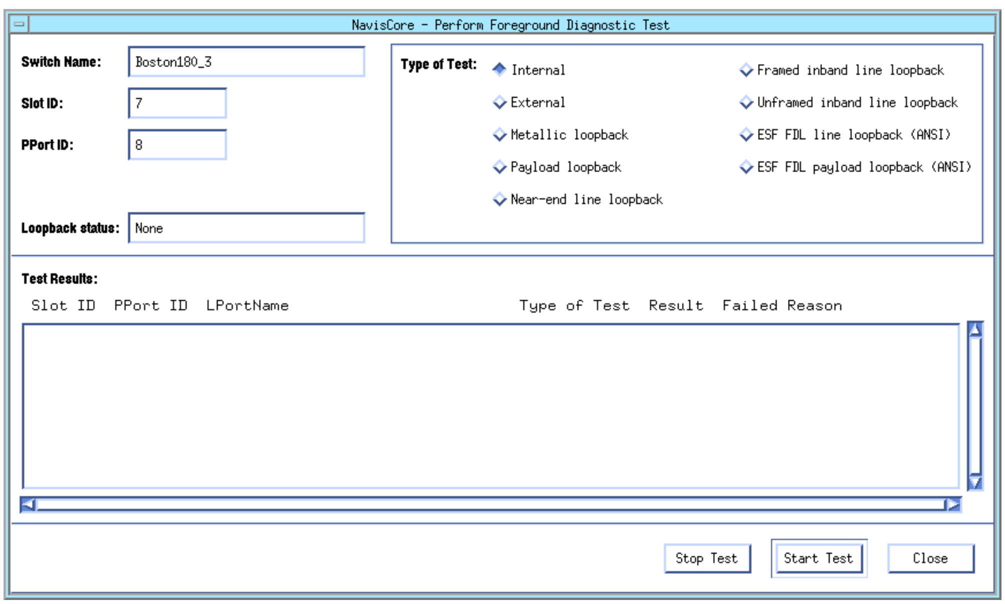


Figure 5-6. Perform Foreground Diagnostic Test Dialog Box (T1/E1 Loopback)

7. Select one of the following tests:
   - Metallic Loopback (ATM IOMs only)
   - Payload loopback
   - Line loopback
   - Framed inband line loopback
   - Unframed inband line loopback
   - ESF FDL line loopback (ANSI)
   - ESF FDL payload loopback (ANSI)
8. Choose Start Test to start a selected T1/E1 loopback test. The system displays the test results at the bottom of the dialog box.
9. Choose Stop Test to disable the selected T1/E1 loopback test and return to a normal state.

> The loopback state is not stored in PRAM. If you reboot the module, the DS1 returns to a normal state.

10. When you are finished running the loopback test, reset the physical port's admin status to *Up*.

Loopback Tests for Channelized DS3 and DS3-1-0 Modules

The loopback options for channelized DS3 and DS3-1-0 modules enable you to test the transmission path of a specific DS1 or DS0 channel. You can generate the following types of loopback tests:

DS1 Near-End Loopback — Tests the DS1 channels and logical ports on the channelized DS3 module or DS3-1-0 module. This test enables you to test the physical path for data transmission, by looping back traffic from the DACS/MUX, CSU, or DSU in one or both directions.

DS0 Near-End Loopback (Channelized DS3-1-0 Modules Only) — Tests the DS0 channels and logical ports on the channelized DS3-1-0 module. This test enables you to test the physical path for data transmission, by looping back traffic from the DACS/MUX, CSU, or DSU in one or both directions.

DS1 Far-End Loopback — Tests the DS1 channels and logical ports on the channelized DS3 module or DS3-1-0 module. This test enables you to test the physical path for data transmission, by looping back traffic from the switch to the DACS/MUX, or from the CSU/DSU and back to the originating switch.

DS1 BERT (Channelized DS3 Modules Only) — Generates and monitors Bit Error Rate Test (BERT) patterns and measures the quality of data transmission on any DS1 channel on a channelized DS3 IOM. Use this test in conjunction with a loopback test.

DS0 BERT (Channelized DS3-1-0 Modules Only) — Generates and monitors Bit Error Rate Test (BERT) patterns and measures the quality of data transmission on any DS0 channel on a channelized DS3-1-0 IOM. Use this test in conjunction with a loopback test.

DS1 Near-end Loopback Tests

The DS1 near-end loopback option enables you to test the physical path for data transmission by performing a payload, line, or diagnostic loopback. When you initiate any of these tests, the entire DS1 channel of the physical port is put into loopback mode from the near-end.

You can generate and receive the following types of DS1 near-end loopback tests (the default Test Type is *Clear Loopback*):

Payload — A near-end loopback in which the incoming DS1 payload is looped back toward the network after extracting and reinserting the framing pattern into the transmitted DS1 data stream.

Line — A near-end loopback that operates upon receipt of a specific framed pulse pattern. The line loopback pulse codes and functions are either *Activate* or *Deactivate*. You can perform line loopback tests on each of the 28 DS1 channels.

Diagnostic — A near-end loopback in which the transmitted signal is returned as the received signal. This test is internal to the channelized DS3 module or DS3-1-0 module and does not require a CSU/DSU. Figure 5-7 illustrates a DS1 near-end diag loopback in which the test pattern generation originates at the channelized DS3 module and loops back to the channelized DS3 module. This test is internal to the module.

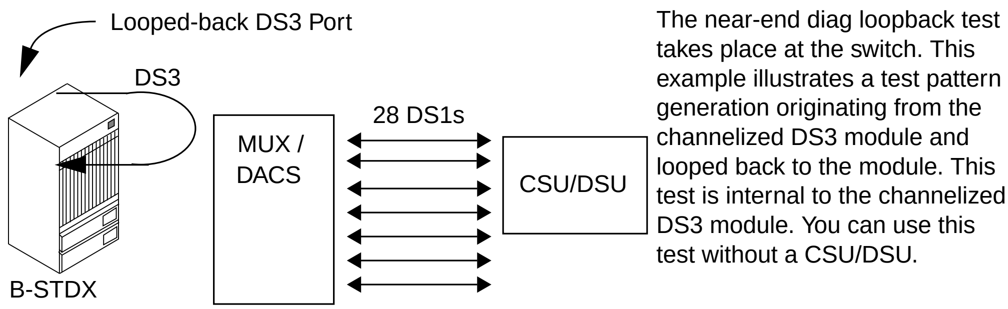


Figure 5-7. Near-end Diag Loopback

Figure 5-8 illustrates a near-end loopback test in which the test pattern originates at the CSU/DSU and passes through the DACS/MUX. The multiplexer (MUX) joins the 28 DS1 channels and combines them into one DS3 signal. The signal is looped back at the DS3 port and returned to the CSU/DSU.

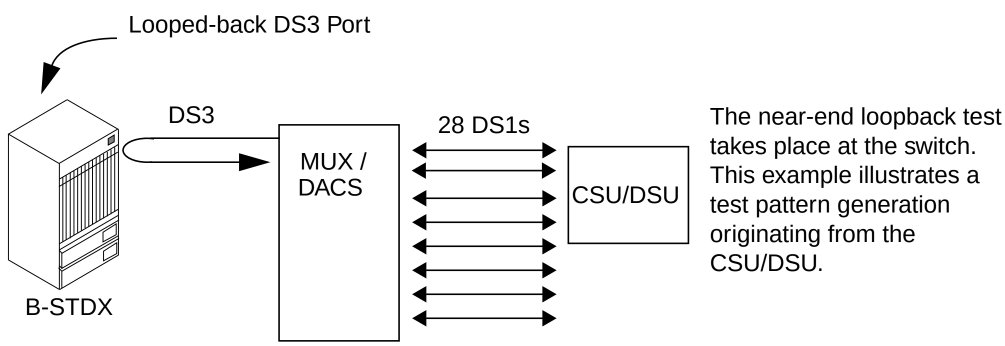


Figure 5-8. Near-end Loopback

DS1 Far-end Loopback Tests

Use the far-end loopback option to loop data from the switch to the DACS/MUX or CSU/DSU and back to the originating switch.

Table 5-3 lists and describes the types of far-end loopback tests you can generate and receive from the DS1 channel (the default Test Type is *Send No Code*).

Table 5-3. Far-end Loopback Tests

Loopback Test	Description
Activate Framed CSU Line Loopback	Requested by the CSU; returns information to the switch on the receive line.
Release Framed CSU Line Loopback	Sends a CSU code to stop the Far-end loopback and return to normal two-way traffic.
Activate NI Line Loopback	Requested by the NI; returns information to the switch on the receive line.
Release NI Line Loopback	Sends an NI code to stop the Far-end loopback.
Activate ESF ANSI Line Loopback	Requested by Extended Superframe (ESF); returns information to the switch on the receive line.
Release ESF ANSI Line Loopback	Sends an ESF code to stop the Far-end loopback.
Activate ESF ANSI Payload Loopback	Requested by ESF; returns information to the switch as framed data.
Release ESF ANSI Payload Loopback	Sends an ESF ANSI code to stop the Far-end payload loopback.
Activate Unframed CSU Line Loopback	Requested by the CSU; returns information to the switch on the receive line.
Release Unframed CSU Line Loopback	Sends a CSU code to stop the Far-end line loopback and return to normal two-way traffic.
Activate Unframed NI Line Loopback	Requested by the NI; returns information to the switch on the receive line.
Release Unframed NI Line Loopback	Sends an NI code to stop the Far-end line loopback.
Activate OOB NI Line Loopback	Requested by an out of band NI; returns information to the switch on the receive line.
Release OOB NI Line Loopback	Sends an out of band NI code to stop the Far-end line loopback.

Figure 5-9 illustrates a far-end CSU/DSU loopback that takes place at the CSU/DSU.

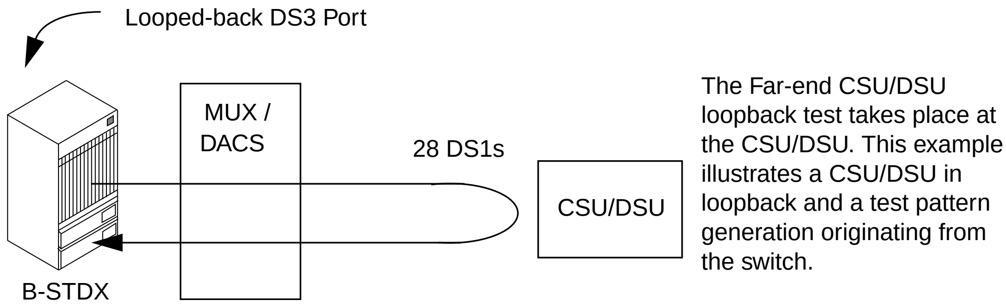


Figure 5-9. DS1 Far-end CSU/DSU Loopback

Figure 5-10 illustrates a DS1 Far-end NI loopback using Smartjacks and/or a Midspan Repeater. The NI loopback originates at the CSU/DSU and test pattern generation originates at the switch.

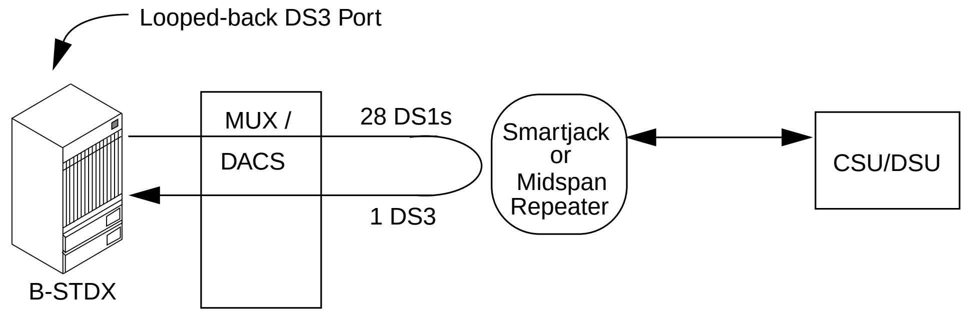


Figure 5-10. DS1 Far-end NI Loopback

Starting and Ending a DS1 Loopback Test

To start and end a DS1 loopback on a channelized DS3 module or DS3-1-0 module:

1. On the network map, select the switch object from which you want to obtain physical port and channel diagnostic information.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Double-click on the physical port that you want to test. The Set Physical Port Attributes dialog box appears. Figure 5-11 shows a Set Physical Port Attributes dialog box for a channelized DS3 physical port. (The Set Physical Port Attributes dialog box for a channelized DS3-1-0 physical port is similar in appearance.)

Select a channel by double-clicking it, or by clicking it once and choosing Set Chan Attr.

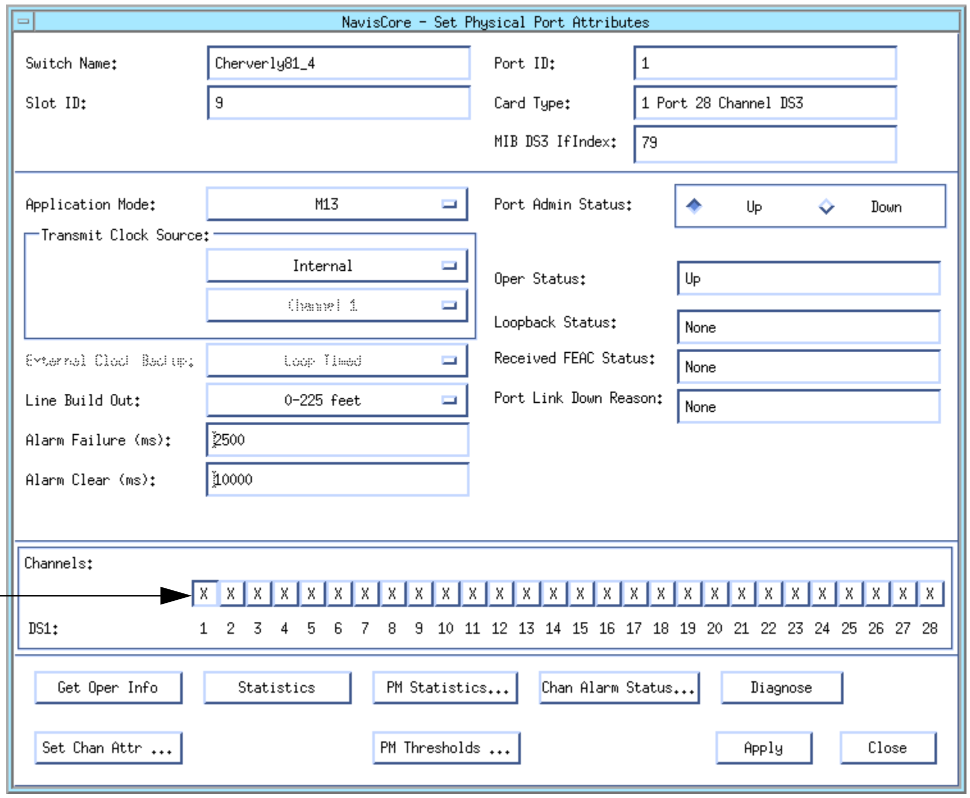


Figure 5-11. Set Physical Port Attributes Dialog Box

4. Double-click on the channel button of the DS1 channel that you want to test, or select a channel and choose Set Chan Attr. The Set Channel Attributes dialog box appears.

Figure 5-12 shows a Set Channel Attributes dialog box for a DS1 channel on a channelized DS3 physical port. (The Set Channel Attributes dialog box for a channelized DS3-1-0 physical port is similar in appearance.)

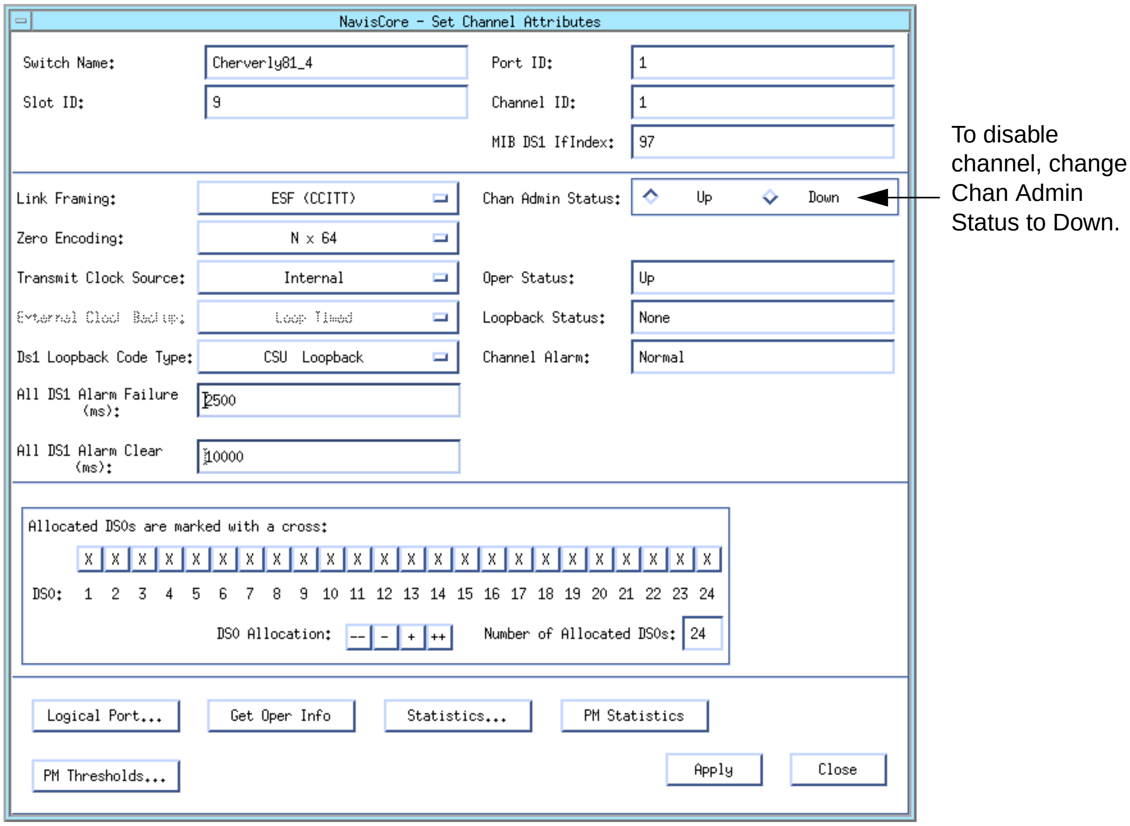


Figure 5-12. Set Channel Attributes Dialog Box

5. Disable the channel for use during the loopback test by changing the chan admin status to *Down*.
6. Choose Apply.
7. Choose Close. The system then redisplays the Set Physical Port Attributes dialog box.
8. Verify the channel you want to test is selected.
9. Choose Diagnose. The Perform Foreground Channel Diagnostic Test dialog box appears.

Figure 5-13 shows the Perform Foreground Channel Diagnostic Test dialog box for a DS1 channel on a channelized DS3 physical port. (The Perform Foreground Channel Diagnostic Test dialog box for a DS1 channel on a channelized DS3-1-0 physical port is similar in appearance, except the BERT option is not supported.)

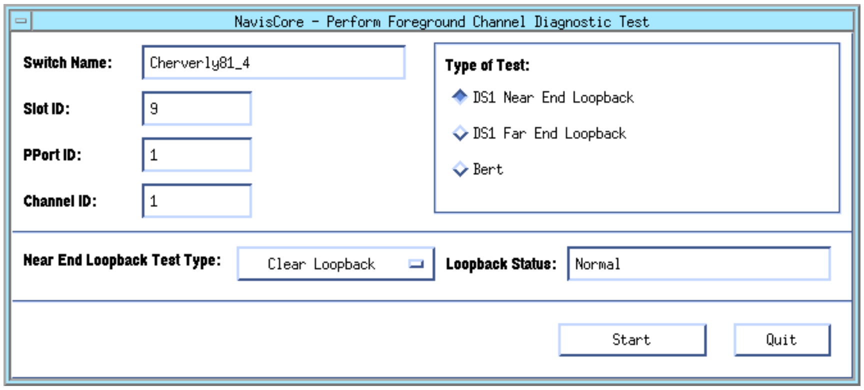


Figure 5-13. Perform Foreground Channel Diagnostic Test Dialog Box (DS1 Channel Loopback)

Table 5-4 describes the Perform Foreground Channel Diagnostic Test dialog box fields.

Table 5-4. Perform Foreground Channel Diagnostic Test Fields

Field	Displays...
Slot ID	I/O slot number in which the module resides.
PPort ID	Port number.
Channel ID	Channel number of the channel you are testing.
Loopback Test Type	The current loopback test type.
Loopback Status	Channel's current loopback status.

10. Follow the instructions in the next section according to the type of test you want to generate. For instructions on BERT testing, see "DS1 BERT Testing for Channelized DS3" on page 5-33. Note that DS1 BERT testing is not available for DS3-1-0 modules.

Generating a DS1 Near-end Loopback

This section describes how to generate a DS1 near-end loopback test. For more information about test types, see "DS1 Near-end Loopback Tests" on page 5-22.

1. To generate a DS1 near-end loopback test, select DS1 Near-End Loopback for the Type of Test (as shown in Figure 5-14).
2. In the Near-End Loopback Test Type field, select one of the following options: Payload Loopback, Line Loopback, or Diagnostic Loopback. Do not select the Clear Loopback option at this time. This option is for stopping a test.
3. Choose Start to begin the test. The loopback test takes approximately 15 seconds to complete. Test results appear in the Loopback Status field as shown in Figure 5-14.

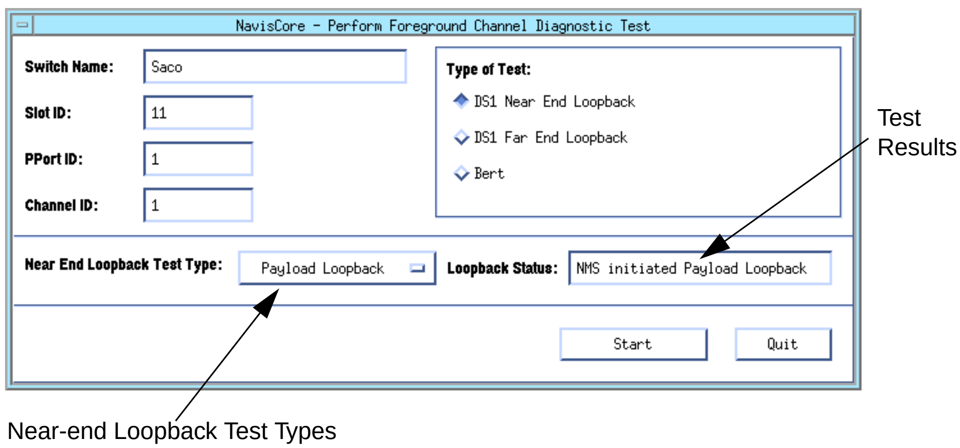


Figure 5-14. DS1 Near-end Loopback Test Type Selections

4. Optionally, for DS1 channels on channelized DS3 physical ports only, select Bert for the type of test and inject a bit error. (See "Starting and Ending a BERT Test for a DS1 Channel" on page 5-34 for instructions.) BERT tests are not supported on channelized DS3-1-0 modules.
5. To stop the test, select Clear Loopback in the Near-End Loopback Test Type field and choose Start.

> If you choose Quit before stopping the test, the test will continue to run and the channel admin status will remain Down. To stop the test, select Clear Loopback and choose Start.

6. When you are finished running the loopback test, reset the chan admin status to *Up*.

Generating a DS1 Far-end Loopback

This section describes how to generate a DS1 far-end loopback test for a DS1 channel on a channelized DS3 module or DS3-1-0 module. For more information about test types, see "DS1 Far-end Loopback Tests" on page 5-24.

1. On the Perform Foreground Channel Diagnostic Test dialog box (see Figure 5-15), select DS1 Far- End Loopback for the type of test.

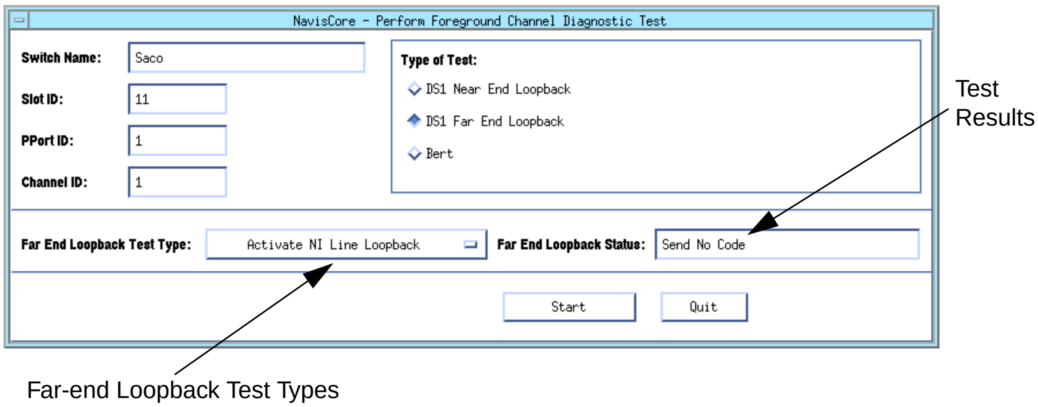


Figure 5-15. DS1 Far-end Loopback Test Type Selections

2. In the Far-End Loopback Test Type field, select one of the following options:
   - Activate Framed CSU Line Loopback
   - Activate NI Line Loopback
   - Activate ESF ANSI Line Loopback
   - Activate ESF ANSI Payload Loopback
   - Activate Unframed CSU Line Loopback
   - Activate Unframed NI Line Loopback
   - Activate OOB NI Line Loopback

   Do not select Release [*Test Type*] Loopback at this time. This option is for stopping a test.

3. Choose Start to begin the test. The loopback test takes approximately 15 seconds to complete.
4. Optionally, for DS1 channels on channelized DS3 physical ports only, select Bert for the type of test and inject a Bit Error Rate. (See "Starting and Ending a BERT Test for a DS1 Channel" on page 5-34 for instructions.) BERT tests are not supported on channelized DS3-1-0 modules.
5. To stop the test, select Release [*Test Type*] Loopback in the Far-End Loopback Test Type field and choose Start.

> If you choose Quit before releasing the test, the test will continue to run and the chan admin status will remain Down. To stop the test, select Release [Test Type] Loopback in the Far-End Loopback Test Type field and choose Start.

6. When you are finished running the loopback test, reset the chan admin status to *Up*.

Activating and Ending a DS0 Near-End Loopback

For testing DS0 channels on DS3-1-0 modules, the DS0 loopback option enables you to test the transmission path of a logical port by looping back traffic in one or both directions. You can initiate a DS0 loopback over one or more DS0 channels of a logical port. Use the DS0 near-end loopback option to loop back traffic from the office channel unit (OCU), CSU, or DSU. Figure 5-16 illustrates a DS0 near-end loopback.

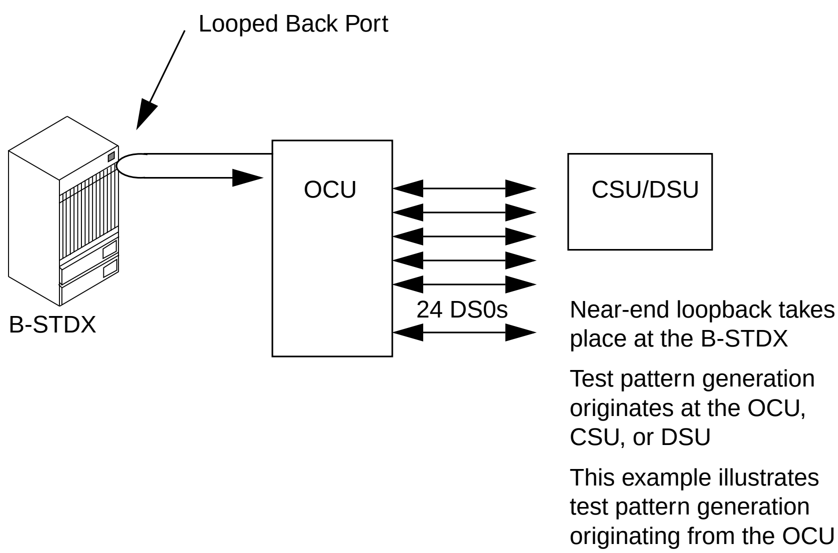


Figure 5-16. DS0 Near-end Loopback for DS3-1-0

To activate and end a DSO Near-End loopback:

1. On the network map, select the switch object from which you want to obtain physical and logical port diagnostic information.

2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears.

3. Double-click on the physical port. The Set Physical Ports Attributes dialog box appears.

4. Double-click on the channel button of the DS1 channel associated with the DS0 channels you want to test, or select the DS1 channel and choose Set Chan Attr. The Set Channel Attributes dialog box appears.

5. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.
6. Select the logical port that you want to test.
7. Disable the logical port as follows:
   a. Choose Modify from the Set All Logical Ports in PPort dialog box. The system then displays the first of two Modify Logical Port dialog boxes.
   b. Choose OK. The system displays the second Modify Logical Port dialog box.
   c. Change the value in the Admin Status field to *Down*.
   d. Choose OK.
8. Choose Options ⇒ Diagnostics.
9. Choose View. The Perform Foreground Diagnostic Test dialog box appears (see Figure 5-17).

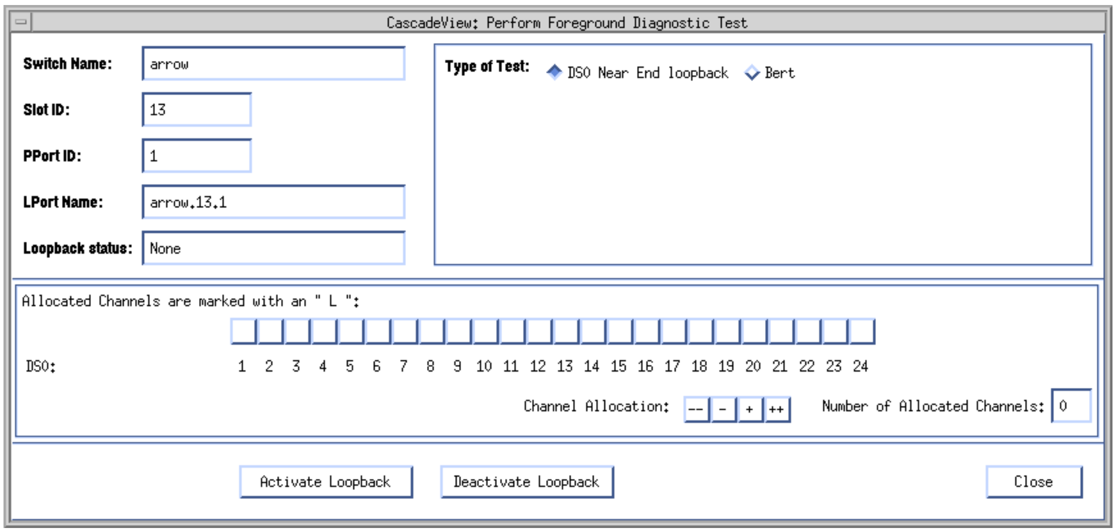


Figure 5-17. Perform Foreground Diagnostic Test Dialog Box (DS0 Channel Loopback)

10. Select DS0 Near End loopback as the type of test. The system then displays all of the logical port channels.
11. Select the channels on which you want to perform a DS0 near-end loopback. An **L** indicates a DS0 is in a loopback state.

    You can select one or more channels by clicking on the appropriate channel(s) or by using the channel selection buttons described in Table 5-5.

Table 5-5. DS0 Channel Selection Buttons

Button	Function
+	Starts at the left and selects one channel at a time
-	Starts at the right and deselects one channel at a time
++	Selects all channels
--	Deselects all channels

12. Select Activate Loopback to activate a DS0 loopback test.

13. Select Deactivate Loopback to return to a normal state.

> The loopback state is not stored in PRAM. If you reboot the module, the DS0 returns to a normal state.

14. When you finish running the test, reset the logical port's admin status to *Up*.

DS1 BERT Testing for Channelized DS3

Bit Error Rate Testing (BERT) generates and monitors BERT patterns and measures the quality of data transmission on any DS1 channel on a channelized DS3 module. The generation and monitoring functions are independent and can be invoked separately or together. The errors in the pattern of transmitted bits are counted to determine the Bit Error Rate.

You use the BERT test in conjunction with the loopback test to qualify new T1 services or debug problems with existing services. You can insert bit errors (*Inject Error* option) into the DS1 data stream when you are performing a loopback test by inserting a single or continuous bit error. Table 5-6 lists and describes the types of BERT patterns you can generate and receive from the DS1 channel.

Table 5-6. BERT Test Patterns for DS1 Channels

BERT Test Pattern	Description
All Zeros	Generates and expects data in zeros (for example: 0X00).
All Ones	Generates and expects data in ones (for example: 0XFF).
One Zero	Alternates ones and zeros (for example: 0XAA).
One One Zero Zero	Alternates between two (1s) and two (0s) (for example: 0XCC).
One Of Eight	Each byte is "10000000" (for example: 0X80).

Table 5-6. BERT Test Patterns for DS1 Channels (Continued)

BERT Test Pattern	Description
Three Of Twenty Four	Generates and expects the Hex pattern (for example: 0X44,0X40,0X00).
QRSS	Standard Quasi Random pattern with bit stuffing.
1 Byte User Pattern	Repeated user-defined byte pattern.
2 Byte User Pattern	Repeated user-defined 2-byte (16-bit) pattern.
3 Byte User Pattern	Repeated user-defined 3-byte (24-bit) pattern.

Starting and Ending a BERT Test for a DS1 Channel

1. On the network map, select the switch object from which you want to obtain physical port and channel diagnostic information.

2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.

3. Double-click on the channelized DS3 physical port associated with the DS1 channel that you want to test (the test is not supported for DS3-1-0 modules). The Set Physical Port Attributes dialog box appears (see Figure 5-11 on page 5-26).

4. Double-click on the channel button of the DS1 channel that you want to test, or select the channel and choose Set Chan Attr.

5. Disable the channel during the loopback test by changing the chan admin status to *Down*.

6. Choose Apply.

7. Choose Close.

The system then redisplays the Set Physical Port Attributes dialog box.

8. Choose Diagnose. The Perform Foreground Channel Diagnostic Test dialog box appears (see Figure 5-18).

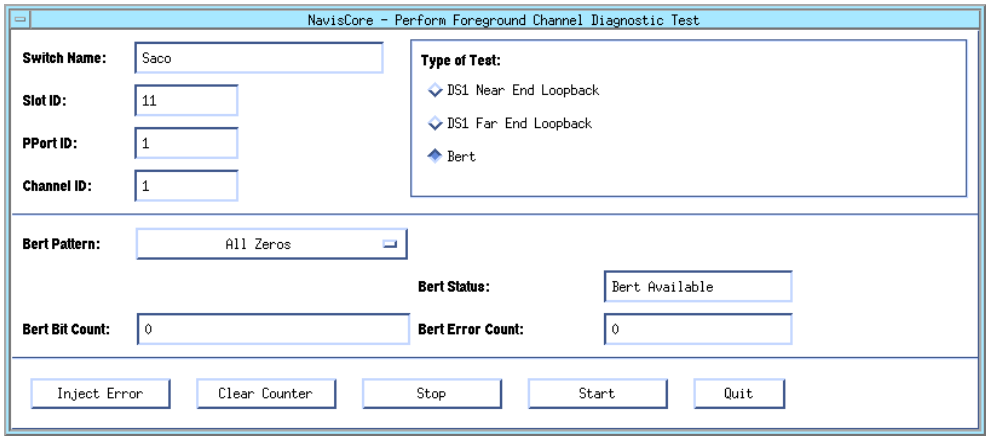


Figure 5-18. Perform Foreground Diagnostic Test Dialog Box (BERT)

9. Select Bert in the Type of Test field as shown in Figure 5-18.

Table 5-7 describes the fields on this dialog box.

Table 5-7. DS1 BERT Test Fields

Field	Displays...
Switch Name	Name of the switch in which the module resides.
Slot ID	Slot number in which the I/O module resides.
PPort ID	Physical port number.
Channel ID	Channel number of the channel you are testing.
Bert Pattern	The BERT pattern you select for the test.
Bert Bit Count	Number of received bits.
Bert Status	Current BERT state (Unavailable, Out of Frame, Available, In-Frame).
Bert Error Count	Number of received bit errors.

10. Select a BERT pattern in the Bert Pattern field. The default BERT pattern is *All Zeros* (see Table 5-6 on page 5-33 for a description of BERT patterns).

11. Select Clear Counter to clear the Bit Count and Error Count fields and return the value to zero.

12. Choose Start to begin the test. Test results appear in the Bert Status field (see Figure 5-19).

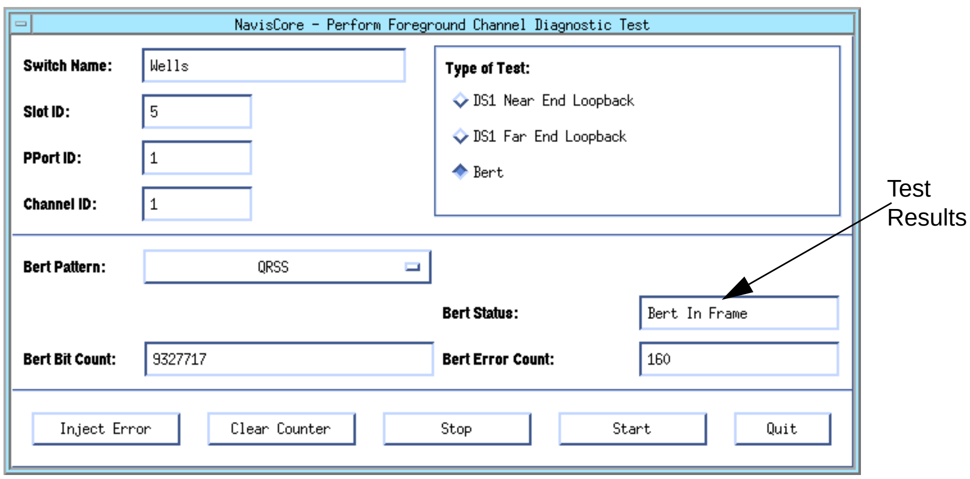


Figure 5-19. Perform Foreground Channel Diagnostic Test Dialog Box

13. Choose Inject Error to inject a bit error and detect a loss of pattern sync. Test results appear in the Bit Count and Error Count fields. Compare the displayed Bert Error Count to the expected count.

14. To stop the test and exit, choose Stop and Quit.

15. When you are finished running the test, reset the chan admin status to *Up*.

Inject Error Example

Figure 5-20 shows a BERT test using a QRSS pattern. Test results are displayed in the Bit Count and Error Count fields. The Bert Error Count field displays a count of 1. If you choose Inject Error again, the Bert Error Count field increments by 1 and displays a count of 2.

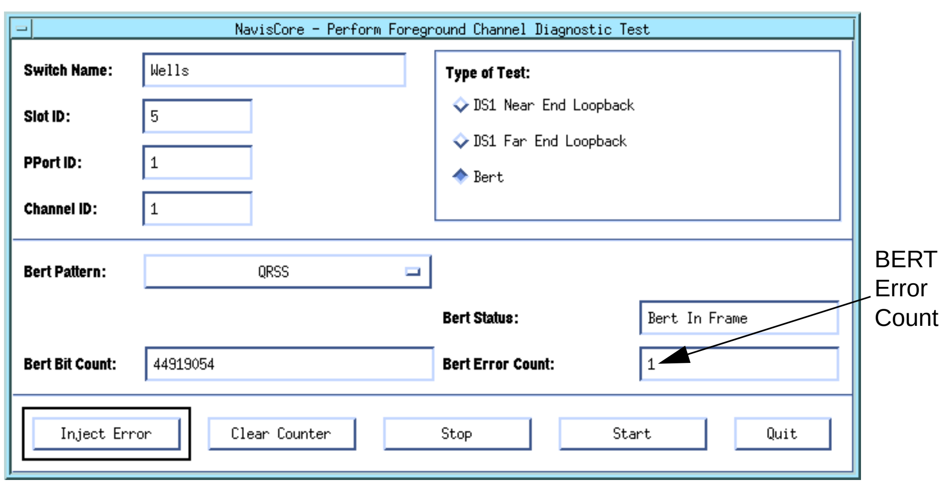


Figure 5-20. BERT Error Count Example

DS0 BERT Testing for Channelized DS3-1-0

BERT generates and monitors test patterns and measures the quality of data transmission on any logical port associated with DS0 channels on DS3-1-0 modules. The generation and monitoring functions are independent, and can be run separately or together. The errors in the pattern of transmitted bits are counted to determine the Bit Error Rate.

The BERT test automatically detects *any* repetitive pattern of specified length (rather than looking for the selected pattern). You should compare the pattern that you select to the pattern automatically detected in the BERT test.

You use the BERT test in conjunction with the loopback test to qualify new logical port services or debug problems with existing services. You can insert bit errors (*Inject Error* option) into the defined logical port data stream when you are performing a loopback test by inserting a single bit error. Table 5-8 lists and describes the types of BERT patterns you can generate and receive from the DS0 channels.

Table 5-8. BERT Test Patterns for DS0 Channels

BERT Test Pattern	Description	Detected Pattern
All Zeros	Generates and expects data in zeros.	0
All Ones	Generates and expects data in ones.	FF
One Zero	Alternates ones and zeros.	AA,55
One One Zero Zero	Alternates between two (1s) and two (0s).	66,99,CC,33
1 of 8	Each byte is “10000000”, “00100000”.	1,2,4,8,10,20,40,80
3 of 24	Generates and expects the Hex pattern.	11,111,1110,1000, 8880,88 ...
QRSS	Standard Quasi Random pattern with bit stuffing.	(no random pattern displayed)
1 Byte User Pattern	Repeated user defined byte pattern.	11
2 Byte User Pattern	Repeated user-defined 2-byte (16-bit) pattern.	2F2F
3 Byte User Pattern	Repeated user-defined 3-byte (24-bit) pattern.	3A4B5C

Starting and Ending a BERT Test for a DS0 Channel

1. On the network map, select the switch object from which you want to obtain logical port and channel diagnostic information.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Double-click on the physical port that you want to test. The Set Physical Port Attributes dialog box appears (see Figure 5-11 on page 5-26).
4. Double-click on the channel button of the DS1 channel associated with the DS0 channels you want to test, or select a DS1 channel and choose Set Chan Attr. The Set Channel Attributes dialog box appears.
5. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.
6. Select a logical port associated with the DS0 channels and choose Modify. The Modify Logical Port Type dialog box appears.
7. Choose OK. The Modify Logical Port dialog box appears.
8. Disable the logical port during the loopback test by changing the logical port admin status to *Down*, then choose OK. The Set All Logical Ports in PPort dialog box reappears.
9. Select Options ⇒ Diagnostics.
10. Choose View. The Perform Foreground Diagnostic Test dialog box appears (see Figure 5-21).

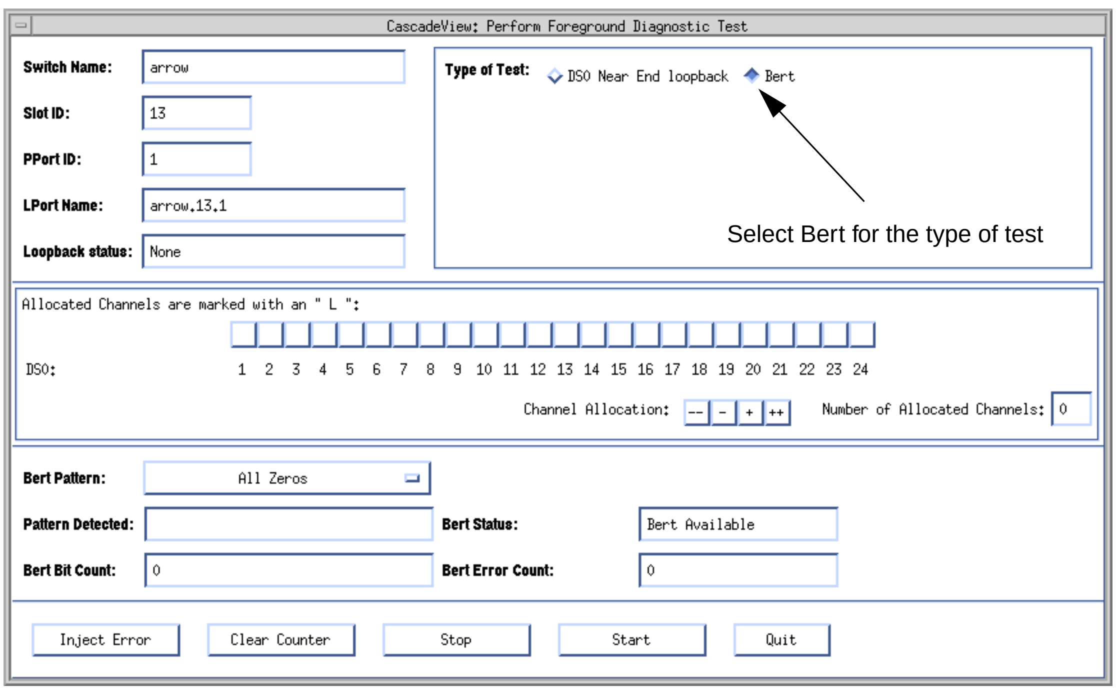


Figure 5-21. Perform Foreground Diagnostic Test Dialog Box (DS0 BERT)

11. Select Bert for the type of test.

Table 5-9 describes the fields on this dialog box.

Table 5-9. DS0 BERT Test Fields

Field	Displays...
Switch Name	Name of the switch in which the module resides.
Slot ID	Slot number in which the I/O module resides.
PPort ID	Physical port number.
Lport Name	Name of the logical port you are testing.
Loopback Status	Current loopback status.
Allocated Channels	The DS0 channels allocated to the logical port.
Bert Pattern	The BERT pattern you select for the test.
Pattern Detected	The BERT pattern detected.
Bert Bit Count	Number of received bits.
Bert Status	Current BERT state (Unavailable, Out of Frame, Available, In-Frame).
Bert Error Count	Number of received bit errors.

12. Select a BERT pattern in the Bert Pattern field. The default BERT pattern is *All Zeros* (see Table 5-8 on page 5-37 for a description of BERT patterns).
13. Select Clear Counter to clear the Bit Count and Error Count fields and return the value to zero.
14. Choose Start to begin the test. Test results appear in the Bert Status field.
15. Choose Inject Error to inject a bit error and detect a loss of pattern sync. Results appear in the Bit Count and Error Count fields. Compare the displayed Bert Error Count to the expected count.
16. To stop the test and exit, choose Stop and then Quit.
17. When you finish running the test, change the chan admin status to *Up*.

DS3/E3 Loopbacks

Table 5-10 lists and describes DS3/E3 loopback tests.

> Some DS3/E3 modules do not support all of the loopback tests described in Table 5-10.

Table 5-10. DS3/E3 Loopback Tests

Loopback Test	Description
Near-end line	Loops the receiver to the transmitter to loop the incoming signal back to the far-end.
Far-end	Sends a code to request the far end to set itself into loopback mode. This type of loopback involves sending an in-band FEAC loop-up signal to the device attached to the physical port. When you start this test, the attached device responds by placing itself in the FEAC loop-up state (assuming the attached device supports FEAC loop-up and down signalling). The attached device will remain in that state until you stop the test (which causes a FEAC loop-down signal to be sent). Running this test has no effect on the DS3 physical port (other than the attached device entering a FEAC loop-up state). This loopback test can be used in conjunction with the external loopback test, as the attached device can first be placed in a FEAC loop-up state using the far-end loopback test, and then the external loopback test can be run. The fact that the attached device will be in a FEAC loop-up state means that if the transmission path is good, the test should pass.
Payload	A near-end loopback in which the signal transmitted beyond the loopback point (the forward signal) when the loopback is activated is the same as the received signal at the loopback point. This type of loopback is similar to a near-end line loopback in that the incoming signal from the device attached to the physical port is looped back. However, with the payload loopback, the loopback is made after the physical port framer device, such that the signal from the outside traverses the framer device and is then looped back. This is a more comprehensive test than the near-end line loopback because when you verify the integrity of the signal passing through the loopback, the integrity of the CBX 500 card framer is also verified. The physical port remains in this state until you stop the test.
Near-end diag	Loops the transmitter to the receiver to loop the outgoing signal back to the DS3 port. This test enables the module to test itself.

DS3/E3 Loopback Traps

The NMS generates a trap when a DS3 interface changes its loopback state. For more information about the type of trap that the NMS generates, see Appendix A, "Trap Alarm Condition Messages."

Activating and Ending a DS3/E3 Loopback

1. On the network map, select the switch object from which you want to obtain physical port diagnostic information.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the physical port that you want to test. To do this, double-click on the physical port. The Set Physical Ports Attributes dialog box appears.
4. Disable the physical port as follows:
   - **a.** Change the port admin status to *Down*.
   - **b.** Choose Apply. The system then prompts you to confirm the change.
   - **c.** Choose OK.
   - **d.** Choose Close. The system then redisplays the Set Switch Back Panel dialog box.
5. Verify that the physical port you want to test is still selected.
6. Choose Diag. The Perform Foreground Diagnostic Test dialog box appears.

   Table 5-11 describes the Perform Foreground Diagnostic Test dialog box fields.

Table 5-11. Perform Foreground Diagnostic Test Dialog Box Fields (DS3/E3)

Field	Displays...
Switch Name	Name of the switch in which the module resides.
Slot ID	Slot number in which the I/O module resides.
PPort ID	Physical port number.
Loopback Status	Physical port's current loopback status.

7. Select the type of loopback test you want to generate:
   - Near-end line
   - Far-end
   - Payload (ATM DS3 modules only)
   - Near-end diag (channelized DS3 modules only)

   Table 5-10 on page 5-40 describes each of these loopback tests.

8. Choose Start Test to start the test pattern generation.

   Test results appear in the Test Results box at the bottom of the Perform Foreground Diagnostic Test dialog box.

9. Choose Stop Test to return to a normal state.

> The loopback state is not stored in PRAM. If you reboot the module, the DS3/E3 module returns to a normal state.

10. To exit the dialog box, choose Close. The Switch Back Panel dialog box appears.
11. Double-click on the physical port.
12. Enable the physical port by changing the admin status to *Up*.
13. Choose Apply.
14. Choose Close. The system redisplays the Switch Back Panel dialog box.

DS0 Loopback for Channelized T1, ISDN PRI, and DSX

The DS0 loopback option enables you to test the transmission path of a logical port by looping back traffic in one or both directions. This option is available for the following modules (all of which are supported on the B-STDX 8000/9000):

- Channelized T1
- 4-port ISDN PRI
- 4-port DSX

You can initiate a DS0 loopback over one or more contiguous DS0 channels of a logical port. Use the DS0 near-end loopback option to loop back traffic from the OCU, CSU, or DSU.

Figure 5-22 illustrates a DS0 near-end loopback.

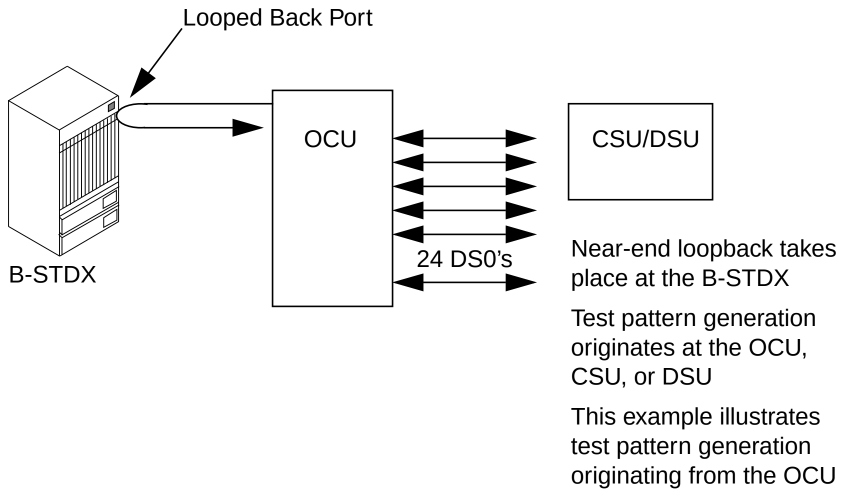


Figure 5-22. DS0 Near-end Loopback for Channelized T1, ISDN PRI, and DSX

Use the DS0 far-end loopback option to specify that data from a switch should be looped from the switch to the OCU, CSU, or DSU and back to the originating switch. Figure 5-23 illustrates a DS0 far-end loopback that occurs at the OCU.

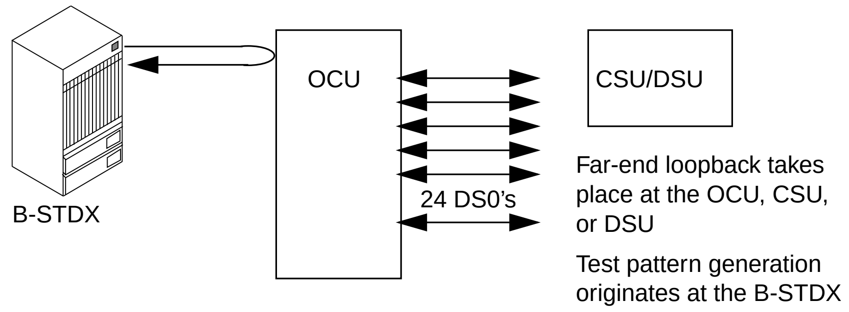


Figure 5-23. DS0 Far-end Loopback

In a far-end loopback, up to three midspan repeaters may be used to boost the signal between the OCU and the CSU/DSU. Figure 5-24 illustrates the use of midspan repeaters in a far-end loopback.

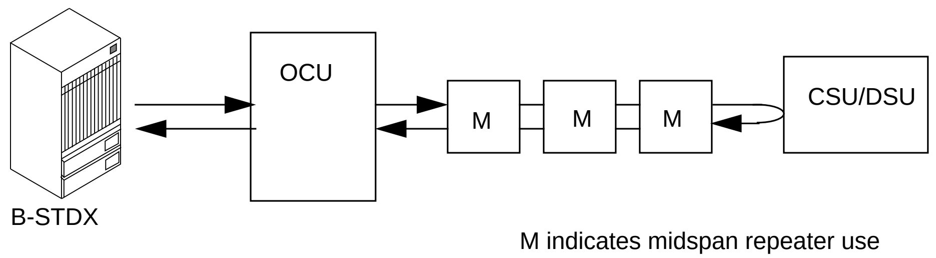


Figure 5-24. Far-End Loopback Using Midspan Repeaters

DS0 far-end loopback is a two-step process that requires you to:

1. Activate the DS0 far-end loopback.
2. Start the test pattern generation from the switch.

You can activate a DS0 far-end loopback test from a logical port that has only one DS0 channel on the logical port. However, the test pattern can be sent from the switch to any consecutive number of DS0 channels.

> Some older T1 module revisions do not support the DS0 loopback feature. If a module does not support the DS0 loopback feature, the DS0 loopback options are grayed out on the Perform Foreground Diagnostic Test dialog box.

Activating and Ending a DS0 Near-End Loopback

1. On the network map, select the switch object from which you want to obtain physical and logical port diagnostic information.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears.
3. Double-click on the physical port associated with the logical port that you want to test. The Set Physical Ports Attributes dialog box appears.
4. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.
5. Disable the logical port as follows:
   a. Choose Modify from the Set All Logical Ports in PPort dialog box. The system then displays the first of two Modify Logical Port dialog boxes.
   b. Choose OK. The system displays the second Modify Logical Port dialog box.
   c. Change the value in the Admin Status field to *Down*.
   d. Choose OK. The system then prompts you to confirm the change.
   e. Choose OK.
6. Choose Options ⇒ Diagnostics.
7. Choose View. The Perform Foreground Diagnostic Test dialog box appears (see Figure 5-25).

Select consecutive DS0 channels

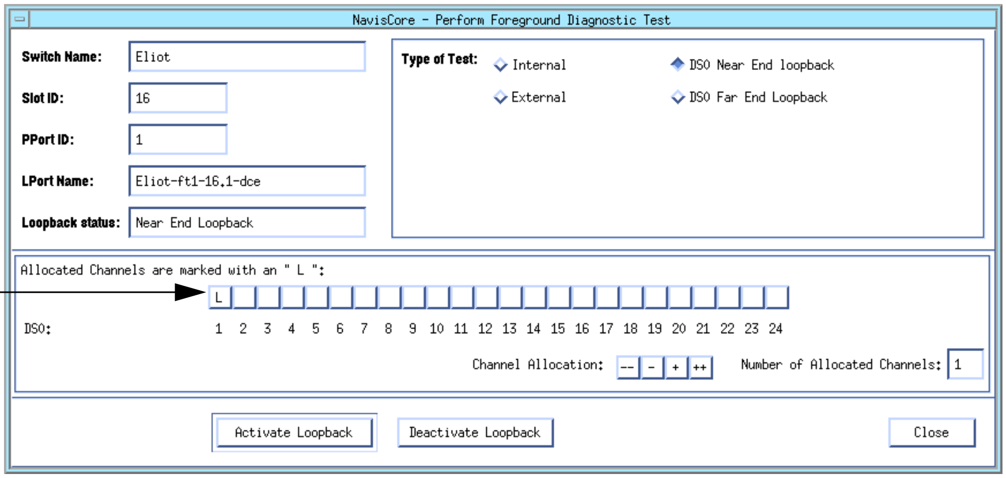


Figure 5-25. Perform Foreground Diagnostic Test Dialog Box (DS0/LPort Near-end Loopback)

8. Select DS0 Near End Loopback as the type of test. The system then displays all of the logical port channels.

9. Select the channels on which you want to perform a DS0 near-end loopback. An **L** indicates a DS0 is in a loopback state.

> Select consecutive DS0 channels. DS0 loopback does not support noncontiguous DS0 channels.

You can select one or more channels by clicking on the appropriate channel(s) or by using the channel selection buttons listed in Table 5-5.

10. Select Activate Loopback to activate a DS0 loopback test.

11. Select Deactivate Loopback to return to a normal state.

> The loopback state is not stored in PRAM. If you reboot the module, the DS0 returns to a normal state.

12. When you are finished running the test, reset the logical port's admin status to *Up*.

Activating and Ending a DS0 Far-End Loopback

1. On the network map, select the switch object from which you want to obtain physical and logical port diagnostic information.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Double-click on the physical port associated with the logical port that you want to test. The Set Physical Port Attributes dialog box appears.
4. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.

> The DS0 far-end loopback test is intended for use with single DS0 applications only. Fractional T1 loopback codes are not supported. The DS0 far-end loopback test is a latching loopback.

5. Disable the logical port as follows:
   - **a.** Choose Modify from the Set All Logical Ports in PPort dialog box. The system then displays the first of two Modify Logical Port dialog boxes.
   - **b.** Choose OK. The system displays the second Modify Logical Port dialog box.
   - **c.** Change the value in the Admin Status field to *Down*.
   - **d.** Choose OK. The system then prompts you to confirm the change.
   - **e.** Choose OK.
6. Choose Options ⇒ Diagnostics.
7. Choose View. The Perform Foreground Diagnostic Test dialog box appears (see Figure 5-26).

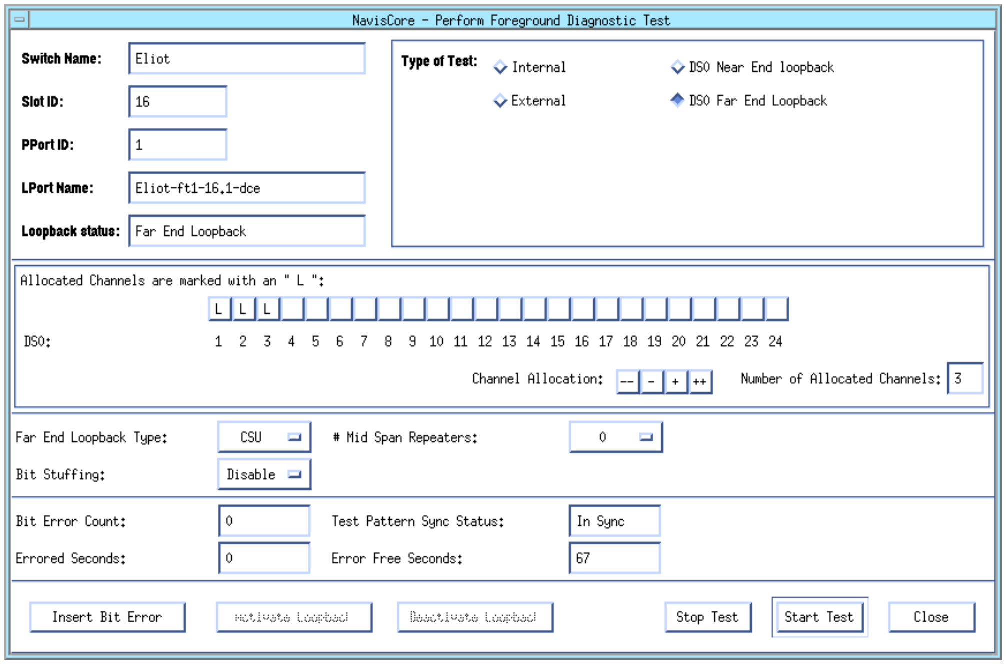


Figure 5-26. Perform Foreground Diagnostic Test Dialog Box (DS0/LPort Far-end Loopback)

8. Select DS0 Far End Loopback as the type of test. The system then displays all of the logical port channels.

9. Select the channel to test. An **L** indicates that the DS0 channel is in a loopback state.You can select a channel by clicking on the appropriate channel.

> The initiation of the DS0 far-end loopback can only be applied to a logical port that has only one DS0 channel. However, the test pattern can be sent from the remote switch to any consecutive number of DS0 channels.
>
> The loopback state is not stored in PRAM. If you reboot the module, the DS0 returns to a normal state. However, the end device (OCU, DSU, or CSU) remains in a loopback state.

10. Complete the following fields:

    Far-End Loopback Type — Specifies the far-end loopback as one of the following types: OCU, CSU, or DSU (see Table 5-12).

Table 5-12. DS0 Far-end Loopback Types

Loopback Type	Description
OCU	Specifies an Office Channel Unit (OCU) loopback type that interfaces to the 56/64 Kilobytes per second span.
CSU	Specifies that the DS0 loopback should loop back the CSU at the customer premise; however, this loopback has the capability to disable any intermediate loopbacks and “punch through” the midspan repeaters and/or smartjacks that are used to boost the signal.
DSU	Specifies that the loopback starts at the DSU device that is closest to the customer equipment (possibly a single CSU/DSU device).

Bit Stuffing — Designates whether bit stuffing is enabled or disabled for the selected logical port. This parameter only applies to T1/E1, DSX-1, and channelized DS3 modules. Bit stuffing affects the available bandwidth of each DS0 channel. If bit stuffing is enabled the available bandwidth is 56 Kbps. If bit stuffing is disabled, the available bandwidth is 64 Kbps.

 # Mid Span Repeaters — This function applies to CSU loopbacks only. Specify the number of mid span repeaters in your network configuration. Enter a value of 1, 2, or 3 to specify the number of midspan repeaters that your configuration uses.

If you are not sure of the number of midspan repeaters that your system uses, and you know that there are three or less, enter a value of 3. Entering a value of 3 will not affect the loopback if you only have one or two midspan repeaters. However, the loopback will not provide valid data if you have more than three repeaters in your configuration.

If you supply a value for this field, the system will “punch-through” and disable the loopback at intermediate midspan repeaters in the configuration.

11. Select Activate Loopback to activate a DS0 loopback.
12. Select Start Test to start the test pattern generation from the switch associated with the selected logical port. The system then displays the DS0 far-end loopback statistics.

Table 5-13 describes these statistics.

Table 5-13. DS0 Far-End Loopback Statistics

Statistic	Description
Bit Error Count	The total number of accumulated bit errors that are received while running the loopback test.
Errored Seconds	The number of seconds during the loopback test that errors occur. The system counts one or more bit errors in any one second increment as an errored second.
Test Pattern Sync Status	Indicates any loss of pattern synchronization that occurs during the test.
Error Free Seconds	The number of seconds during testing in which no bit errors occur.

13. You can *optionally* choose Insert Bit Error to insert a bit error into the test pattern. The purpose of the Insert Bit Error function is to validate the activation of a loopback test or to verify that a connection to remote equipment is operating successfully.

14. Choose Stop Test to stop the test pattern generation.

15. Choose Deactivate Loopback to return to a normal state.

16. When you are finished running the test, reset the logical port's admin status to *Up*.

Test Pattern Generation

The Start Test button on the Perform Foreground Diagnostic Test dialog box enables you to generate and receive a test traffic pattern. The test pattern for a DS0 loopback is 2047.

You can start a test traffic pattern as part of a DS0 far-end loopback test or by using external equipment to generate and receive the test pattern. If you are not performing a loopback test but are using external equipment for the test, choose Start Test to generate test traffic on any selected set of consecutive DS0 channels. You can also receive the test pattern on the same set of consecutive DS0 channels.

Loopback Tests for OC-n/STM-n Ports

You can perform the following loopback tests on OC-n/STM-n ports:

Near-End Line Loopback — Enables the IOA component of the module to transmit received cells back to the sender, without passing the cells to the module. When you initiate a line loopback, the entire physical port is put into the loopback from the near-end. This enables you to generate and receive line loopback code from the physical port of these modules.

Internal Loopback — Sets up a cell loopback signal between the IOM component of the module and the IOA component of the module. This signal does not go “off card”. Use this test to check IOM and IOA internal hardware.

External Loopback — Performs a cell loopback test that directs a signal back towards the source. This tests the ability of the port to send and receive data. You must install a fiber optic loopback connector on the physical port you are testing.

To perform loopback tests on OC-n/STM-n ports:

1. On the network map, select the switch object from which you want to obtain physical port diagnostic information.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Double-click on the physical port that you want to test. The Set Physical Ports Attributes dialog box appears.
4. Disable the physical port as follows:
   a. Change the port admin status to *Down*.
   b. Choose Apply. The system then prompts you to confirm the change.
   c. Choose OK.
   d. Choose Close. The system then redisplays the Set Switch Back Panel dialog box.
5. Verify that the physical port you want to test is still selected.
6. Choose Diag. The Perform Foreground Diagnostic Test dialog box appears.

Figure 5-27 shows the Perform Foreground Diagnostic Test dialog box for an OC12/STM-4 physical port.

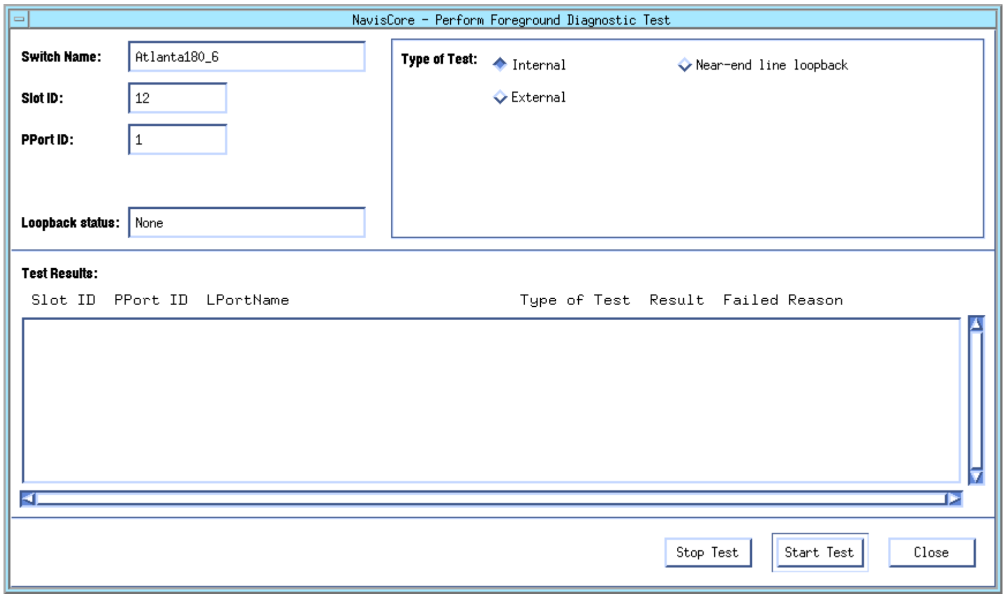


Figure 5-27. Perform Foreground Diagnostic Test Dialog Box (OC12/STM-4)

7. Select the type of loopback test you want to generate.

8. Choose Start Test to start the test pattern generation.

Test results appear in the Test Results box at the bottom of the dialog box.

9. Choose Stop Test to return to a normal state.

10. To exit the dialog box, choose Close. The Switch Back Panel dialog box appears.

11. Double-click on the physical port.

12. Enable the physical port by changing the admin status to *Up*.

13. Choose Apply.

14. Choose Close. The system redisplays the Switch Back Panel dialog box.

The loopback state is not stored in memory. If you reboot the module, the port returns to a normal state.

Loopback Tests for HSSI Ports

HSSI loopbacks on the B-STDX 8000/9000 are initiated by the DTE through the HSSI LA/LB interface signals. The B-STDX 8000/9000 switch drives these signals when you initiate the loopback from the NMS.

You can perform the following loopback tests on HSSI ports:

External Local DTE — Sends a signal to the DSU to indicate that the DTE (switch) is performing a loopback test on the HSSI interface.

External Local Line — Sends a signal to the DSU to indicate that the DTE (switch) is performing a loopback test on the DSU DS3 interface.

External Remote Line — Sends a signal to the DSU to indicate that the DTE (switch) is performing a loopback test on the DSU DS3 interface.

To perform loopback tests on HSSI ports:

1. On the network map, select the switch object from which you want to obtain physical port diagnostic information.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Double-click on the physical port that you want to test. The Set Physical Ports Attributes dialog box appears.
4. Disable the physical port as follows:
   a. Change the port admin status to *Down*.
   b. Choose Apply. The system then prompts you to confirm the change.
   c. Choose OK.
   d. Choose Close. The system then redisplays the Set Switch Back Panel dialog box.
5. Verify that the physical port you want to test is still selected.
6. Choose Diag. The Perform Foreground Diagnostic Test dialog box appears.

Figure 5-28 shows the Perform Foreground Diagnostic Test dialog box for a HSSI physical port.

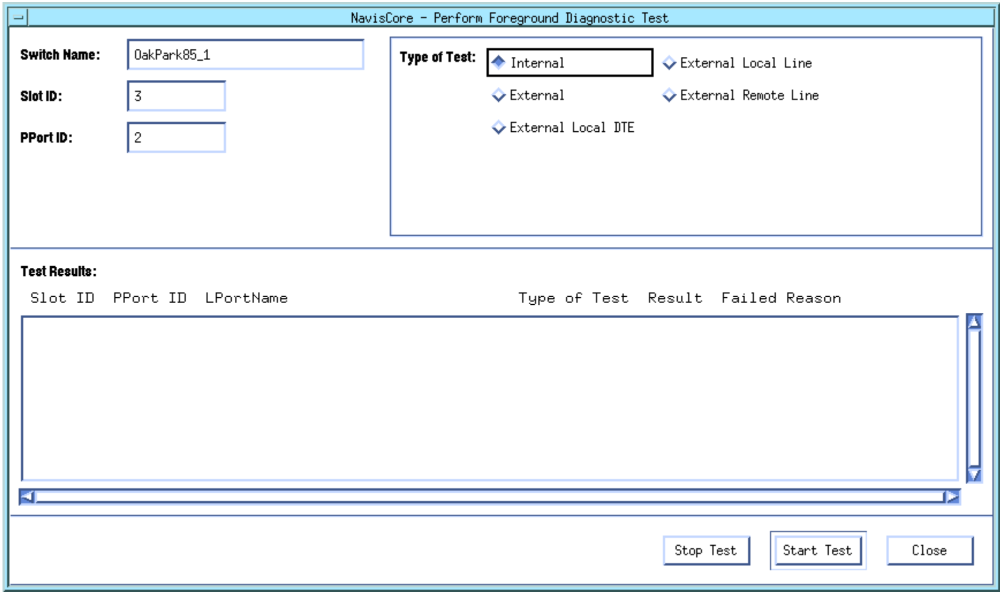


Figure 5-28. Perform Foreground Diagnostic Test Dialog Box (HSSI Ports)

7. Select the type of loopback test you want to generate.:
8. Choose Start Test to start the test pattern generation.

   Test results appear in the Test Results box at the bottom of the dialog box.
9. Choose Stop Test to return to a normal state.
10. To exit the dialog box, choose Close. The Switch Back Panel dialog box appears.
11. Double-click on the physical port.
12. Enable the physical port by changing the admin status to *Up*.
13. Choose Apply.
14. Choose Close. The system redisplays the Switch Back Panel dialog box.

6

Monitoring Logical Ports

NavisCore enables you to monitor the status, configuration attributes and statistics for a logical port. This chapter describes how to monitor logical ports and provides details on logical port status, attributes, and statistics that apply to multiple network services (ATM, Frame Relay, SMDS and so on). Subsequent chapters provide service-specific information on monitoring logical ports.

Accessing Logical Port Monitor Functions

You can access the dialog boxes that display logical port status, attributes, and statistics in two ways:

- From the Monitor menu (described in this chapter).
- From the View Physical Port Attributes dialog box for the physical port associated with a logical port. See "Reviewing Physical Port Status" on page 2-44 for information about this access method.

Viewing Logical Port Status

To view logical port status:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1).

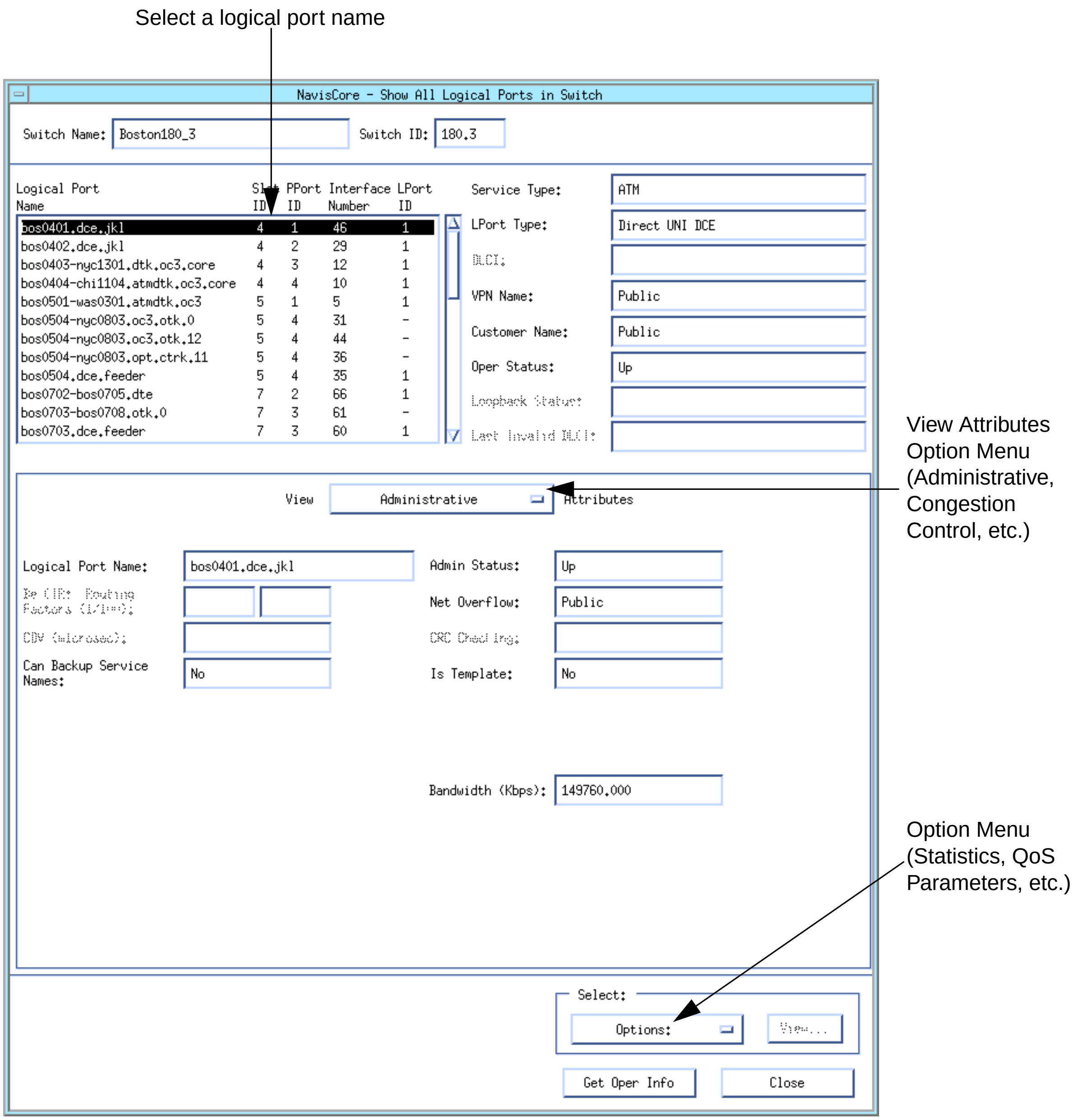


Figure 6-1. Show All Logical Ports in Switch Dialog Box

3. Select a logical-port name from the list.

Table 6-1 describes the general fields on this dialog box.

Table 6-1. Show All Logical Ports in Switch Fields

Field	Displays...
Switch Name	The switch name entered at the time of configuration.
Switch ID	The subnetwork number/host number portion of the in-band IP address of the switch in the internal trunk IP network. For example, “44.5” means that the subnetwork number in the IP address is “44” and the host number is “5.”
Logical Port Name	A unique alphanumeric name for this logical port.
Slot ID	The physical slot number of the IOM that contains the selected logical port.
PPort ID	The number of the physical port for which the selected logical port is configured.
Interface Number	The number assigned by the NMS when the port was configured. This number is a unique identifier used internally to specify a particular logical port in a switch. The traps and circuit monitoring screens refer to the logical port by its interface number (*ifnum*).
LPort ID	The number that uniquely identifies each logical port per physical port.
Service Type	The type of service configured for this logical port, such as ATM or Frame Relay.
LPort Type	The configured type of the selected logical port, such as UNI DCE.
DLCI	(*Frame Relay circuits only*) The data link connection identifier (DLCI). The DLCI is a 10-bit address that identifies a circuit in a Frame Relay network.
VPN Name	A virtual private network (VPN) name. A VPN enables network providers to reserve dedicated network resources for those customers who require guaranteed performance, reliability, and privacy. A VPN provides a dedicated bandwidth to the network customer; however, the provider manages the network.
Customer Name	The name of the customer to which this logical port is dedicated.
Oper Status	Whether the selected port is operationally Up, Down, or Unknown. Unknown indicates that the NMS is unable to contact the switch to retrieve status.
Loopback Status	Whether loopback testing is enabled on this logical port. The default is None (no testing).
Last Invalid DLCI	(*Frame Relay circuits only*) The last invalid DLCI that the switch detected. If a value appears in this field, either the switch or the customer premise equipment (CPE) was not configured properly. Check this value if you have a DLCI that is not receiving traffic.

Table 6-2 describes the option menu selections and buttons on this dialog box. Note that fields vary, depending on the selected logical port type.

Table 6-2. Show All Logical Ports Menus and Buttons

Option Menu/Button	Enables you to...
Options (option menu)	Select an option, then choose View. Options include: *Statistics* – View the summary statistics for the selected logical port. See "Viewing Logical Port Summary Statistics" on page 6-19 for more information. *QoS Parameters* – View the Quality of Service (QoS) parameters (including bandwidth and routing metrics) for selected ATM and Frame Relay logical ports. See "Viewing QoS Parameters" on page 6-13 for more information. *NTM Parameters* – View the configured network traffic management (NTM) parameters for selected ATM logical ports. For more information, see "Viewing NTM and NDC Statistics" on page 13-30. *NTM Statistics* – View the NTM statistics for selected ATM logical ports. For more information, see "Viewing NTM and NDC Statistics" on page 13-30. *NDC Statistics* – View the NDC statistics for selected ATM logical ports. For more information, see "Viewing NTM and NDC Statistics" on page 13-30. *Accounting* – Access the ATM accounting functions for a logical port. For more information, see the *NavisXtend Accounting Server Administrator's Guide.* *Screen Assignments* – View the port SVC security screen assignments for the selected ATM or Frame Relay logical port. For ATM logical port security screens, see "Viewing Port Security Screens" on page 13-82. For Frame Relay logical port security screens, see "Viewing Port Security Screens" on page 14-49. *IP Parameters* – View IP parameters and statistics for the selected logical port. See "Viewing IP Parameters" on page 8-21 for more information. *PPP Options* – View PPP options configured for the logical port. See the *NavisCore Frame Relay Configuration Guide* for more information.
View Attributes (option menu)	View logical port attributes. See "Viewing Logical Port Attributes" on page 6-5 for more information.
Get Oper Info (button)	Update status information for the selected logical port. The Oper Status field indicates whether this port is operationally Up, Down, or Unknown. Unknown indicates that the NMS is unable to contact the switch to retrieve status.
View (button)	View dialog boxes associated with an Options menu selection.
Close (button)	Exit the Show All Logical Ports in Switch dialog box.

4. Select the View Attributes option menu to select attributes for the logical port.
5. When you finish viewing the logical port information, choose Close to return to the network map.

Viewing Logical Port Attributes

Logical port attributes vary, depending on the type of logical port you are monitoring.

Some attributes are available for multiple services and logical port types. Table 6-3 lists and describes these attributes.

Table 6-3. Logical Port Attributes Available for Multiple Services

Attribute	Service/LPort Type Supported
Administrative	All services and their logical port types. See “Viewing Administrative Attributes” on page 6-7 for more information.
Congestion Control	Frame Relay (all port types), Multilink Frame Relay Trunks, Direct Line Trunks, ATM Direct Trunks (B-STDX ports only), and SMDS (SSI-DTE and DXI/SNI ports). See “Viewing Congestion Control Attributes” on page 6-10 for more information.
Trap Control	Frame Relay (all port types), Multilink Frame Relay Trunks, Direct Line Trunks, ATM Direct Trunks (B-STDX ports only), ISDN (all port types), SMDS (all port types), and Ethernet. See “Viewing Trap Control Attributes” on page 6-12 for more information.

Other attributes are specific to individual network services. Table 6-4 lists these attributes and the service they support.

Table 6-4. Service-specific Logical Port Attributes

Attribute	Service Supported
ATM	ATM (see “Viewing ATM UNI/NNI Attributes” on page 7-3 for more information).
ATM FCP	ATM (see “Viewing ATM FCP Attributes” on page 7-24 for more information).
ILMI/Signaling/OAM	ATM (see “Viewing ILMI/Signaling/OAM Attributes” on page 7-7 for more information).
PNNI Parameters	ATM (see “Viewing PNNI Logical Port and Node Parameters” on page 7-14 for more information).
Opt Trunk VPI Range	ATM (see “Viewing OPTimum Trunk VPI Range Attributes” on page 7-37 for more information).
SVC VPI/VCI Range	ATM (see “Viewing SVC VPI/VCI Range Attributes” on page 7-26 for more information).
Traffic Descriptors	ATM (see “Viewing Traffic Descriptor Attributes” on page 7-33 for more information).
Discard/Congestion Mapping	ATM-to-Frame Internetworking (see “Viewing Discard/Congestion Mapping Attributes” on page 7-38 for more information).

Table 6-4. Service-specific Logical Port Attributes (Continued)

Attribute	Service Supported
SVC Parameters	ATM (see "Viewing SVC Parameters" on page 7-27 for more information) and Frame Relay (See "Viewing Frame Relay SVC Parameters" on page 9-9 for more information).
SVC Routing Priorities	ATM (see "Viewing SVC Routing Priorities" on page 7-31 for more information) and Frame Relay (See "Viewing SVC Routing Priorities" on page 9-12 for more information).
Frame Relay SVC	Frame Relay (see "Viewing Frame Relay SVC Attributes" on page 9-7 for more information).
Link Management	Frame Relay (see "Viewing Link Management Attributes" on page 9-2 for more information).
Priority Frame	Frame Relay (see "Viewing Priority Frame Attributes" on page 9-5 for more information).
Ethernet Frame	IP (see "Viewing Ethernet Logical Ports" on page 8-81 for more information).
SMDS	SMDS (see "Viewing SMDS Logical Port Attributes" on page 10-1 for more information).
ISDN	ISDN (see Chapter 11, "Monitoring ISDN" for more information).
Authentication	ISDN (see Chapter 11, "Monitoring ISDN" for more information).

To view logical port attributes, from the View Attributes option menu on the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2), select the attribute type you want to view. The attribute fields then appear on the Show All Logical Ports in Switch dialog box. The default attribute type is "Administrative."

Viewing Administrative Attributes

Table 6-5 describes logical port administrative attribute fields. Note that all of these fields do not necessarily apply to all logical ports. If a field is grayed out or does not appear at all, then the field does not apply to the logical port you are monitoring.

Table 6-5. Administrative Attributes Fields

Field	Displays...
Logical Port Name	The name of the logical port.
Be CIR: Routing Factors (1/100s)	The circuit priority for OSPF. The CIR Be/Routing value represents the UNI bandwidth percentage on all configured zero CIR circuits. Valid values range from 50 (default) to 100 percent.
MLFR Trunk Bundle Name	*(Multilink Frame Relay (MLFR) member logical ports only)* The name of the MLFR trunk bundle to which the member belongs. See “Monitoring Multilink Frame Relay” on page 9-19 for more information on MLFR.
Bit Stuffing	Whether bit stuffing is enabled for the selected logical port. This parameter applies only to logical ports associated with physical ports on T1/E1 and DSX-1 modules.
CDV (microsec)	*(ATM, Optimum Cell Trunks only)* The maximum cell delay variation (in microseconds) for this logical port. This value only applies to constant bit rate (CBR) traffic and specifies the maximum variation in time delays between cells going out of this logical port. The usage parameter control (UPC) uses this value to police the requested traffic descriptor. The default value is 684 for logical ports associated with DS3 physical ports, or 191 for logical ports associated with OC3c physical ports. To change the default, you need to know the maximum CDV for PVCs on this port, as well as the traffic requirements of the hardware on the other end of the connection.
Can Backup Service Names	A value of *Yes* or *No* to specify whether this logical port can be backed up to a service name binding. If the logical port is to be used to implement APS Resilient UNI, this field displays *Yes*. See “Viewing Physical Port Redundancy” on page 2-66 for more information on APS Resilient UNI.
VP Shaping Rate	(*VP Shaping for CBX 500 ATM IOMs only*) The VP shaping rate configured for the logical port. The shaper uses the VP shaping rate to determine the maximum rate at which cells are transmitted. In effect, the VP shaping rate acts as the peak cell rate (PCR). A shaper implements shaping, which is a technique that the CBX 500 ATM Flow-Control Processor (FCP) uses to control the transmission rate of cells in an ATM network. The shaper is contained in the chip on the ATM FCP. ATM FCPs support VP shaping only. With VP shaping, you provision one rate (the VP shaping rate) for each VP. The switch then schedules the aggregate traffic of each VP with this rate.
VP Shaping	(*VP Shaping in CBX 500 ATM IOMs only*) A value of *Enabled* if VP shaping is enabled; displays *Disabled* if VP shaping is disabled. The CBX 500 must have the ATM FCP configured in order to enable VP shaping.

Table 6-5. Administrative Attributes Fields (Continued)

Field	Displays...
Shaper ID	(*VP/VC Shaping in B-STDX 9000 ATM IWU/CS IOMs only*) The identifier of the shaper configured for the logical port. A shaper implements shaping, which is a technique that the ATM IWU IOM or the ATM CS IOM uses to control the transmission rate of cells in an ATM network. The shaper is contained in the chip on the ATM IWU IOM or ATM CS IOM. Each chip supports 15 user-configurable shapers, and each shaper can have multiple virtual circuits assigned to it. For ATM direct trunk logical ports associated with ATM IWU/CS IOMs and ATM OPTimum trunk logical ports associated with ATM IWU/CS IOMs, this field is blank. The switch dynamically selects a shaper for each circuit routed over these trunks.
Shaper Priority	(*VP/VC Shaping in B-STDX 9000 ATM IWU/CS IOMs only*) The priority assigned to the shaper. The switch services a shaper's circuits only if no higher priority shapers are waiting to be served. Priority ranges from 0 (the highest priority) to 15 (the lowest priority). For ATM direct trunk logical ports associated with ATM IWU/CS IOMs and ATM OPTimum trunk logical ports associated with ATM IWU/CS IOMs, this field is blank. The switch dynamically selects a shaper for each circuit routed over these trunks.
Sustainable Cell Rate (cells/sec)	(*VP/VC Shaping in B-STDX 9000 ATM IWU/CS IOMs only*) The sustainable cell rate (SCR). The SCR defines the average rate, in cells per second, at which the shaper transmits cells. The SCR must be less than or equal to the peak cell rate (PCR) for the shaper. If the SCR is less than the PCR, the shaping algorithm uses the maximum burst size (MBS) value as a credit mechanism to allow cells to be transmitted at the PCR. For ATM direct trunk logical ports associated with ATM IWU/CS IOMs and ATM OPTimum trunk logical ports associated with ATM IWU/CS IOMs, this field is blank. The switch dynamically selects a shaper for each circuit routed over these trunks.
Shaper Type	(*VP/VC Shaping in B-STDX 9000 ATM IWU/CS IOMs only*) The type of shaping configured for the logical port. Possible values are: *VC* – Shaping is performed on a circuit-by-circuit basis for each circuit assigned to the shaper. *VP* – Shaping is performed on an aggregate (that is, virtual path) basis for all of the circuits assigned to the shaper.
Admin Status	The logical port status values. A value of *Up* indicates that the logical port is activated. A value of *Down* indicates that the port has never been activated or that the logical port is offline so that diagnostics can be run to test the port. A logical port with an admin status of *Down* is not operational.
Net Overflow	A value of *Public* if the customer (on a private network) is allowed to use a public trunk in the event of overflow or trunk failure. *Restrict* if the customer is restricted to its own private network. ***Note:*** *If the Net Overflow value is Restrict, the customer must have a redundancy plan in place. If not, network failure will result in the event a trunk goes down.*

Table 6-5. Administrative Attributes Fields (Continued)

Field	Displays...
CRC Checking	*(HSSI modules only)* The type of cyclic redundancy check performed on incoming data. Data is checked in either 4K (CRC 16) or 8K (CRC 32) frames.
Is Template	A value of *Yes* or *No* to indicate whether you can use this logical port configuration as a template.
Peak Cell Rate (cells/sec)	(*VP/VC Shaping in B-STDX 9000 ATM IWU/CS IOMs only*) The peak cell rate (PCR). The PCR defines the maximum rate, in cells per second, at which the shaper transmits cells. The PCR must be greater than or equal to the SCR for the shaper. If the PCR is greater than the SCR, then the shaping algorithm uses the maximum burst size (MBS) value as a credit mechanism to allow cells to be transmitted at the PCR. For ATM direct trunk logical ports associated with ATM IWU/CS IOMs and ATM OPTimum trunk logical ports associated with ATM IWU/CS IOMs, this field is blank. The switch dynamically selects a shaper for each circuit routed over these trunks.
CIR Oversubscription	*(Frame Relay UNI/NNI logical ports only) Yes* or *No* to indicate whether Committed Information Rate (CIR) oversubscription is enabled. The CIR is the rate at which the network transfers information under normal operating conditions for each circuit that uses the logical port. If CIR oversubscription is enabled (Yes), the NMS calculates the sum of the CIRs of all the circuits that use the logical port, and then determines whether the sum exceeds the threshold set by the CIR oversubscribed percentage. If you try to configure circuits that exceed the threshold, the NMS informs you. For example, if you set the CIR oversubscribed percentage to 100 percent, and you are about to oversubscribe by 110 percent, the NMS informs you that you are about to exceed the threshold.
CIR Oversubscribed Percentage	*(Frame Relay UNI/NNI logical ports only)* The percentage by which the total CIR for all the circuits that use the logical port may be oversubscribed.
Bandwidth (Kbps)	The bandwidth supported for the selected logical port.
Maximum Burst Size (cells)	(*VP/VC Shaping in B-STDX 9000 ATM IWU/CS IOMs only*) The maximum burst size (MBS) for the shaper, in number of cells. This value determines the maximum number of cells that can be transmitted at the PCR. For ATM direct trunk logical ports associated with ATM IWU/CS IOMs and ATM OPTimum trunk logical ports associated with ATM IWU/CS IOMs, this field is blank. The switch dynamically selects a shaper for each circuit routed over these trunks.
Allocated Channels	*(Logical ports associated with channelized IOMs only)* The channels allocated to the logical port.

Viewing Congestion Control Attributes

Table 6-6 describes congestion control attribute fields.

Table 6-6. Congestion Control Attributes Fields

Field	Displays...
Closed Loop Enabled	A value of *On* or *Off* to indicate whether the specified congestion control values are applied. The default value for this field is *Off*.
Mild Thrhld	The mild threshold value which determines how the switch reacts to congestion at the mild threshold state.
Bad PVC Factor	The factor used to determine the threshold for bad PVC detection. Values range from 0 through 32.
Check Interval	The time interval (in seconds) between two successive congestive-state checks. The default value for this field is 1.
CLLM Thrhld None	(*Frame Relay UNI/NNI logical ports only*) The threshold percentage value (from 1 to 100) of Backward Explicit Congestion Notification (BECN) frames received on any virtual circuit on this port. If the percentage of BECN frames received on any virtual circuit is *less than* this threshold value, the virtual circuit is in a non-congested state. If the percentage of BECN frames received on any virtual circuit *exceeds* this threshold value, *but does not exceed* the value of CLLM Thrhld Mild, the virtual circuit is in a mild congested state. See “Monitoring CLLM Congestion Notification” on page 9-22 for more information.
CLLM Admin State	(*Frame Relay UNI/NNI logical ports only*) The state of Consolidated Link Layer Management (CLLM) notification for the logical port: *Enabled* or *Disabled*. See “Monitoring CLLM Congestion Notification” on page 9-22 for more information.
Sev Thrhld (56 Byte)	The severe threshold value which determines how the switch reacts to congestion at the severe threshold state.
Amber Pm (%)	A value that controls the reduction percentage of the excess burst size (Be) when mild congestion occurs. The default is 50.
Clear Delay	The time delay (in seconds) before a congestion clearance message is sent when the congested port becomes less congested. The default value for this field is 3.
CLLM Thrhld Mild	(*Frame Relay UNI/NNI logical ports only*) The threshold percentage value (from 1 to 100) of BECN frames received on any virtual circuit on this port. If the percentage of BECN frames received on any virtual circuit *exceeds* this threshold value, the virtual circuit is in an absolute congested state. See “Monitoring CLLM Congestion Notification” on page 9-22 for more information.

Table 6-6. Congestion Control Attributes Fields (Continued)

Field	Displays...
Call Admission Control	*(Frame Relay UNI logical ports only)* One of the following: *Enabled* – Call Admission Control (CAC) is enabled. The logical port rejects a circuit creation request if there is not enough available bandwidth. *Disabled* – CAC is disabled. You effectively disable Ascend's Call Master Connection Admission Control function on the logical port. The logical port attempts to create a circuit even if there is not enough available bandwidth (for VFR-NRT and UFR queries only).
Abs Thrhld (56 Byte)	The absolute congestion threshold value, which is specified in units of data buffers queued for transmission.
Amber Ps (%)	A value that controls the reduction percentage of the excess burst size (Be) when severe congestion occurs. The default value for this field is 100. If 100 is used, all amber packets are discarded.
CLLM Interval	(*Frame Relay UNI/NNI logical ports only*) The time duration (in seconds) between two consecutive CLLM messages sent over the logical port. The CLLM message is sent as long as at least one virtual circuit on the logical port remains in a congested state. See "Monitoring CLLM Congestion Notification" on page 9-22 for more information.

Viewing Trap Control Attributes

Table 6-7 describes logical port trap-control attribute fields.

Table 6-7. Trap-Control Attributes Fields

Field	Displays...
Congestion Threshold (%)	A value from 0 to 100; the default is 0. If the rate of congestion over a one-minute period exceeds the threshold percentage specified, a trap is sent to the NMS. When you configure the logical port, you can adjust this value depending on how sensitive your network needs to be to congestion. Setting this value low generates a trap at the first sign of congestion; setting this value high generates a trap only for serious network congestion. A default value of 0 disables the congestion threshold feature, and no congestion traps are generated for the logical port.
Frame Err/min Threshold	The configured threshold of frame errors on the logical port that triggers a trap to be sent to the NMS. The default value is 0, which disables trap generation until you set a non-zero value. The range of values for this field is 0 to 16384.
SMDS PDU Viol Threshold (0 - 255)	The configured threshold of SMDS PDU violations. The default value is 0. The range of values for this field is 0 to 255.
SMDS PDU Violation Traps	A value of *Enabled* specifying that the NMS issues traps for PDU violations. An SMDS PDU violation can be either an SIP3 SMDS address failure or an invalid DXI2 frame header. These errors indicate that incoming frames are bad, which usually means that there are problems with the CPE configuration. A value of *Disabled* specifies that the NMS will not issue traps for SMDS PDU violations.

Viewing QoS Parameters

This section describes how to view the QoS parameters for ATM and Frame Relay logical ports. These parameters enable you to view the bandwidth and routing metrics (if applicable) for the various QoS classes.

To view QoS parameters:

1. From the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2), select Options ⇒ QoS Parameters.
2. Choose View. The Show Logical Port QoS Parameters dialog box appears (see Figure 6-2 and Figure 6-3).

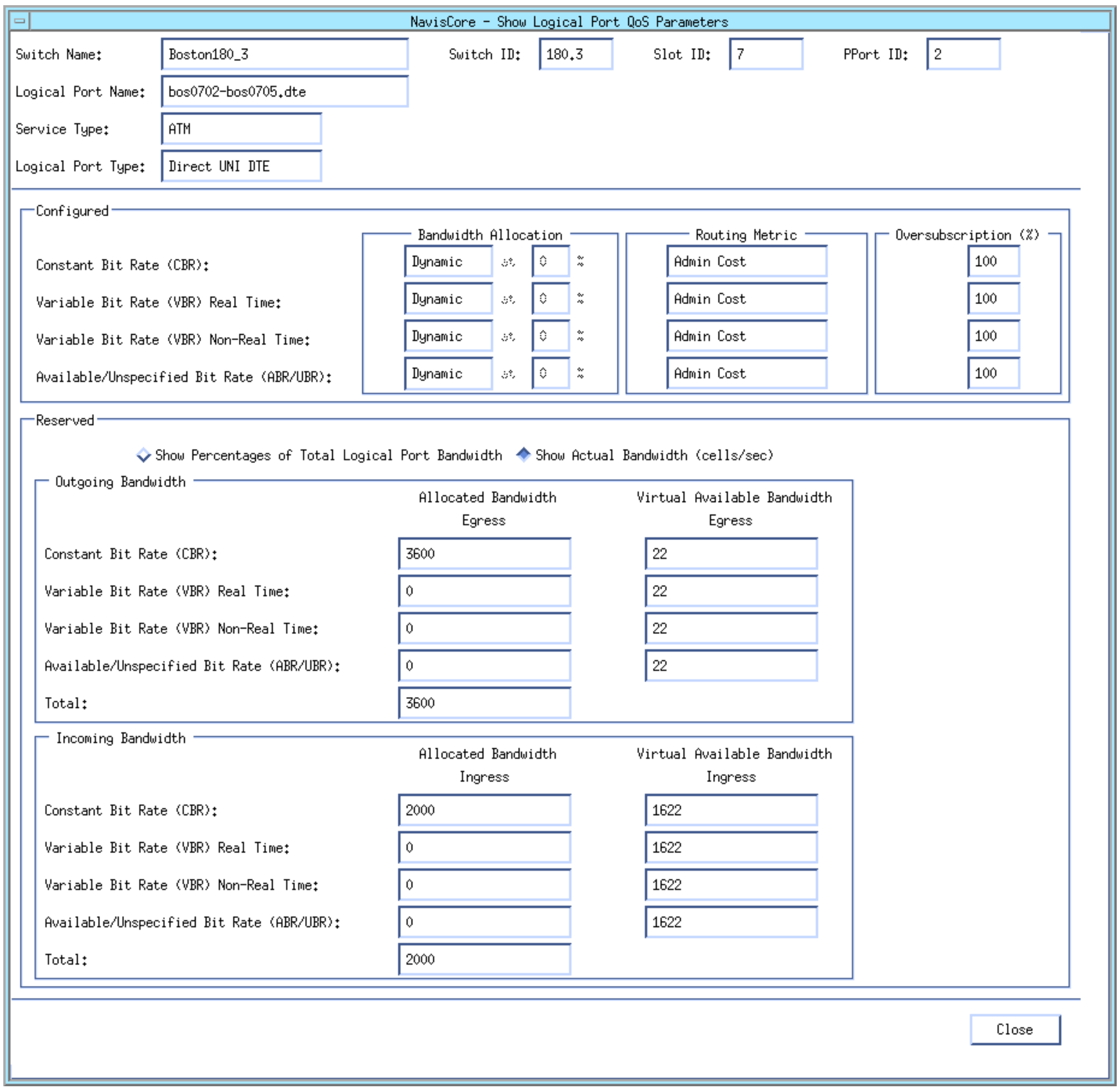


Figure 6-2. Show Logical Port QoS Parameters Dialog Box (ATM)

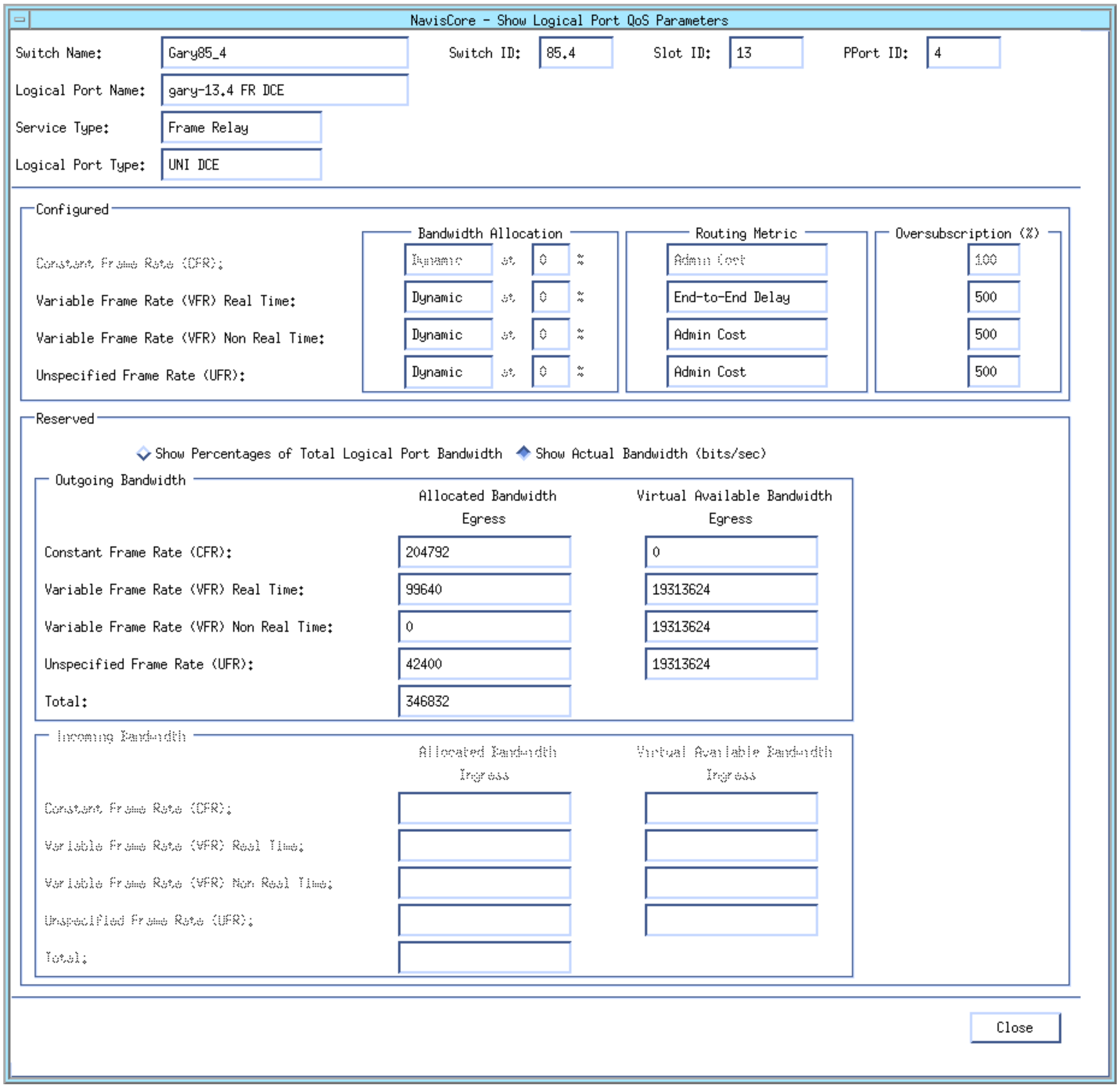


Figure 6-3. Show Logical Port QoS Parameters Dialog Box (Frame Relay)

Two buttons on the dialog box enable you to toggle between two modes: the actual bandwidth and the percentages of total logical port bandwidth. When the dialog box first appears, it displays the actual bandwidth.

3. To view the percentages of total logical port bandwidth, choose the Show Percentages of Total Logical Port Bandwidth button (see Figure 6-4 and Figure 6-5).

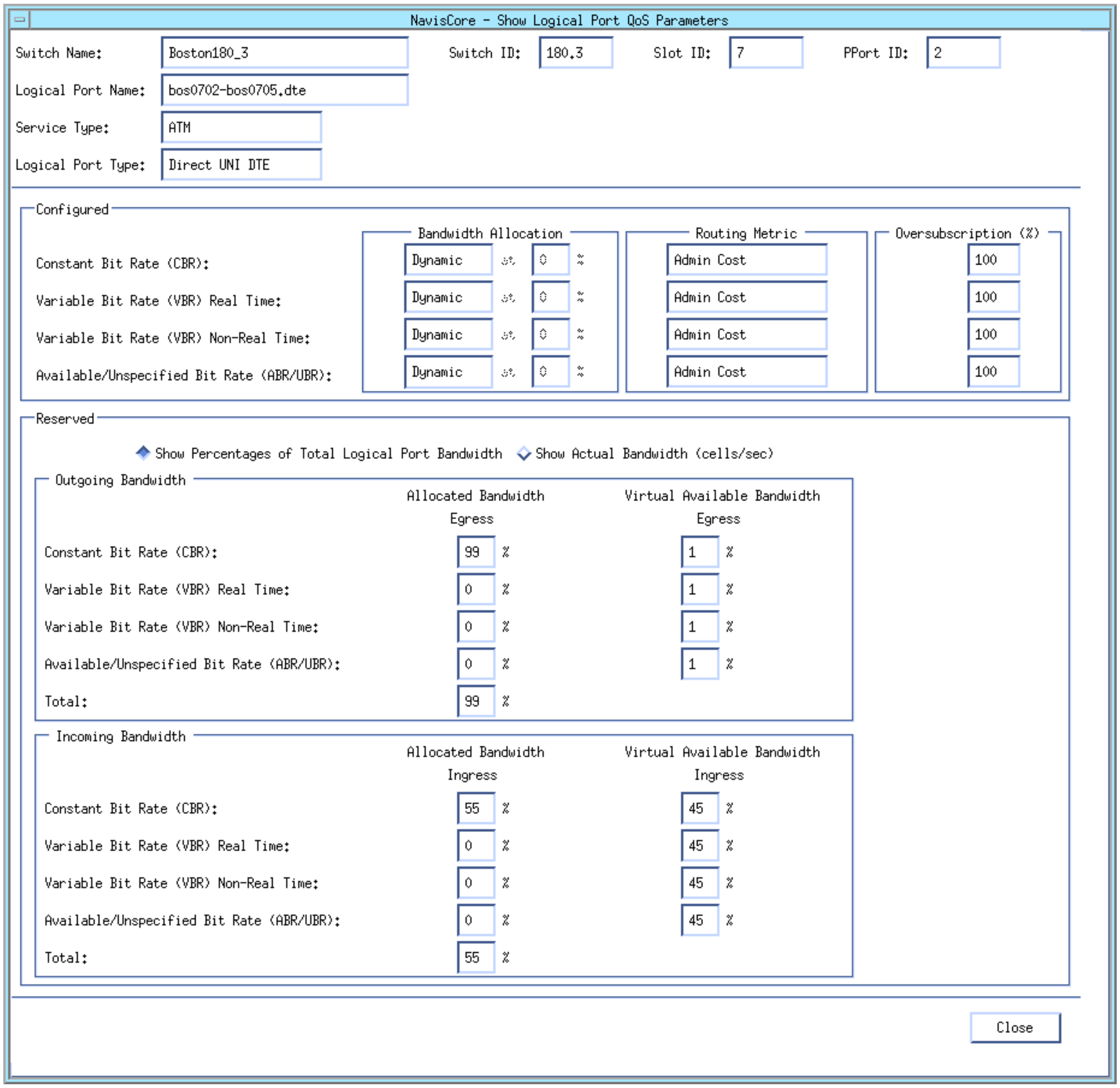


Figure 6-4. Percentages of Logical Port Bandwidth (ATM)

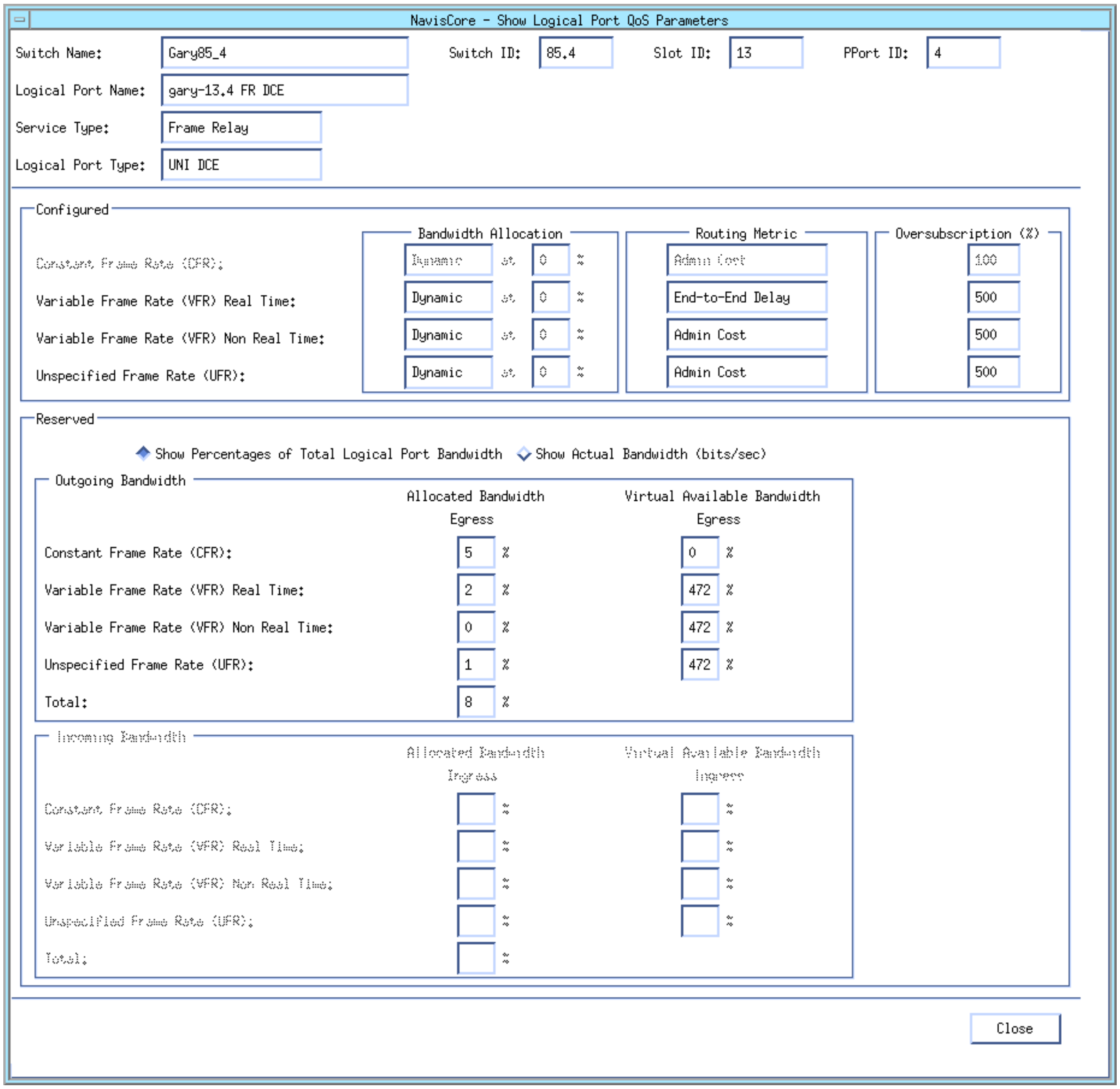


Figure 6-5. Percentages of Logical Port Bandwidth (Frame Relay)

Table 6-8 describes the dialog box fields.

Table 6-8. Show Logical Port QoS Parameters Fields

Field	Displays...
Switch Name	The name of the switch.
Switch ID	The switch ID number, which consists of the subnetwork number and the host number from the in-band IP address of the switch in the internal trunk IP network. For example, “44.5” means that the subnetwork number in the IP address is “44” and the host number is “5.”
Slot ID	The slot number of the module you are monitoring.
PPort ID	The physical port number.
Logical Port Name	The logical-port name.
Service Type	The service type.
Logical Port Type	The logical-port type (for example, Direct Trunk).
Configured – The configured QoS values (CBR, VBR-RT, VFR-RT, VBR-NRT, VFR-NRT, ABR/UBR, UFR) for the logical port:	
Bandwidth Allocation	A value of *Dynamic* or *Fixed* for each service class. *Dynamic* enables the bandwidth allocation to change dynamically according to bandwidth demands. Dynamic bandwidth allocation pools the remaining bandwidth for this logical port. This includes bandwidth that has not already been allocated to a specific queue or assigned to a connection. *Fixed* specifies the percentage of bandwidth that is reserved for the service class. If all four service classes are set to Fixed, all four values should equal 100% bandwidth.
Routing Metric	The routing metric configured for the logical port. Routing metrics allow the switch to select less congested paths and avoid congested paths when transferring data. Options include: *Cell/Frame Delay Variation* – Measures the average variation in delay between one cell/frame and the next, measured in fractions of a second. When emulating a circuit, cell/frame delay variation measurements allow the network to determine if cells are arriving too fast or too slow. *End-to-End Delay* – Measures the time it takes a cell/frame to get from one end of a connection to the other. *Admin Cost* – Measures the administrative cost associated with the logical port. The administrative cost is specified by the administrator, enabling you to adjust path selection manually.

Table 6-8. Show Logical Port QoS Parameters Fields (Continued)

Field	Displays...
Oversubscription (%)	A minimum value of 100% to indicate the virtual bandwidth available for a service class. A value of 100% ensures that the port will deliver all user data for that service class without unanticipated delays or excessive cell loss. A value of 200% effectively doubles the virtual bandwidth available for that service class. However, if all network traffic attempts to use the network resources at precisely the same time (for example, during multiple file transfer sessions over the same trunk), some traffic may be delayed or dropped. ***Note:*** *The Oversubscription value for CBR is always set at 100% and cannot be modified.*
Outgoing Bandwidth (Reserved) – For each ATM or Frame Relay QoS class, this frame of the dialog box displays the egress values for allocated bandwidth and virtual available bandwidth. These bandwidth values appear as a percentage of total logical port bandwidth or as the actual bandwidth (in frames or cells per second), depending on the selected mode (“Show Percentages of Total Logical Port Bandwidth” or “Show Actual Bandwidth”).	
Constant Bit Rate *(ATM only)*	The allocated bandwidth and virtual bandwidth egress values assigned to the CBR QoS class. This class handles digital information, such as video and digitized voice, which must be represented by a continuous stream of bits. CBR traffic requires guaranteed throughput rates and service levels.
Constant Frame Rate *(Frame Relay only)*	The allocated bandwidth and virtual bandwidth egress values assigned to control traffic, which is not a QoS class that you can configure.
Variable (Bit/Frame) Rate (VBR/VFR) Real Time	The allocated bandwidth and virtual bandwidth egress values assigned to either the VBR-RT or VFR-RT QoS class. These classes are designed for packaging special delay-sensitive applications, such as packet video, that require low cell/frame delay variation between endpoints.
Variable (Bit/Frame) Rate (VBR/VFR) Non-Real Time	The allocated bandwidth and virtual bandwidth egress values assigned to either the VBR-NRT or VFR-NRT QoS class. These classes handle packaging for transfer of long, bursty data streams over a pre-established connection. These classes are also used for short, bursty data, such as LAN traffic. CPE protocols adjust for any delay or loss incurred through the use of VBR-NRT or VFR-NRT.
Available/Unspecified (Bit/Frame) Rate (ABR/UBR/UFR)	The allocated bandwidth and virtual bandwidth egress values assigned to the ABR/UBR or UFR QoS class. These classes are primarily used for LAN traffic. The CPE should compensate for any traffic delay or loss.
Total	The total allocated egress bandwidth.
Incoming Bandwidth (Reserved) – For each ATM QoS class, this frame of the dialog box displays the ingress values for allocated bandwidth and virtual available bandwidth. (Note that ingress values do not apply to Frame Relay logical ports.) These bandwidth values appear as a percentage of total logical port bandwidth or as the actual bandwidth (in frames or cells per second), depending on the selected mode (“Show Percentages of Total Logical Port Bandwidth” or “Show Actual Bandwidth”).	
Constant Bit Rate	The allocated bandwidth and virtual bandwidth ingress values assigned to the CBR QoS class.

Table 6-8. Show Logical Port QoS Parameters Fields (Continued)

Field	Displays...
Variable Bit Rate (VBR) Real Time	The allocated bandwidth and virtual bandwidth ingress values assigned to the VBR-RT QoS class.
Variable Bit Rate (VBR) Non-Real Time	The allocated bandwidth and virtual bandwidth ingress values assigned to the VBR-NRT QoS class.
Available/Unspecified Bit Rate (ABR/UBR)	The allocated bandwidth and virtual bandwidth ingress values assigned to the ABR/UBR QoS class.
Total	The total allocated ingress bandwidth.

4. When you finish viewing QoS parameters, choose Close to return to the Show All Logical Ports dialog box.

Viewing Logical Port Summary Statistics

You can view summary statistics for a logical port. Statistics vary, depending on the service configured for the port. See the following chapters for information on logical port summary statistics.

ATM — Chapter 7, "Monitoring ATM Logical Ports."

IP — Chapter 8, "Monitoring IP."

Frame Relay — Chapter 9, "Monitoring Frame Relay Logical Ports."

SMDS — Chapter 10, "Monitoring SMDS."

ISDN — Chapter 11, "Monitoring ISDN."

Viewing All Logical Ports in a Physical Port

To view the logical ports for a selected physical port:

1. On the network map, double-click on the appropriate switch object. The system displays the NavisCore Switch Back Panel dialog box.
2. Double-click on the physical port that you want to monitor. The system displays a dialog box enabling you to view the attributes of the selected physical port.
3. Choose the Logical Port command button. The Show All Logical Ports in PPort dialog box appears (see Figure 6-6).

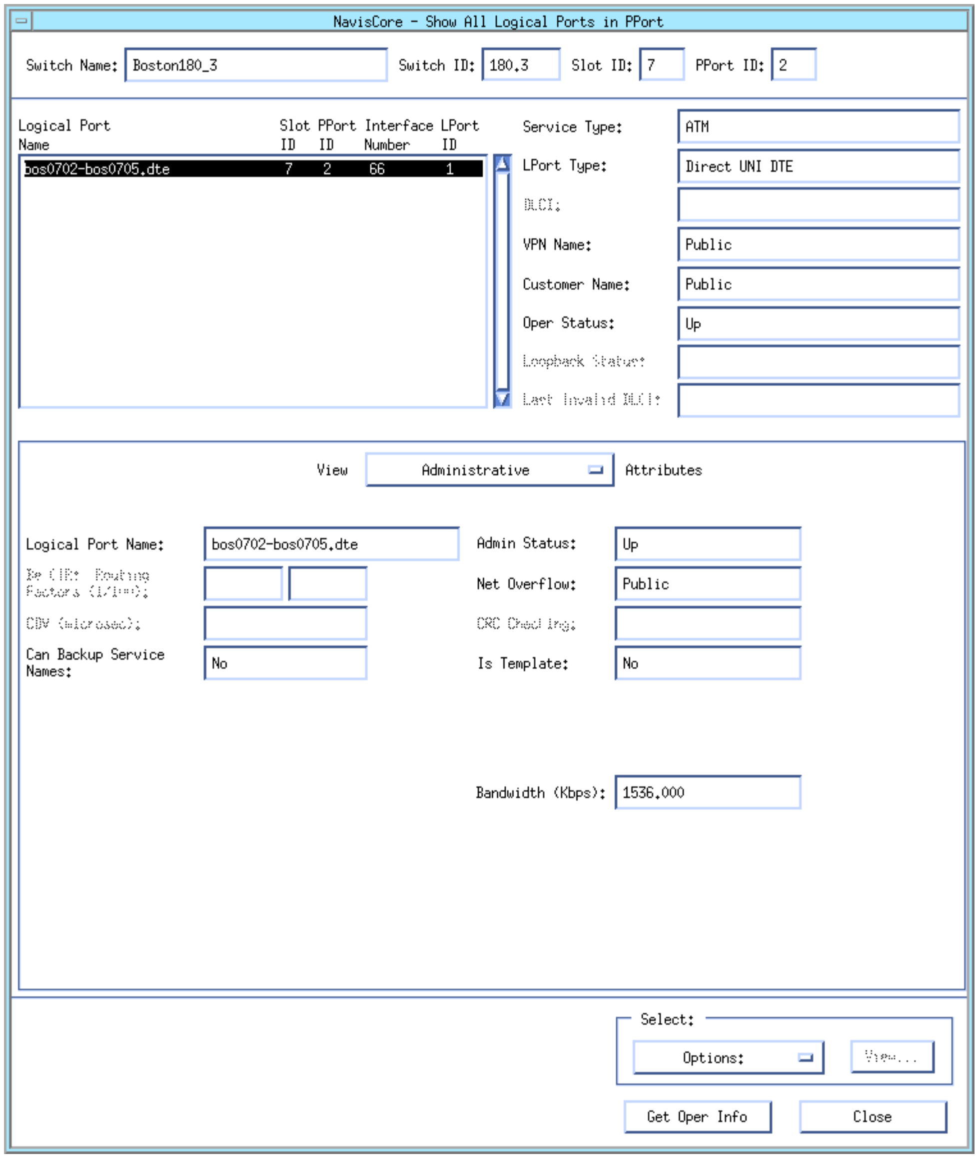


Figure 6-6. Show All Logical Ports in PPort Dialog Box

The dialog box displays information about the physical port and associated logical ports. You can perform the same management tasks from this dialog box as you can from the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).

7

Monitoring ATM Logical Ports

This chapter describes monitoring ATM-specific logical port attributes and statistics. See Chapter 13, “Monitoring ATM Circuits” for information on monitoring ATM circuits.

Viewing ATM-Specific Logical Port Attributes

You can access the dialog boxes for viewing ATM logical port attributes in two ways:

- From the Monitor menu. This chapter presents this method of accessing ATM logical port attribute dialog boxes.
- From the View Physical Port Attributes dialog box for the physical port to which the ATM logical port is mapped. See “Reviewing Physical Port Status” on page 2-44 for information on this method.

To view ATM-specific logical port attributes from the Monitor menu:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1 on page 6-2).
3. Select the appropriate logical port name from the list box on the left.
4. Choose the View Attributes option menu to view various attributes for the logical port. Only the selections that apply to the selected logical port appear. These selections include attributes that are not specific to ATM, and attributes that are specific to ATM.

   See Chapter 6, “Monitoring Logical Ports” for information on attributes that are not specific to ATM.

Table 7-1 identifies each of the ATM-specific attribute types you can select, along with a reference to the table that describes the attribute fields.

Table 7-1. ATM-Specific Logical Port Attribute Types

For Information About...	See...
ATM	Table 7-2 on page 7-4
ILMI/Signaling/OAM	Table 7-3 on page 7-8
PNNI Parameters	Table 7-6 on page 7-20
ATM FCP	Table 7-9 on page 7-25
SVC VPI/VCI Range	Table 7-10 on page 7-26
SVC Parameters	Table 7-11 on page 7-27
SVC Routing Priorities	Table 7-14 on page 7-32
Traffic Descriptors (node and card)	Table 7-15 on page 7-35
OPTimum Trunk VPI Range	Table 7-16 on page 7-38
Discard/Congestion Mapping	Table 7-17 on page 7-39

Viewing ATM UNI/NNI Attributes

To view ATM UNI/NNI attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View ATM Attributes. The ATM UNI/NNI attributes fields appear (see Figure 7-1).

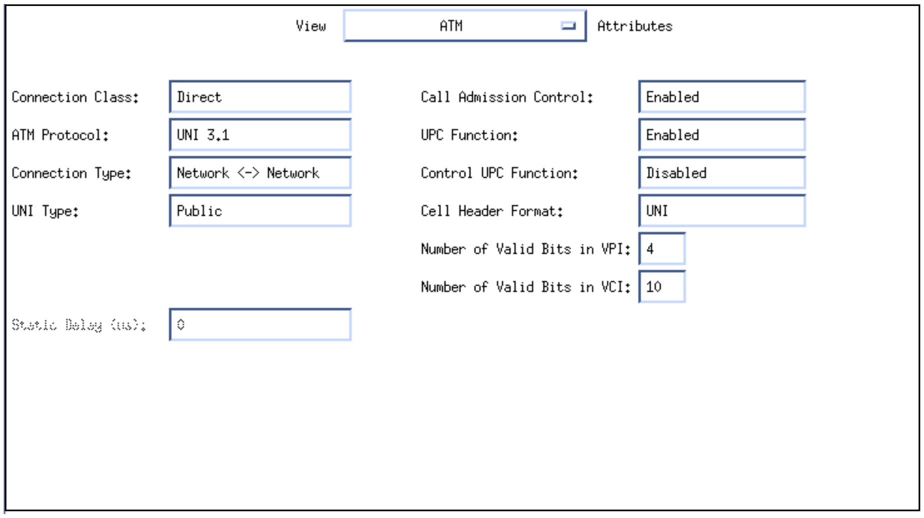


Figure 7-1. ATM UNI/NNI Attributes Fields

Table 7-2 describes the ATM UNI/NNI attributes fields. For additional information on the ATM UNI/NNI attributes, see the *NavisCore ATM Configuration Guide.*

Table 7-2. ATM UNI/NNI Attributes Fields

Field	Applicable Logical Port Type	Displays...
Connection Class	UNI DCE/DTE or NNI	The UNI logical port connection class, either Direct or Virtual. This field is set to Direct when you configure the first UNI/NNI logical port on this physical port. When you configure subsequent UNI/NNI ports on this physical port, this field displays Virtual. For NNI and trunk logical port types, this field defaults to Direct and cannot be changed.
ATM Protocol	All	The ATM protocol. The equipment to which you connect this logical port must support the protocol. One of the following protocols appears: • *UNI 4.0* • *UNI 3.1* • *UNI 3.0* • *IISP 3.1* • *IISP 3.0* • *BICI 1.1* • *PNNI 1.0* • *ITU UNI* The default signaling tuning parameters are based on the ATM protocol specified for the logical port. If you change the signaling tuning parameters for this port, and later change the UNI version, the default signaling tuning parameters for the ATM protocol you select overwrite these changes. For more information on signaling tuning parameters, see the *NavisCore ATM Configuration Guide*.
Connection Type	UNI DCE and NNI	The connection type. Possible connection types include: • *Network <–> Endsystem* – This port connects to a router or host. • *Network <–> Network* – This port connects to another ATM switch.

Table 7-2. ATM UNI/NNI Attributes Fields (Continued)

Field	Applicable Logical Port Type	Displays...
UNI Type	UNI DCE/DTE	The UNI type. This field displays "Public" if at least one end of this connection attaches to a public network. This field displays "Private" if this connection resides completely within a private network.
Static Delay	NNI	The measured, one-way delay for a trunk, from 0 to 167777214 microseconds. If the value is 0, then the Static Delay value is disabled for the trunk. If this value is in use (that is, a non-zero value is set), an SVC originating from this logical port is not routed over a path whose total end-to-end delay exceeds the entered value. This means that if you enable this field and enter in a value of 500 microseconds, the SVC is not routed over a path with a total end-to-end delay that exceeds 500 microseconds. The NMS calculates the total end-to-end delay for a path by using the sum of the end-to-end delays for each trunk in the path. See the *NavisCore ATM Configuration Guide* for more information.
VPI Start	Virtual UNI/NNI	The first virtual path identifier (VPI) in the VPI range. For network-to-network virtual UNI/NNI configurations, the first VPI is used for control channels only (i.e., signaling and ILMI). For network-to-endsystem virtual UNI/NNI configurations, there are no restrictions. Note that this field appears for virtual UNI/NNI logical ports only.
VPI Stop	Virtual UNI	The last VPI in the VPI range. The last VPI is calculated according to the following formula: `VPI Stop <= (2^numvpibits - 1)` where "numvpibits" equals the value in the Number of Valid Bits in VPI field. Note that this field appears for virtual UNI logical ports only.
Call Admission Control	All	One of the following: *Enabled* – Call Admission Control (CAC) is enabled. When enabled (the default), the port rejects a circuit creation request if there is not enough available bandwidth. When disabled, the port attempts to create a circuit even if there is not enough available bandwidth (for VBR-NRT queue only). *Disabled* – CAC is disabled.

Table 7-2. ATM UNI/NNI Attributes Fields (Continued)

Field	Applicable Logical Port Type	Displays...
UPC Function	UNI DCE/DTE	One of the following: *Enabled* (default) – The Usage Parameter Control (UPC) function is enabled for PVCs and SVCs. Cells that do not conform to the traffic parameters are dropped or tagged as they come into the port. *Disabled* – The UPC function is disabled for PVCs and SVCs. All traffic, including non-conforming traffic, passes in through the port. If you disable the UPC function on a logical port, quality of service is no longer guaranteed on the network due to the potential for increasing the cell loss ratio on network circuits. For this reason, *Ascend recommends that you leave the UPC function enabled on all logical ports*. This function can also be enabled or disabled for individual PVCs. If you need to enable or disable the UPC function on a per PVC basis, you must enable or disable the UPC function on the logical port. For more information on UPC traffic parameters, see the *NavisCore ATM Configuration Guide*.
NPC Function	NNI	One of the following: *Enabled* (default) – The Network Parameter Control (NPC) function is enabled. Cells that do not conform to the traffic parameters are dropped or tagged as they come into the port. *Disabled* – The NPC function is disabled. All traffic, including non-conforming traffic, passes in through the port. If you disable the NPC function on a logical port, quality of service is no longer guaranteed on the network due to the potential for increasing the cell loss ratio on network circuits. For this reason, *Ascend recommends that you leave the NPC function enabled on logical ports*. Note that this field appears for NNI logical ports only.
Control UPC Function	UNI DCE/DTE	One of the following: *Enabled* – UPC is enabled for the logical port's control circuits (signaling and ILMI). When enabled, you prevent an attached device from overloading the switch with data on the control circuit. The switch polices the control circuit to configurable traffic characteristics. The attached device typically needs to support per-VC shaping. *Disabled* – UPC is disabled for the logical port's control circuits.

Table 7-2. ATM UNI/NNI Attributes Fields (Continued)

Field	Applicable Logical Port Type	Displays...
Cell Header Format	All	A value that controls the number of VPI bits in the ATM cell header for virtual path connections (VPCs). If the value is UNI, 8 bits of VPI are used. If the value is NNI, 12 bits of VPI are used.
Number of Valid Bits in VPI	All	The number of bits reserved for storing the VPI in the ATM cell header. This field applies to virtual channel connection (VCC) switching only. VPCs have access to the full number of VPI bits (8 or 12, depending on cell header format).
Number of Valid Bits in VCI	All	The number of bits reserved for storing the virtual channel identifier (VCI) in the ATM cell header. This field applies to VCC switching only.

Viewing ILMI/Signaling/OAM Attributes

To view ILMI/Signaling/OAM attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View ILMI/Signaling/OAM Attributes. The ILMI/Signaling/OAM attributes fields appear (see Figure 7-2).

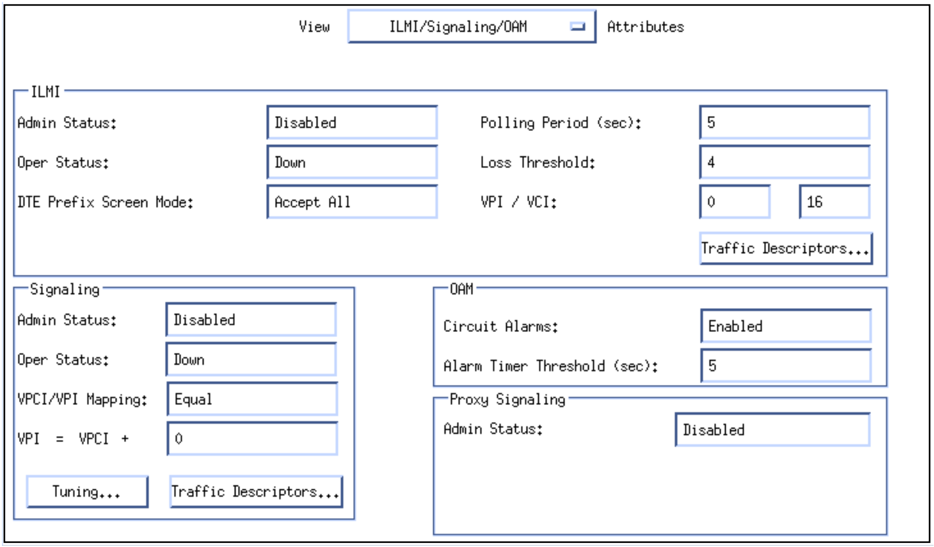


Figure 7-2. ILMI/Signaling/OAM Attributes Fields

The Tuning, Traffic Descriptors, and Show Table buttons allow you to view additional attributes.

The Tuning button allows you to view signaling parameters. See “Viewing Logical Port Signaling Parameters” on page 7-11 for more information on signaling parameters.

The Traffic Descriptors button in the ILMI part of the dialog box allows you to view traffic descriptors configured for ILMI, and the Traffic Descriptors button in the Signaling part of the dialog box allows you to view traffic descriptors configured for signaling. See “Viewing Traffic Descriptor Attributes” on page 7-33 for more information on traffic descriptors.

The Show Table button appears only if you configured a VPCI/VPI mapping value of “Table.” See Table 7-3 for a description of the Show Table button.

Table 7-3 describes the ILMI/Signaling/OAM attributes fields and buttons. For more information on the ILMI/Signaling/OAM attributes, see the *NavisCore ATM Configuration Guide*.

Table 7-3. ILMI/Signaling/OAM Attributes Fields and Buttons

Field/Button	Displays/Function
ILMI Attributes (UNI DCE/DTE and PNNI logical ports only)	
Admin Status	One of the following: *Enabled* – ILMI is enabled for the logical port. *Disabled* – ILMI is disabled for the logical port. If the attached device does not support ILMI, ILMI should be disabled.
Oper Status	The current operational status of the ILMI control circuit.
DTE Prefix Screen Mode (DTE ports)	The various DTE prefix screening modes. Options include: *Accept All* – No screening occurs; accepts all prefixes. *Node Prefix* – Accepts only network prefixes that partially or fully match a configured node prefix. *Port Prefix* – Accepts only network prefixes that partially or fully match a configured port prefix. *Node or Port Prefix* – Accepts only network prefixes that partially or fully match either a configured node prefix or a configured port prefix. *Reject All* – Rejects all network prefixes received from an external network.
Polling Period	The polling period (T) for an ILMI poll. The switch generates an ILMI poll every (T) seconds. The default is 5 seconds.
Loss Threshold	The number of times (K) the logical port will issue an ILMI poll before the link is considered down. If no responses are seen in K x T seconds, the link is considered down. The default is 4.
VPI	The ID of the virtual path for ILMI traffic. The default is 0.

Table 7-3. ILMI/Signaling/OAM Attributes Fields and Buttons (Continued)

Field/Button	Displays/Function
VCI	The ID of the virtual channel for ILMI traffic. The default is 16.
Traffic Descriptors	Choose this command to display ILMI control circuit traffic descriptors. See “Viewing Traffic Descriptor Attributes” on page 7-33 for more information.
Signaling Attributes (UNI DCE/DTE and PNNI logical ports only)	
Admin Status	One of the following: *Enabled* – The logical port supports the UNI signaling protocol. *Disabled* (the default) – The logical port supports PVCs only (that is, you will not create SVCs on the port).
Oper Status	The current operational status of the signaling control circuit.
VPCI/VPI Mapping	The VPCI-to-VPI mapping type used to calculate the VPI (that is, given a VPCI, calculate the VPI). (VPCI stands for virtual path connection identifier.) The VPCI-to-VPI mapping types are as follows: *Equal* – The VPI equals the VPCI (VPI = VPCI). The VPCI offset is 0. *Positive Offset* – The VPI equals the sum of the VPCI and the VPCI offset (VPI = VPCI + Offset). *Negative Offset* – The VPI is calculated by subtracting the VPCI offset from the VPCI (VPI = VPCI - Offset). *Table* – The VPI equals the value of the VPI field in the VPCI table. Each row in this table maps a VPI to a corresponding VPCI, switch, and logical port. Use the Show Table button to display this table. See Table 7-4 for a description of the fields in the VPCI table.
VPI = VPCI (+ or -)	The VPCI offset, which is used to calculate the VPI as described in the previous row. This field does not appear if the VPCI/VPI mapping value is “Table.” In its place, the Show Table button appears.
Show Table	Displays the VPCI table, which maps a VPI to a corresponding VPCI, switch, and logical port. See Table 7-4 for a description of the fields in the VPCI table. This button appears in place of the VPI = VPCI (+ or -) field when the VPCI/VPI mapping value is “Table.” Otherwise, this button does not appear.
Tuning	Displays the Signaling Tuning Parameters dialog box. For information about tuning parameters, see “Viewing Logical Port Signaling Parameters” on page 7-11.
Traffic Descriptors	Displays signaling control circuit traffic descriptors. See “Viewing Traffic Descriptor Attributes” on page 7-33 for more information.

Table 7-3. ILMI/Signaling/OAM Attributes Fields and Buttons (Continued)

Field/Button	Displays/Function
OAM Attributes	
Circuit Alarms	One of the following: *Enabled* – The circuit alarms status is enabled (the default), which allows this logical port to generate OAM AIS alarms. The switch uses these alarms to signal when the circuits have gone down. *Disabled* – The circuit alarms status is disabled, which prevents OAM AIS alarms from being generated on this logical port. See “Testing ATM Circuits” on page 13-90 for more information on OAM.
Alarm Timer Threshold (sec)	The number of seconds a circuit can be down before the switch generates an OAM AIS alarm. The default is 5 seconds. See “Testing ATM Circuits” on page 13-90 for more information on OAM.
Proxy Signaling	
Admin Status	One of the following: *Disabled* – Proxy signaling is disabled. *Agent* – The logical port acts as a proxy signaling agent (PSA). Applies to DCE UNI logical ports only. *Client* – A peer PSA performs signaling on behalf of the logical port. Applies to DCE UNI logical ports only.

Table 7-4 describes the VPCI table fields.

Table 7-4. VPCI Table Fields

Field	Displays...
VPCI	The VPCI that identifies the virtual path connection between the logical port you are monitoring, and the switch and logical port on the other end of the connection.
VPI	The VPI that identifies the virtual path between the logical port you are monitoring, and the switch and logical port on the other end of the connection.
Peer Switch Name	The switch on the other end of the connection.
Peer LPort Index	The index value of the logical port on the other end of the connection.
Row Status	The status of the row (*Active* or *Inactive*).

Viewing Logical Port Signaling Parameters

This section describes the signaling tuning parameters for a logical port. In an ATM network, signaling is responsible for establishing and releasing SVCs. Signaling is used only on ingress and egress ports, including user-to-network, network-to-user, and network-to-network ports.

To view signaling tuning parameters, choose the Tuning button in the Signaling part of the ILMI/Signaling/OAM Attributes dialog box (see Figure 7-2 on page 7-7). The Show Logical Port Signaling Tuning Parameters dialog box appears (see Figure 7-3).

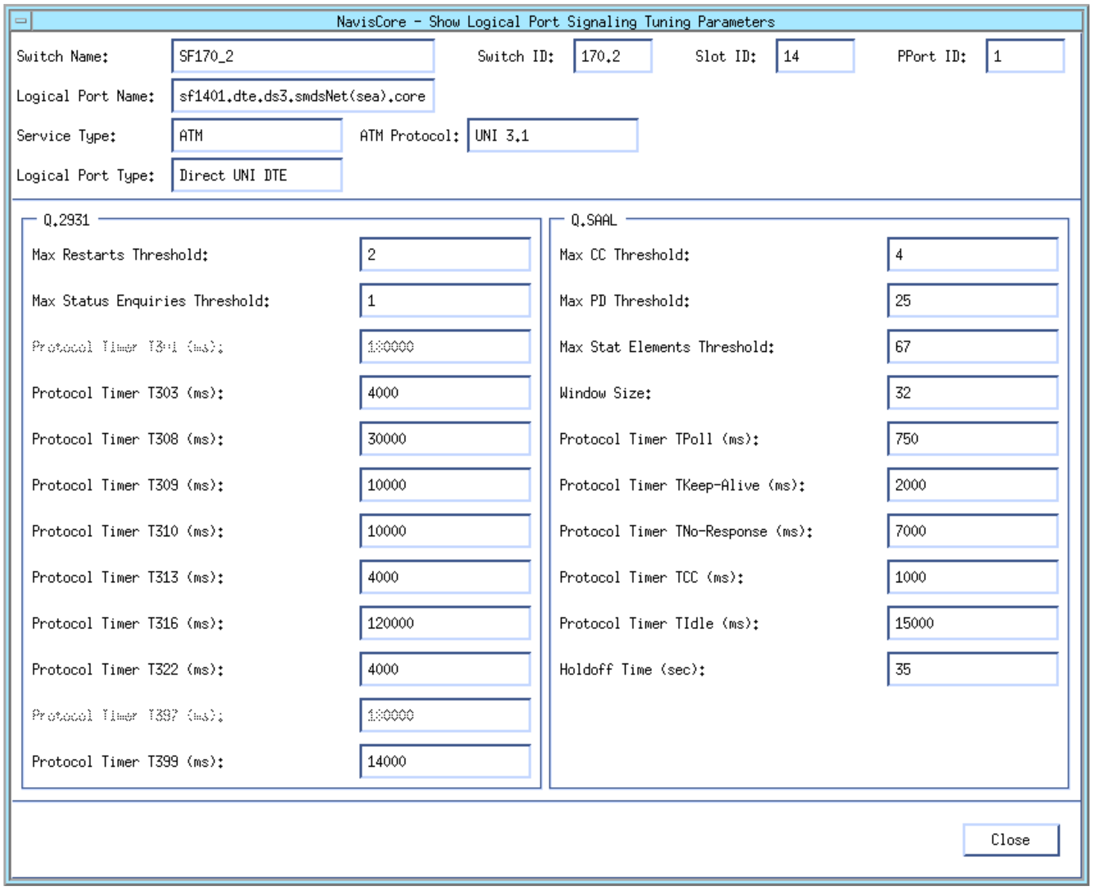


Figure 7-3. Show Logical Port Signaling Tuning Parameters

The Show Logical Port Signaling Tuning Parameters dialog box displays the Q.2931 thresholds and timers, and the Signaling ATM Adaptation Layer (SAAL) protocol data unit (PDU) thresholds and timers. The displayed defaults are based on the selected ATM protocol type for the logical port.

Table 7-5 describes the Show Logical Port Signaling Tuning Parameters fields.

Table 7-5. Show Logical Port Signaling Tuning Parameters Fields

Field	Displays...
Q.2931 (Signaling)	
Max Restarts Threshold	The maximum number of restarts to send without a response.
Max Status Enquiries Threshold	The maximum number of status enquiries that can be unacknowledged before the call is dropped.
Protocol Timer T301 (UNI 4.0, PNNI, Q.2931/Q.2971 protocol only)	The timer on point-to-point circuits used to supervise the alerting process. The T301 timer is set upon receipt of an ALERTING PDU and determines how long to wait for receipt of a CONNECT PDU.
Protocol Timer T303	The amount of time to wait for a response after a SETUP PDU has been sent.
Protocol Timer T308	The amount of time to wait for a response after a RELEASE PDU has been sent.
Protocol Timer T309	The amount of time to wait after an SAAL disconnect before calls are dropped.
Protocol Timer T310	The amount of time to wait for the next response after a CALL PROCEEDING PDU has been received.
Protocol Timer T313	The amount of time to wait for a CONNECT ACK PDU after a CONNECT PDU has been sent. This function is disabled for DCE logical ports.
Protocol Timer T316	The amount of time to wait for a RESTART ACK PDU after a RESTART PDU has been sent.
Protocol Timer T322	The amount of time to wait for a STATUS PDU after a STAT ENQUIRY PDU has been sent.
Protocol Timer T397 (UNI 4.0, PNNI, Q.2931/Q.2971 protocol only)	The amount of time to wait for an ADD PTY ACK PDU after a PARTY ALERTING PDU has been received. (This timer performs an equivalent function to T301 for point-to-multipoint circuits.)
Protocol Timer T398	The amount of time to wait for a DROP PTY ACK PDU after a DROP PTY PDU has been sent.
Protocol Timer T399	The amount of time to wait for a response after an ADD PTY PDU has been sent.
Q.SAAL	
Max CC Threshold	The maximum number of transaction retries for control PDUs.
Max PD Threshold	The maximum number of data PDUs without a POLL. The default is 25.
Max STAT Elements Threshold	The maximum number of missing elements in a STAT PDU. The default is 67.

Table 7-5. Show Logical Port Signaling Tuning Parameters Fields (Continued)

Field	Displays...
Window Size	The maximum number of unacknowledged PDUs that may exist at any time. If this number is reached or exceeded, the switch does not send any more PDUs. Decreasing this value slows down peer signaling; increasing this value speeds up peer signaling. The default is 32.
Protocol Timer TPoll (ms)	How often a poll is sent when the SAAL is active.
Protocol Timer TKeep-Alive (ms)	How often a poll is sent when the SAAL is in the transient state.
Protocol Timer TNo-Response (ms)	The maximum amount of time that can pass without a STATUS PDU being received.
Protocol Timer TCC (ms)	The retry time for control PDUs.
Protocol Timer TIdle (ms)	How often a poll is sent when SAAL is idle. This parameter does not apply to UNI 3.0 connections.
Holdoff Time (sec)	The amount of time, in seconds, that the logical port refrains from re-establishing the ATM signaling connection after you modify a physical port or logical port, or after a physical port alarm is detected. This timer mechanism converts SAAL reset conditions into SAAL failure conditions. The default is 35 seconds.

Viewing PNNI Logical Port and Node Parameters

NavisCore allows you to view Private Network-to-Network Interface (PNNI) logical port configuration parameters and PNNI node configuration parameters. PNNI is a standard designed by the ATM Forum that defines both an ATM routing protocol and an ATM signaling protocol. Ascend supports PNNI on CBX 500 and GX 550 switches. For a detailed explanation of PNNI routing and signaling, see the *ATM Forum Technical Committee Private Network-Network Interface Specification Version 1.0* (af-pnni-0055.000), available from the ATM Forum's web site (http://www.atmforum.com).

About PNNI Routing

This section provides a brief overview of the PNNI routing protocol.

The PNNI routing protocol provides for dynamic routing configuration and a highly scalable routing scheme. In an ATM network, nodes that support PNNI routing are organized into peer groups. Each peer group is identified by a peer group identifier.

On Ascend switches, the peer group identifier appears by default at the beginning of each peer group member's ATM End System Address (AESA). For example, suppose that five CBX 500 switches are in a peer group, and the ID of that peer group is 39999999. This means that 39999999 would appear at the beginning of the AESA of each of the five switches.

> The way in which peer group IDs are configured depends on the vendor implementation.

Peer groups can be organized hierarchically. To accomplish a hierarchical organization of peer groups, each peer group is represented to the next level of the hierarchy by an abstract entity called a logical group node. The functions of the logical group node are performed by a lowest-level node in the peer group called the peer group leader. Members of the peer group communicate to elect the peer group leader based on leadership priority. The member that has the highest leadership priority is chosen to be the peer group leader and becomes the parent of the peer group, which is now referred to as a child peer group.

> For its first release of PNNI routing, Ascend switches do not support PNNI hierarchy, and cannot act as border nodes, peer group leaders, or logical group nodes. Ascend switches can participate in peer group leader election.

As the parent of its child peer group, the logical group node is eligible to join the next highest peer group in the hierarchy, which can be made up of other parents (i.e., logical group nodes) representing other child peer groups and physical nodes. In turn, the members of the next highest peer group in the hierarchy choose a logical group node, which represents them to the third level of the hierarchy — and on up the hierarchical chain, forming a kind of ancestry consisting of children, parents, grandparents, and so on.

Figure 7-4 shows a simple two-tiered PNNI routing hierarchy, with six lowest-level nodes divided into two child peer groups (PG1 and PG2). The logical group nodes that are the parents of each of the child peer groups form a top-tier peer group (PG3). As a result, each logical group node is a member of two groups — its child group and its peer group.

> Peer groups may contain both logical group nodes and lowest-level nodes. For example, in Figure 7-4, a physical node could also be a member of PG3.

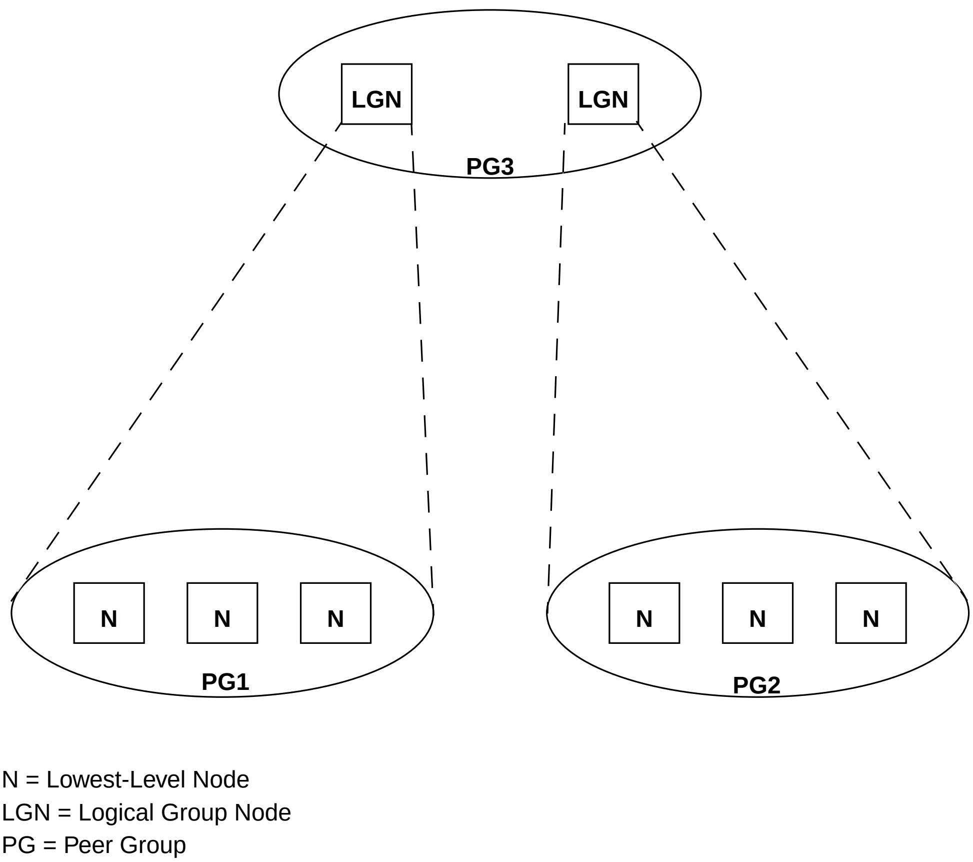


Figure 7-4. Simple PNNI Routing Hierarchy

Neighboring lowest-level nodes within a peer group exchange information to synchronize their topology databases. The topology database contains information on the peer group in which a node resides and information which allows the node to reach destinations in other peer groups. A node receives information about the network beyond the peer group from its peer group leader.

In its role as logical group node, the peer group leader collects routing information from all of the nodes in its child peer group and propagates a summarized version of that information to the higher-level peer group. In turn, the peer group leader receives summarized routing information from its peers and distributes that information to the other nodes in its child group.

This automated process of collection and propagation eliminates the need for manual configuration and maintenance of routing information on network nodes. In effect, PNNI allows network nodes to automatically learn the topology of the network, and use the topological knowledge they acquire to route data to its correct destination.

Figure 7-5 illustrates the flow of PNNI topology information within peer groups and between peer groups. The neighboring nodes in each peer group exchange topology information to synchronize each other’s topology databases. Logical group nodes also propagate information about how to reach their child groups to other logical group nodes.

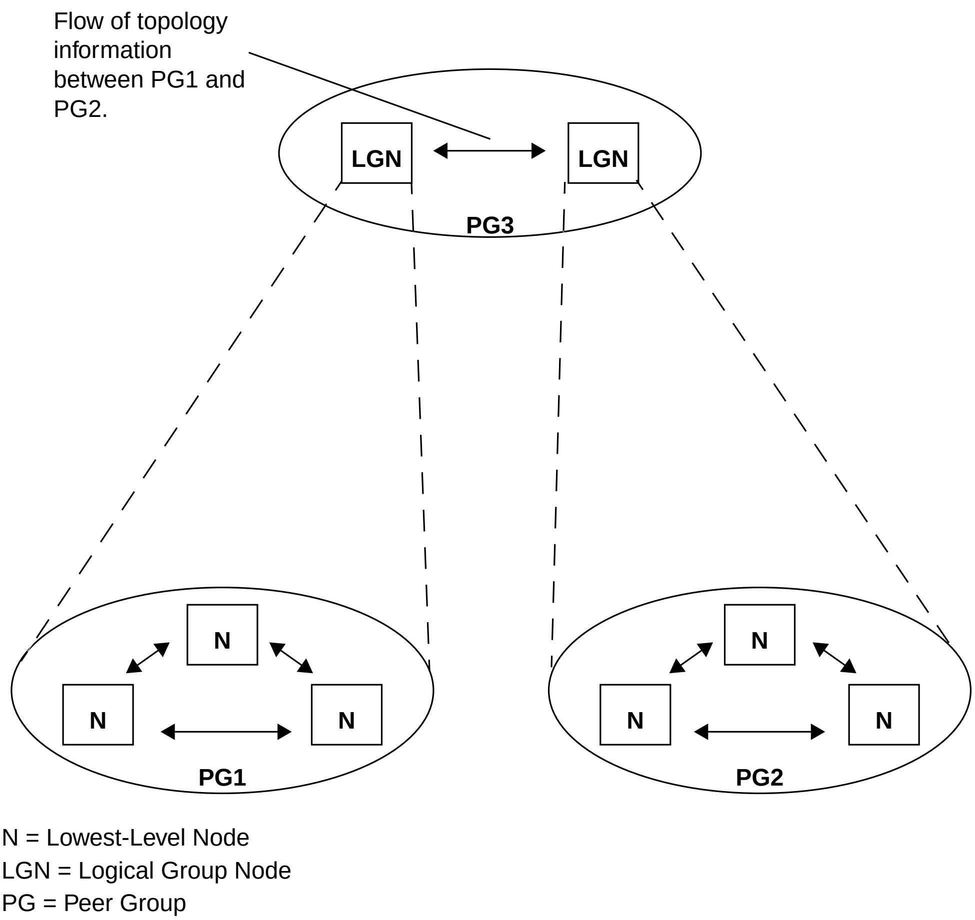


Figure 7-5. Flow of PNNI Topology Information

The following packets carry PNNI control information during exchanges between neighbors:

Hello Packets — Contain information that neighboring nodes exchange to discover and verify each other's identity and to determine the status of the links that connect them.

Database Summary Packets — Contain the identifying information of all PNNI Topology State Elements (PTSEs) in a node's topology database. A PTSE is a collection of PNNI topology information that is sent to all nodes in a peer group. When a node first learns the existence of a neighboring peer node that resides in the same peer group, it initiates a database exchange process in order to synchronize its topology database with its neighbor. When one neighbor sends a database summary packet to another neighbor, the other neighbor responds with its own database summary packet.

PTSE Request Packets — Contain one or more entries that request PTSEs. When a node examines received database summary packets from neighbors and detects one or more missing PTSEs in its topology database, it builds a PTSE request packet. This packet contains a list of IDs that identify the missing PTSEs. The node sends the PTSE request packet to neighbors, which respond with a PTSP.

PNNI Topology State Packets (PTSPs) — Contain one or more PTSEs. A node sends PTSPs when it:

- Detects that its local topology information has changed, in which case it immediately sends PTSP(s) containing information about the change to its neighbors.
- Receives a PTSP from a neighbor that contains new topology information, in which case it propagates the information to other neighbors in PTSP packets.
- Responds to PTSE requests during topology database synchronization.

Note that the first two bullets describe the most common reasons for sending PTSPs. The last bullet describes the least common reason.

PTSE Acknowledgment Packets — Contain acknowledgments of receipt of PTSEs.

When a node receives PTSEs, the receiving node acknowledges receipt by sending one or more PTSE acknowledgment packets.

In Ascend's PNNI implementation, each CBX 500 and GX 550 switch requires a logical port for each of its neighbors. The logical port type is ATM NNI, and the protocol type is PNNI 1.0. For example, each lowest-level node in PG1 in Figure 7-4 would have two ATM NNI logical ports (with protocol type of PNNI) configured — one for each of its neighboring nodes in PG1.

When you configure each logical port, you can assign an administrative weight to each QoS category. This weight allows you to configure the network to favor one path over another path for a given QoS category (when the path constraint for an SVC is the administrative weight). The weights of all the network interfaces along a path are added up, and switches choose the path with the lowest cumulative weight when making routing decisions.

For example, suppose that VBR Real Time traffic has two available paths for reaching a given destination. One path has a weight of 1000 while another path has a weight of 4000. If the call requests VBR-RT QoS and the administrative weight as metrics, the switch will choose the path with the weight of 1000.

About PNNI Signaling

This section provides a brief overview of PNNI signaling.

PNNI signaling allows ATM SVC calls to be set up across a private network that supports the PNNI protocol. It is based on a subset of UNI 4.0 signaling. It does not support some UNI 4.0 signaling features such as leaf-initiated joint capability or user-to-user supplementary service, but adds new features which support the use of PNNI routing for dynamic call setup, and PNNI crankback for the dynamic re-routing of call setups around failed nodes or links or links with insufficient resources.

PNNI signaling makes use of PNNI routing information. PNNI uses the route calculations derived from the reachability, connectivity, and resource information dynamically maintained by PNNI routing. These routes are calculated as needed from the node's view of the current topology.

Viewing PNNI Logical Port Parameters

To view PNNI logical port parameters:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View PNNI Parameters Attributes. A dialog box appears that displays the PNNI logical port parameters fields (see Figure 7-6).

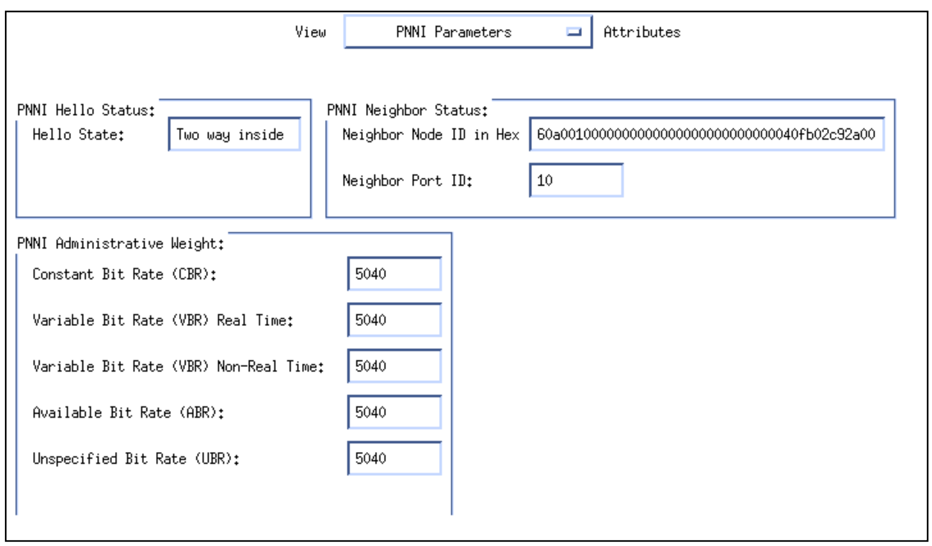


Figure 7-6. PNNI Logical Port Parameters

Table 7-6 provides summary descriptions of the PNNI logical port parameters. For more information on the PNNI logical port parameters, see the *NavisCore ATM Configuration Guide* and the *ATM Forum Technical Committee Private Network-Network Interface Specification Version 1.0* (af-pnni-0055.000), available from the ATM Forum's web site (http://www.atmforum.com).

Table 7-6. PNNI Logical Port Parameters Fields

Field	Displays...
PNNI Hello Status	
Hello State	The state of the PNNI Hello Finite State Machine (FSM) associated with the logical port you are monitoring. This state machine manages the exchange of hello packets between the switch and its neighbor. Neighboring nodes exchange these packets to discover and verify each other's identity and to determine the status of the links that connect them. See Table 7-7 for a description of the hello states that appear in this field.
PNNI Neighbor Status	
Neighbor Node ID in Hex	The hexadecimal node ID of the neighbor with which the switch communicates over the physical interface associated with the logical port. Each logical port on the switch communicates with a single neighbor that is reached over the physical interface (e.g., OC-12c) with which the logical port is associated.
Neighbor Port ID	The port ID that the neighbor assigns to its point of attachment to the logical link between the neighbor and the switch. A logical link represents the connectivity between two nodes. This connectivity includes individual physical links, individual virtual path connections, and parallel physical links or virtual path connections. A value of 0 indicates that the neighbor node has not assigned a port.
PNNI Administrative Weight – You can assign an administrative weight to each QoS category. This weight allows you to configure the network to favor one path over another path for a given category. The weights of all the network interfaces along a path are added up, and switches choose the path with the lowest cumulative weight when making routing decisions. For example, suppose that VBR Real Time traffic has two available paths for reaching a given destination. One path has a weight of 1000 while another path has a weight of 4000. The switch will choose the path with the weight of 1000.	
Constant Bit Rate (CBR)	The administrative weight assigned to the CBR QoS category for the network interface associated with the logical port.
Variable Bit Rate (VBR) Real Time	The administrative weight assigned to the VBR Real Time QoS category for the network interface associated with the logical port.
Variable Bit Rate (VBR) Non-Real Time	The administrative weight assigned to the VBR Non-Real Time QoS category for the network interface associated with the logical port.
Available Bit Rate (ABR)	The administrative weight assigned to the ABR QoS category for the network interface associated with the logical port.
Unspecified Bit Rate (UBR)	The administrative weight assigned to the UBR QoS category for the network interface associated with the logical port.

Table 7-7 describes PNNI Hello Finite State Machine states.

Table 7-7. PNNI Hello Finite State Machine States

Hello State	Description
Down	Indicates that no PNNI routing packets are sent or received over the link. This state is the initial state of the Hello FSM. This state is also reached when lower-level protocols have indicated that the link is not usable. For example, *Down* is reported if the physical link (e.g., a DS3 link) to the neighbor is down, or the switch or its neighbor is not fully configured or operational.
Attempt	Indicates that either no Hello packets or Hello packets containing information that does not match have been received. An example of a mismatch occurs when a switch receives a Hello packet from a neighbor that does not contain the same peer group ID as the switch. If this state persists, check the PNNI routing configuration information on the switch and the neighbor for mismatches. While in the attempt state, the switch attempts to contact the neighbor by periodically sending Hello packets.
One-way inside	Indicates that the switch has received Hello packets from the neighbor on this logical port. From the information in the packets, the switch establishes that both nodes are members of the same peer group. The remote node ID and the remote port ID in the received Hello packets are set to 0.
Two-way inside	Indicates that the switch has recently received Hello packets from the neighbor, indicating that both nodes are members of the same peer group. The packets include the correct remote node ID and the correct port ID. When the Hello FSM reaches this state, the switch and its neighbor can perform bi-directional communication over the link. Database summary packets, PTSE request packets, PTSPs, and PTSE acknowledgment packets can only be transmitted over links that are in this state. For physical links and VPCs, only those links that are in this state can be advertised by the switch in PTSEs as horizontal links.
One-way outside	Indicates that the switch has received Hello packets from the neighbor on this logical port, and the information in the packets have established that the neighbor node belongs to a different peer group. The remote node ID and the remote port ID in the received Hello packets are set to 0. While in this state, and while in the two-way outside state, the switch searches for a common peer group that contains both the switch and the neighbor.
Two way outside	Indicates that the switch has recently received Hello packets from the neighbor, and the packets indicate that the neighbor node belongs to a different peer group. The packets include the correct remote node ID and remote port ID fields, but the nodal hierarchy list does not include any common peer group. While in this state, and while in the one-way outside state, the switch searches for a common peer group that contains both the switch and the neighbor.

Table 7-7. PNNI Hello Finite State Machine States (Continued)

Hello State	Description
Common Outside	Indicates that the switch and its neighbor have found a common level of the routing hierarchy, and have achieved full bi-directional communication. Links that have achieved the Common Outside state can be advertised in PTSEs as uplinks, which connect border nodes and upnodes.
Not Applicable	Indicates that PNNI is not supported for this logical port.

Viewing PNNI Node Parameters

You can view the PNNI node parameters for each switch that supports PNNI in an Ascend network. To view PNNI node parameters:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show All PNNI Node Parameters. The Show All PNNI Node Parameters dialog box appears (see Table 7-7).

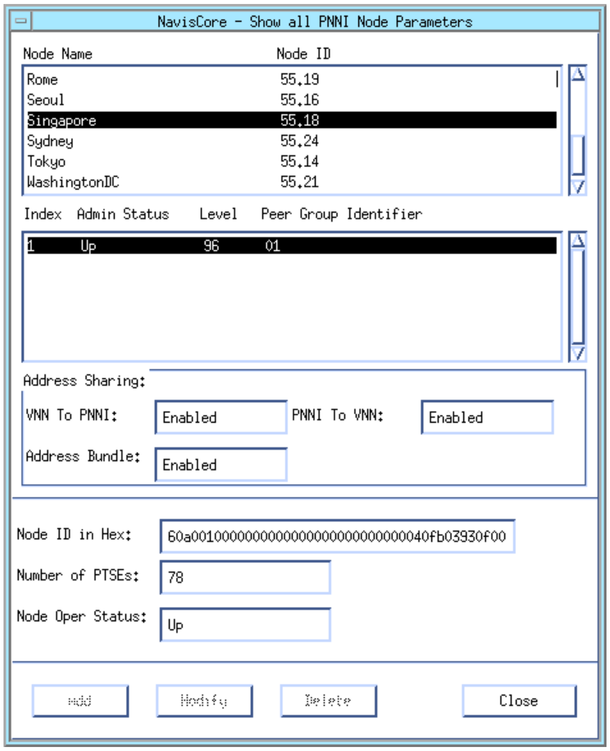


Figure 7-7. Show All PNNI Node Parameters Dialog Box

3. Select each switch that you want to monitor from the list box at the top. As you select each switch, the PNNI parameters for that switch appear in the fields on the dialog box.

Table 7-8 describes the PNNI node parameters fields. For more information on the PNNI node parameters, see the *NavisCore ATM Configuration Guide*.

Table 7-8. PNNI Node Parameters Fields

Field	Displays...
Node Name	The name of the switch.
Node ID	The switch number used as the host assignment in the switch's internal IP address.
Index	The index value that identifies the row entry for the switch in the table that stores the switch parameters. This value is always 1.
Admin Status	The PNNI administrative status (*Up* or *Down*). If PNNI Admin Status is *Down*, then PNNI Node Oper Status is also *Down*.
Level	The number of significant bits available for forming the PNNI Peer Group Identifier. The value can be from 0 to 104. By determining the number of bits allocated for the peer group identifier, the PNNI Level also determines the level of the switch in the PNNI routing hierarchy. The level of the peer group decreases as you move higher up in the hierarchy. For example, a node that is the grandparent of a peer group two levels lower will have fewer bits reserved for its peer group identifier than its grandchildren. As a result, the grandparent will have a smaller peer group identifier than the peer group identifier of its grandchildren.
Peer Group Identifier	The identifier of the peer group to which the switch belongs. The identifier is determined by the PNNI Level value.
VNN To PNNI	One of the following: *Enabled* – Internal addresses that are known to PNNI can be advertised within the Virtual Network Navigator (VNN) domain. Ascend switches use VNN to route network traffic to each other in the Ascend network. *Disabled* – Internal addresses that are known to PNNI cannot be advertised within the VNN domain.
PNNI To VNN	One of the following: *Enabled* – Internal addresses that are known to VNN can be advertised within the PNNI domain. *Disabled* – Internal addresses that are known to VNN cannot be advertised within the PNNI domain.
Address Bundle	One of the following: *Enabled* – Address bundling on a per-node basis is supported within the PNNI domain. *Disabled* – Address bundling on a per-node basis is not supported within the PNNI domain.

Table 7-8. PNNI Node Parameters Fields (Continued)

Field	Displays...
Node ID in Hex	The PNNI node ID of the switch. This ID is not configurable. The switch derives this ID by concatenating the PNNI Level, the hexadecimal value 0xA0, the PNNI Peer Group Identifier and the media access control (MAC) address of the Ethernet interface of the switch. This method of deriving the ID guarantees uniqueness.
Number of PTSEs	The number of PTSEs in the topology database of the switch. A PTSE is a collection of PNNI topology information that is sent to all nodes in a peer group.
Node Oper Status	The PNNI operating status for the switch (*Up* or *Down*). If PNNI Admin Status is *Down*, then PNNI Node Oper Status is also *Down*.

Viewing ATM FCP Attributes

To view ATM FCP attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View ATM FCP Attributes. The ATM FCP attributes fields appear (see Figure 7-8).

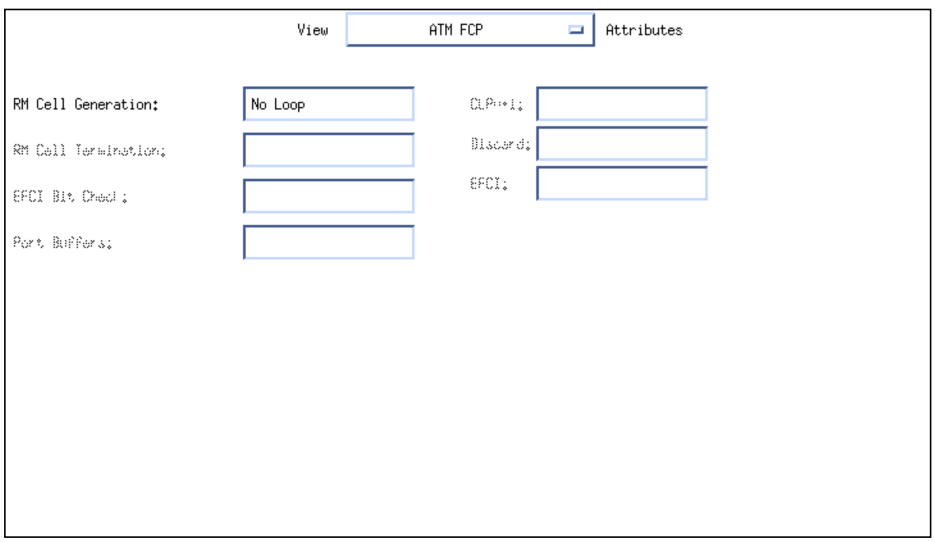


Figure 7-8. ATM FCP Attributes Fields

Table 7-9 describes ATM FCP attribute fields.

Table 7-9. ATM FCP Attributes Fields

Field	Displays...
RM Cell Generation	The type of Resource Management (RM) cell that the FCP generates for the virtual circuit. If the FCP does not generate RM cells, *No loop* is displayed. Otherwise, the FCP generates one of the following types of RM cells: *Cascade Communications Resource Management (CCRM) Cells* – CCRM cells are a subset of the ATM Forum's ATM Traffic Management Specification, Version 4.0, Available Bit Rate (ABR) RM cells. *Backward Congestion Message (BCM) Cells* – BCM cells provide for interoperability with other manufacturer's ATM switches.
RM Cell Termination	The type of RM cell that terminates the logical port: either *CCRM* or *CCRM and BCM*.
EFCI Bit Check	One of the following: *Enabled* – EFCI Bit Check is enabled. The EFCI Bit Check enables you to support control loops across switches that do not have the ATM Flow-Control Processor installed. These switches mark the EFCI bit in data cells to indicate network congestion. If the option is enabled on the next downstream ATM Flow-Control Processor, it takes into consideration these EFCI bits when it generates a backward RM cell. *Disabled* – EFCI Bit Check is disabled.
Port Buffers	The number of cell buffers configured for the logical port.
CLP0+1	The value for the CLP0+1 threshold buffer. The CLP0+1 threshold enables you to reserve buffers before the maximum buffer capacity is reached.
Discard	The value for the global discard threshold buffer. Global discard buffers enable you to reserve buffers for cell discard.
EFCI	The value for the congestion threshold. You can configure the congestion threshold to allow for some margin before the global discard buffer threshold is reached. This margin compensates for some of the closed-loop, flow-control delay in the network prior to discarding cells.

Viewing SVC VPI/VCI Range Attributes

SVC VPI/VCI range attributes provide the ranges of VPIs/VCIs available for SVCs.

To view SVC VPI/VCI range attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View SVC VPI/VCI Range Attributes. The SVC VPI/VCI Range attributes fields appear (see Figure 7-9).

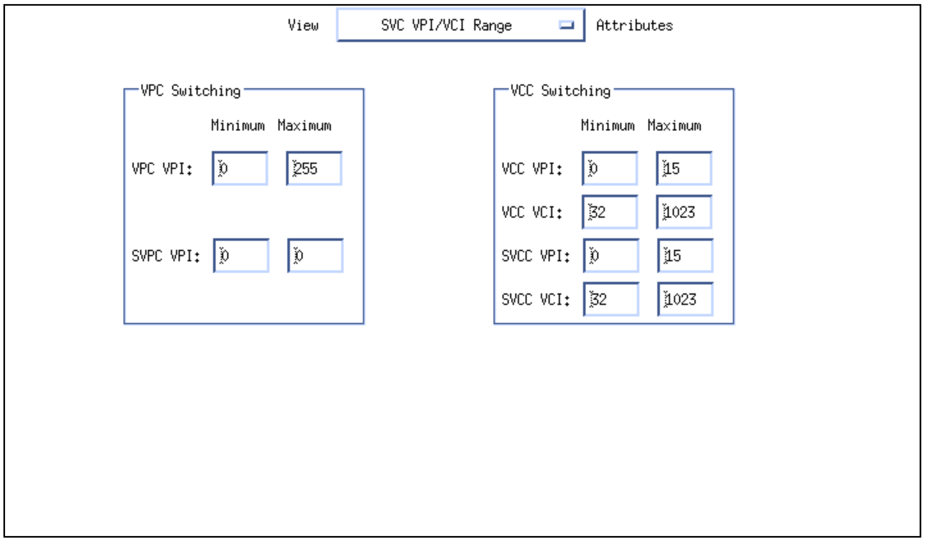


Figure 7-9. ATM SVC VPI/VCI Range Attributes Dialog Box

Table 7-10 describes the SVC VPI/VCI range attributes fields. For more information on the SVC VPI/VCI attributes, see the *NavisCore ATM Configuration Guide.*

Table 7-10. SVC VPI/VCI Range Attributes Fields

Field	Displays...
VPC Switching	
VPC VPI (Min. and Max.)	The range of permanent VPC VPIs.
SVPC VPI (Min. and Max.)	The range of switched VPC VPIs.
VCC Switching	
VCC VPI (Min. and Max.)	The range of VCC VPIs.
VCC VCI (Min. and Max.)	The range of VCC VCIs.
SVCC VPI (Min. and Max.)	The range of switched VCC VPIs
SVCC VCI (Min. and Max.)	The range of switched VCC VCIs.

Viewing SVC Parameters

To view SVC parameters:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View SVC Parameters Attributes. The ATM SVC parameters appear (see Figure 7-10).

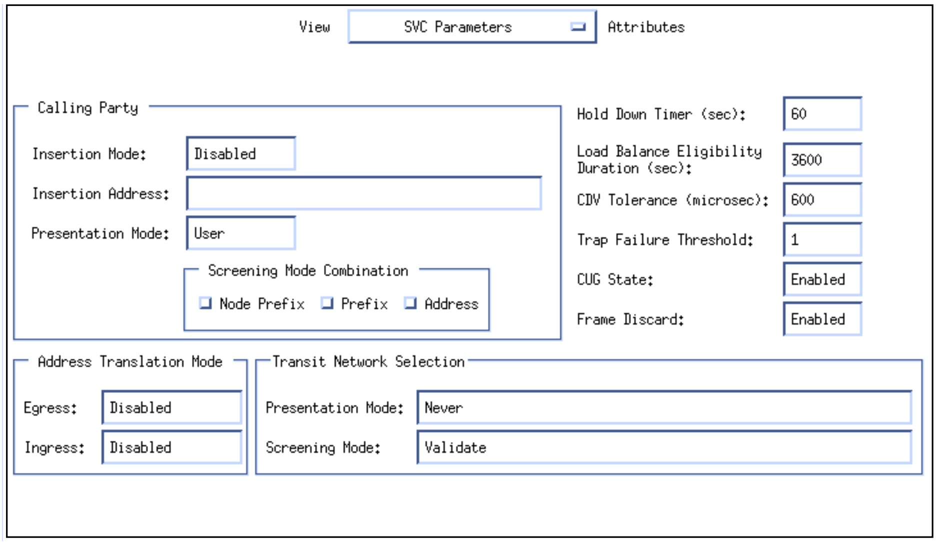


Figure 7-10. ATM SVC Parameters Dialog Box

Table 7-11 describes the ATM SVC parameters.

Table 7-11. ATM SVC Parameters

Field	Displays...
Calling Party Fields	
Insertion Mode	One of the following insertion mode options: *Disabled* – The logical port does not insert or replace the calling party address. *Insert* – If the logical port receives a call that does not have a calling party information element, it inserts the address from the Insertion Address field. *Replace* – The logical port takes one of the following actions when it receives a call: • If there is no calling party address, the logical port inserts the calling party address specified in the Insertion Address field. • If there is a calling party address, the logical port overwrites the existing calling party information element with the address specified in the Calling Party Insertion Address field.

Table 7-11. ATM SVC Parameters (Continued)

Field	Displays...
Insertion Address	The calling party insertion address.
Presentation Mode	One of the following presentation modes: *User* – The logical port includes the calling party address on outgoing calls based on the Presentation Indicator in the SETUP message of the user's call. *Always* – The logical port always includes the calling party address on outgoing calls, regardless of the Presentation Indicator in the SETUP message of the user's call. *Never* – The logical port never includes the calling party address on outgoing calls, regardless of the Presentation Indicator in the SETUP message of the user's call.
Screening Mode Combination	The criteria that an ingress call must match in order to be processed. For example, if *Node Prefix* and *Address* are indicated, all ingress calls must match either a valid node prefix or a valid port address.
General Fields	
Hold Down Timer (sec)	The number of seconds to wait before the network initiates call clearing when a trunk has gone down.
Load Balance Eligibility Duration (sec)	The number of seconds an SVC must be established before a call is eligible for load balance rerouting.
CDV Tolerance (microsec)	The cell delay variation (CDV) tolerance, in microseconds. UPC uses the value in this field to police the requested traffic descriptor.
Trap Failure Threshold	The threshold crossing alarm value for SVC failure traps. The switch generates a trap if the internal SVC failure counter crosses this threshold during the current 15-minute time period. The internal counter is reset every 15 minutes. The default value of one means that if one SVC failure occurs on a logical port, the switch issues a trap. The switch will issue no additional traps until the next 15-minute period expires. If you change the threshold value to 100, it means that 100 SVC failures must occur in a 15-minute window before the switch generates a trap.
CUG State	One of the following: *Enabled* – The logical port supports closed user group (CUG) processing. *Disabled* – The logical port does not support CUG processing.
Frame Discard (CBX 500 switches equipped with Flow Control Processing)	One of the following: *Enabled* – The network performs early packet discard (EPD) for SVCs (originating on this logical port) that use ATM Adaptation Layer 5 (AAL.5) for their connection attempts. *Disabled* – The network always performs cell loss priority one (CLP1) discard on SVCs originating on the logical port.

Table 7-11. ATM SVC Parameters (Continued)

Field	Displays...
Address Translation Mode	
Egress	The configured egress address translation mode option. Table 7-12 describes these options. This option should be compatible with the ingress translation mode option.
Ingress	The configured ingress address translation mode option. Table 7-13 describes these options. This option should be compatible with the egress translation mode option.
Transit Network Selection	
Presentation Mode	One of the following egress presentation modes for the logical port: *Never* – Never signal transit network selection (TNS) in egress calls. *Present Signaled TNS Only* – Signal TNS in egress calls only if TNS was signaled by the user in the ingress call. *Signaled or Source Default* – Signal TNS in egress calls only if TNS was signaled by the user in the ingress call or a source default network ID was provisioned at the ingress user's logical port.
Screening Mode	One of the following screening modes for the logical port: *Ignore* – Ignore the signaled TNS. *Accept* – Always accept the signaled TNS. *Validate* – Screen the signaled TNS and ignore it if there is no match.

Table 7-12 describes egress address translation mode options.

Table 7-12. Egress Address Translation Mode Options

Option	Description
Disabled	No address translation occurs on egress from the logical port.
Tunnel	The call is routed through another network that uses a different address domain. If the calling party address matches a port prefix and the port prefix has a gateway address defined, the switch substitutes the local gateway address for the calling party address, and also substitutes the remote gateway address for the called party address on egress from the logical port. The original addresses are then carried as a sub-address. If Tunnel is specified for egress translation mode, it should also be specified for ingress translation mode.
E.164 Native-to-AESA	Converts native E.164 addresses to an E.164 ATM End System Address (AESA) format. See Table 13-20 on page 13-56 for more information on address formats.

Table 7-12. Egress Address Translation Mode Options (Continued)

Option	Description
E.164 AESA-to-Native	Converts E.164 AESA addresses to native E.164 addresses. See Table 13-20 on page 13-56 for more information on address formats.
Replace	The call is routed into an attached network that uses a different address domain. At the network's egress port, the local gateway address replaces the calling party address and the remote gateway address replaces the called party address.

Table 7-13 describes ingress address translation mode options.

Table 7-13. Ingress Address Translation Mode Options

Option	Description
Disabled	No address translation occurs on ingress to the logical port.
Tunnel	A sub-address is present in the SETUP message to promote it to the address information element at the ingress port.
E.164 Native-to-AESA	Converts native E.164 addresses to E.164 AESA format. See Table 13-20 on page 13-56 for more information on address formats.
E.164 AESA-to-Native	Converts E.164 AESA addresses to native E.164 addresses. See Table 13-20 on page 13-56 for more information on address formats.

Viewing SVC Routing Priorities

SVC routing priorities enable you to assign bandwidth and bumping priority to SVCs based on ingress QoS class. The network routes SVCs originating from this logical port according to the SVC ingress QoS class you select.

To view SVC routing priorities:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View SVC Routing Priorities Attributes. The SVC routing priorities fields appear (see Figure 7-11).

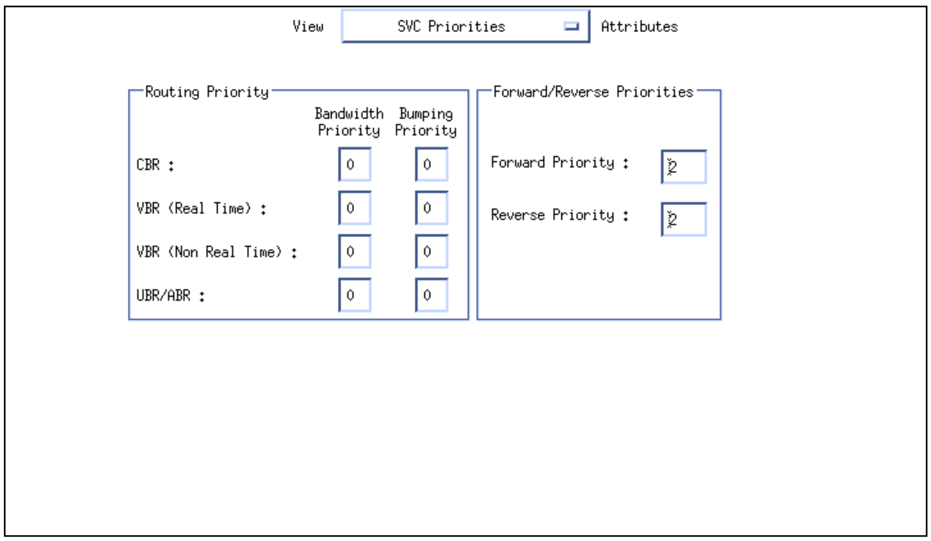


Figure 7-11. ATM SVC Routing Priorities Fields

For each QoS class, the dialog box displays the *bandwidth priority* and the *bumping priority*. In the event of provisioning, trunk failure recovery or load balance re-routing, PVCs and SVCs use the combination of bandwidth priority and bumping priority to preserve proper routing priority.

Bandwidth priority is a value from 0 to 15, where 0 is the highest priority. Bumping priority is a value from 0 to 7, where 0 is the highest priority.

Bandwidth priority supersedes bumping priority. The priority routing algorithm favors VCs with lower bandwidth priorities over VCs with higher bandwidth priorities, regardless of their respective bumping priorities.

If both VCs have an equal bandwidth priority, then the priority routing algorithm favors the VC with the lower bumping priority. For example, suppose that two VCs that traverse an optimal path have a bandwidth priority of two, but one VC has a bumping priority of three and the other VC has a bumping priority of four. In the event of a trunk failure, the VC assigned the bumping priority of three will be favored, and the VC assigned the bandwidth priority of four will be forced on to a non-optimal path.

There are additional rules that govern priority routing. See the *NavisCore ATM Configuration Guide* for more information.

Table 7-14 describes the ATM SVC routing priorities fields.

Table 7-14. ATM SVC Priority Routing Attributes

Field	Description
CBR	The bandwidth priority and the bumping priority for the Constant Bit Rate (CBR) QoS.
VBR (Real Time)	The bandwidth priority and the bumping priority for the Variable Bit Rate (VBR) Real-Time QoS.
VBR (Non Real Time)	The bandwidth priority and the bumping priority for the VBR Non-Real Time QoS.
UBR/ABR	The bandwidth priority and the bumping priority for the Unreliable Bit Rate/Available Bit Rate (UBR/ABR) QoS.
Forward Priority	The discard priority level (from 1 to 3) in the forward direction (caller to callee) for SVCs that originate at this logical port. When a particular service category's output queue becomes congested, it must discard cells. The value in this field sets the discard priority for the SVC in the forward direction. The lower the number, the higher the priority (for example, a value of 1 sets a higher priority than a value of 2).
Reverse Priority	The discard priority level (from 1 to 3) in the reverse (callee to caller) direction for SVCs that originate at this logical port. When a particular service category's output queue becomes congested, it must discard cells. The value in this field sets the discard priority for the SVC in the reverse direction. The lower the number, the higher the priority (for example, a value of 1 sets a higher priority than a value of 2).

Viewing Traffic Descriptor Attributes

You can view traffic descriptor attributes for the following types of logical ports:

ATM UNI — ILMI and signaling control channel traffic descriptors are provided.

ATM Direct and OPTimum Trunks — Node channel and card channel traffic descriptors are provided.

ATM NNI — PNNI, RCC, signaling and ILMI channel traffic descriptors are provided.

You can view traffic descriptor attributes in two ways:

- You can view the traffic descriptor attributes for a logical port.
- You can view the traffic descriptor attributes for the entire switch.

Viewing Traffic Descriptor Attributes for a Logical Port

To view traffic descriptor attributes for a logical port:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1 on page 6-2).
3. Select the appropriate logical port name from the list box on the left.
4. Depending on how the logical port is configured, perform one of the following actions from the View Attributes options menu:
   - For logical ports that support a Direct trunk or an OPTimum trunk, select Traffic Descriptors. Then, select Node-to-Node Mgmt Traffic Descriptors if you want to view the traffic descriptors for the node control channel or select Trunk Signaling Traffic Descriptors if you want to view traffic descriptors for the trunk's control channel. The Show Logical Port Traffic Descriptors dialog box appears (see Figure 7-12).
   - For ATM UNI logical ports, select ILMI/Signaling/OAM. Then, select the Traffic Descriptors button in either the ILMI or Signaling part of the dialog box, depending on whether you want to view traffic descriptors for ILMI or signaling. The Show Logical Port Traffic Descriptors dialog box appears (see Figure 7-12).
5. Select the appropriate traffic descriptor from the list box on the left. The traffic descriptor values appear in the fields on the right.

Figure 7-12 shows a sample Logical Port Traffic Descriptors dialog box. Note that the title of the dialog box changes depending on whether the traffic descriptors are for the node control channel, trunk control channel, ILMI, and so on.

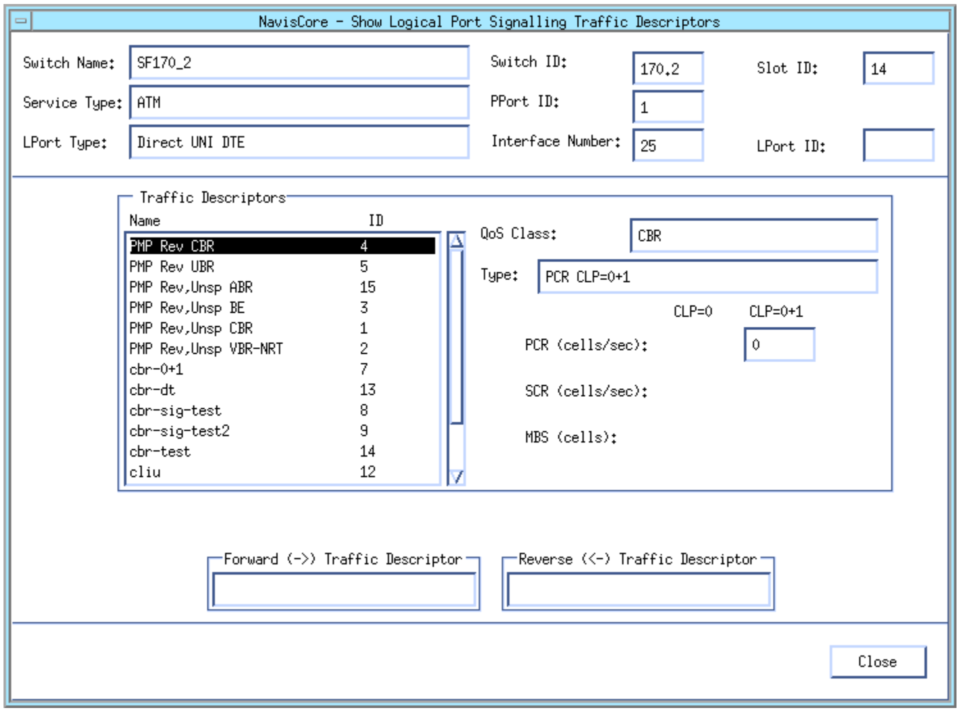


Figure 7-12. Show Logical Port Traffic Descriptors Dialog Box

Table 7-15 on page 7-35 describes the fields on the Show Logical Port Traffic Descriptors dialog box.

Viewing Traffic Descriptor Attributes for the Entire Switch

To view traffic descriptor attributes for an entire switch:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show All ATM Traffic Descriptors. The Show All ATM Traffic Descriptors dialog box appears (see Figure 7-13).
3. Select the appropriate traffic descriptor from the list box on the left. The traffic descriptor values appear in the fields on the right.

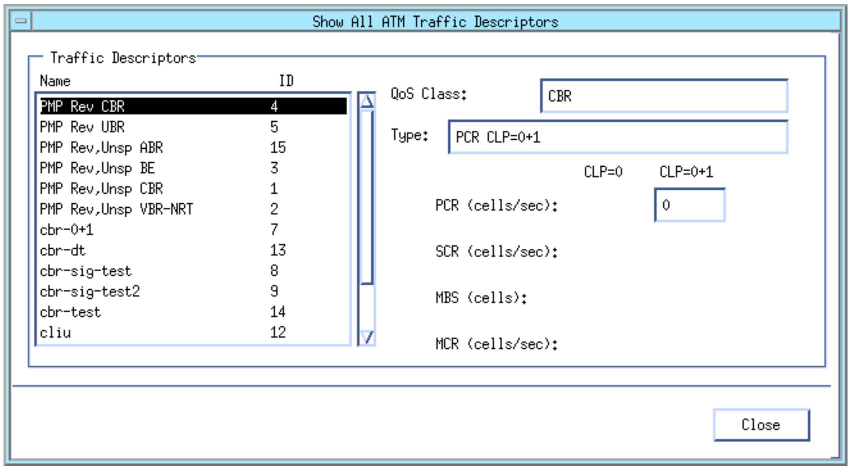


Figure 7-13. Show All ATM Traffic Descriptors Dialog Box

Table 7-15 describes the fields on the Show ATM Traffic Descriptors dialog box.

Traffic Descriptor Attribute Fields

Table 7-15 describes the traffic descriptor attribute fields. For more information on traffic descriptors, see the *NavisCore ATM Configuration Guide.*

Table 7-15. Traffic Descriptor Fields

Field	Displays...
Name	The names of the traffic descriptors.
ID	The IDs of all the traffic descriptors.
QoS Class	The QoS class of service with which the selected traffic descriptor is associated. The QoS classes are: *CBR* – Constant Bit Rate *VBR Real Time* – Variable Bit Rate Real-Time *VBR Non-Real Time* – Variable Bit Rate Non-Real Time *UBR* – Available Bit Rate/Unspecified Bit Rate (ABR/UBR)
Type	The traffic descriptor combination. See the *NavisCore ATM Configuration Guide* for more information on traffic descriptor combinations.
CLP=0	Provides a column for viewing the configured CLP=0 (high priority cell stream) values for PCR, SCR, and MBS.
CLP=0+1	Provides a column for viewing the configured CLP=0+1 (aggregate cell stream) values for PCR, SCR, and MBS.

Table 7-15. Traffic Descriptor Fields (Continued)

Field	Displays...
PCR (cells/sec)	The Peak Cell Rate (PCR), in cells per second, for the CLP=0 and CLP=0+1 traffic parameters. The PCR is the maximum allowed cell transmission rate. It defines the shortest time period between cells and provides the highest guarantee that network performance objectives (based on cell loss ratio) will be met.
SCR (cells/sec)	The Sustained Cell Rate (SCR), in cells per second, for the CLP=0 and CLP=0+1 traffic parameters. The SCR is the maximum average cell transmission rate that is allowed over a given period of time on a given circuit. It allows the network to allocate sufficient resources (but fewer resources than would be allocated based on PCR) for guaranteeing that network performance objectives are met. This parameter applies only to VBR-RT and VBR-NRT traffic; it does not apply to CBR or UBR/ABR traffic.
MBS (cells)	The Maximum Burst Size (MBS), in cells, for the CLP=0 and CLP=0+1 traffic parameters. The MBS is the maximum number of cells that can be received at the Peak Cell Rate. This allows a burst of cells to arrive at a rate higher than the SCR. If the burst is larger than anticipated, the additional cells are either tagged or dropped. This parameter applies only to VBR-RT and VBR-NRT traffic; it does not apply to CBR or UBR/ABR traffic.
Forward (->) Traffic Descriptor	The traffic descriptor for forward traffic, where forward traffic is into the switch.
Reverse (<-) Traffic Descriptor	The traffic descriptor for reverse traffic, where reverse traffic is out of the switch.

Viewing OPTimum Trunk VPI Range Attributes

ATM OPTimum trunks support *virtual paths*. A virtual path is a group of *virtual channels* (VCs) carried between two points. VPIs are 8-bit or 12-bit numbers that identify virtual paths to the ATM logical port. VPIs provide a way to bundle traffic headed in the same direction.

VCs are connections between two communicating ATM entities. They can consist of a group of several ATM links: CPE to central office switch, switch to switch, and switch to user equipment. All communications proceed along this same VC, which preserves call sequence and provides a certain quality of service. VCIs identify virtual channels.

The VPI and VCI are used only for establishing connections between two ATM entities, not the end-to-end connection.

To view OPTimum trunk VPI range attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View Opt Trunk VPI Range Attributes. The OPTimum trunk VPI range attribute fields appear (see Figure 7-14).

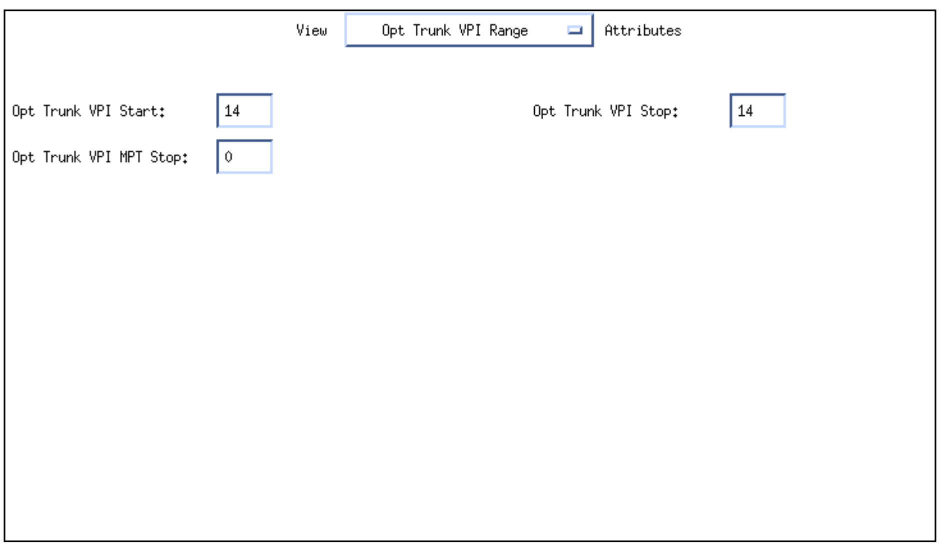


Figure 7-14. Opt Trunk VPI Range Attributes Dialog Box

Table 7-16 describes the OPTimum trunk VPI range attribute fields. For more information on OPTimum trunk VPI range attributes, see the *NavisCore ATM Configuration Guide*.

Table 7-16. OPTimum Trunk VPI Range Attributes Fields

Field	Displays...
Opt Trunk VPI Start Opt Trunk VPI Stop	The VPI start and VPI stop values, which specify the range of VPIs that can be created over the OPTimum trunk. The maximum allowable range is 0 - 255 for a UNI logical port and 0 - 4095 for an NNI logical port. Since you can specify more than one OPTimum trunk on the same physical link, make sure the total number of VPIs allowed on each trunk does not exceed these limits.
Opt Trunk VPI MPT Stop (*OPTimum cell trunks used for MPT traffic only*)	A VPI MPT stop value that specifies which part of the VPI range is dedicated to multipoint-to-point (MPT) traffic. For example: VPI start =2 VPI MPT stop=10 VPI stop=15 VPIs 3 – 10 are dedicated to MPT traffic only; VPIs 2 and 11 – 15 are used for other virtual paths. The default value, 0, prevents MPT traffic from using this OPTimum cell trunk. ***Note:*** *The range of VPIs configured for MPT traffic must be identical on both sides of the trunk.* For more information about MPT traffic, see the *NavisCore IP Navigator Configuration Guide*.

Viewing Discard/Congestion Mapping Attributes

Discard/Congestion mapping attributes allow you to create DE/CLP and FECN/EFCI mappings for ATM-to-Frame internetworking traffic across ATM trunks. You create these mappings for the following types of logical ports:

- ATM Direct trunk logical ports associated with ATM IWU IOMs and ATM CS IOMs on B-STDX 9000 switches
- ATM OPTimum trunk logical ports associated with ATM IWU IOMs and ATM CS IOMs on B-STDX 9000 switches
- ATM OPTimum frame trunk logical ports associated with ATM IWU IOMs and ATM CS IOMs on B-STDX 9000 switches

To view discard/congestion mapping attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View Discard/Congestion Mapping Attributes. The discard/congestion mapping attributes fields appear (see Figure 7-15).

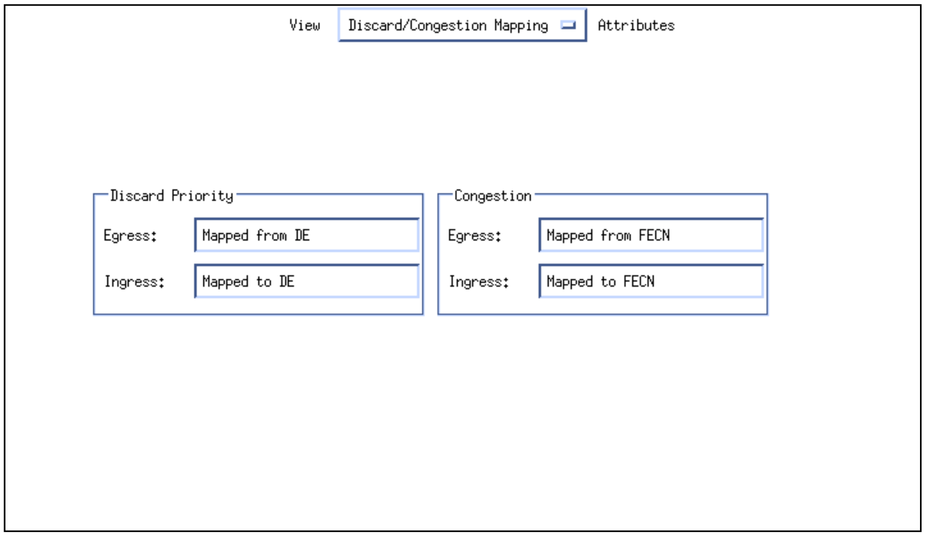


Figure 7-15. Discard/Congestion Mapping Attributes Fields

Table 7-17 describes discard/congestion mapping attributes fields.

Table 7-17. Discard/Congestion Mapping Attributes Fields

Field	Displays...
Discard Priority	
Egress	The type of CLP bit mapping for frames that are segmented into cells for transmission on an ATM trunk. Possible values are: *Mapped from DE* – When the switch segments an egress frame into cells for transmission, the switch sets the CLP bit in each cell to the value of the discard/priority bit. The discard/priority bit is associated with each frame that passes through the switch, and indicates the DE/CLP setting. The DE/CLP mapping occurs just before the frame passes to the hardware for segmentation. The discard/priority bit setting that the switch uses to set the CLP bit is a product of the ingress data stream's discard/priority bit setting and any modifications of this bit due to rate enforcement processing. *Always 0* – The switch sets the value of the CLP bit to 0 in all cells that are a product of segmented frames transmitted on the trunk. *Always 1* – The switch sets the value of the CLP bit to 1 in all cells that are a product of segmented frames transmitted on the trunk.

Table 7-17. Discard/Congestion Mapping Attributes Fields (Continued)

Field	Displays...
Ingress	The DE bit mapping for segmented frames that are received from an ATM trunk. Possible values are: *Mapped to DE* – When the switch receives cells that comprise an ingress frame, the switch sets the discard/priority bit to the value of the CLP bit in the cells for subsequent transmission. If the egress packet format is Frame Relay, the switch includes the discard/priority bit in the Q.922 header as the DE bit. If the egress packet format is ATM, then the switch uses the discard/priority bit to set the CLP bit. Keep in mind that rate enforcement and congestion control processing on the egress IOM use this discard/priority setting. The egress IOM may change the discard/priority bit due to congestion or rate enforcement. *Always 0* – The value of the discard/priority bit is always 0, regardless of the CLP setting received in cells that comprise the frame. This setting is transferred to the egress IOM. Keep in mind that rate enforcement and congestion control processing on the egress IOM use this discard/priority setting. The egress IOM may change the discard/priority bit due to congestion or rate enforcement. *Always 1* – The value of the discard/priority bit is always 1, regardless of the CLP setting received in cells that comprise the frame. This setting is transferred to the egress IOM. Keep in mind that rate enforcement and congestion control processing on the egress IOM use this discard/priority setting. The egress IOM may change the discard/priority bit due to congestion or rate enforcement.
Congestion	
Egress	The EFCI bit mapping for frames that are to be segmented for transmission on an ATM trunk. Possible values are: *Mapped from FECN* – When the switch segments the frame into cells for transmission, the switch sets the value of the EFCI bit to the value of the congestion bit (FECN). The mapping occurs just before the frame passes to the hardware for segmentation. *Always 0* – The value of the EFCI bit is 0 for all cells that comprise frames transmitted on the trunk.
Ingress	The FECN bit mapping for segmented frames received on an ATM trunk. Possible values are: *Mapped to FECN* – The switch sets the congestion bit (FECN) to the value of the EFCI bit received in the cells that comprise an ingress frame. The congestion bit passes with the frame to the egress IOM for subsequent transmission. If the egress packet format is Frame Relay, the egress IOM includes the congestion bit in the Q.922 header as the FECN bit. If the egress packet format is ATM, the EFCI bit is set from the congestion bit. The egress IOM may change the congestion bit due to congestion. *Always 0* – The value of the congestion bit is always 0, regardless of the EFCI bit setting in the cells that comprise the frame. The switch forwards this setting to the egress IOM along with the frame.

Viewing ATM Logical Port Summary Statistics

You can access the dialog boxes for viewing ATM logical port summary statistics in two ways:

- From the Monitor menu. This chapter presents this method of accessing ATM logical port summary statistics dialog boxes.
- From the View Physical Port Attributes dialog box for the physical port to which the ATM logical port is mapped. See "Reviewing Physical Port Status" on page 2-44 for information on this method of accessing logical port statistics dialog boxes.

To view ATM logical port summary statistics from the Monitor menu:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1 on page 6-2).
3. Select the appropriate logical port name from the list box on the left.
4. Select Options ⇒ Statistics.
5. Choose View. The Logical Port Summary Statistics dialog box appears.

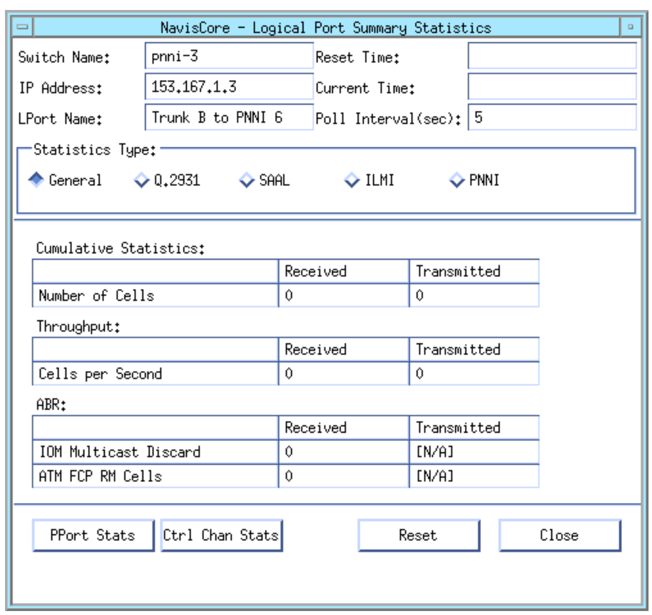


Figure 7-16. Logical Port Summary Statistics Dialog Box

Table 7-18 describes the Logical Port Summary Statistics dialog box buttons.

Table 7-18. Logical Port Summary Statistics Dialog Box Buttons (ATM)

Button	Function
PPort Stats	Displays the Physical Port Summary Statistics dialog box. For details, see "Viewing Physical Port Summary Statistics" on page 3-2.
Ctrl Chan Stats	Displays the Logical Port Control Channel Statistics dialog box. This button does not apply to all ATM logical ports. For details, see "Viewing ATM Control Channel Statistics" on page 7-47.
Reset	Clears the current statistics and updates the time in the Reset Time field.
Close	Closes the dialog box.

The Logical Port Summary Statistics dialog box allows you to toggle between General (i.e., throughput), Q.2931 (also known as Q.93B), SAAL, ILMI, and PNNI statistics. Most statistics have both received and transmitted counters. If any of the toggles are grayed out, the associated statistics do not apply to the logical port you are viewing. Table 7-19, Table 7-20, Table 7-21, and Table 7-22 describe these statistics.

Table 7-19 describes general logical port summary statistics.

Table 7-19. General Logical Port Summary Statistics

Statistic	Description
Number of Cells	The total number of cells received and transmitted by the port since the last reset.
Cells per second	The total number of cells received and transmitted by the port each second.
IOM Multicast Discard	The total number of incoming cells on the port's multicast circuits that were discarded by the ATM Flow-Control Processor (FCP).
ATM FCP RM Cells	The total number of RM cells that the ATM FCP received on the logical port.

Table 7-20 describes the statistics that appear when you select Q.2931 on the Logical Port Summary Statistics dialog box.

Table 7-20. Q.2931 Logical Port Summary Statistics

Statistic	Description
Number or SVCs established	The total number of SVCs established since the IOM became active.
Number of Active SVCs	The number of SVCs that are currently active. The reset statistics function (that you select by using the Reset button) does not update this statistic.
Number of SVC Failures	The total number of SVC failures on this logical port resulting from the transmission or reception of RELEASE, ADD PARTY REJECT, or DROP PARTY PDUs with abnormal cause codes.
Last Cause Code	The last received and transmitted cause code. Cause codes are listed in the ATM/UNI Forum specifications. The reset statistics function (that you select by using the Reset button) does not update this statistic.
Setup PDUs	The number of Setup Protocol Data Units (PDUs). A Setup PDU is used to place a call.
Call Proceeding PDUs	The number of local acknowledgments of a Setup PDU. The local acknowledgment specifies that the call is being processed.
Connect PDUs	The number of Connect PDUs. A Connect PDU is used to accept a call.
Connect Acknowledge PDUs	The number of local acknowledgments to Connect PDUs.
Release PDUs	The number of Release PDUs. A Release PDU is used to terminate calls. A value in this field that exceeds the value for the number of Connect PDUs indicates that the system is dropping calls.
Release Complete PDUs	The number of Release Complete PDUs. A Release Complete PDU is a local acknowledgment that the Release PDU was received.
Add Party PDUs	The number of Add Party PDUs. An Add Party PDU is used to add a leaf to a point-to-multipoint connection.
Add Party Acknowledge PDUs	The number of Add Party Acknowledgment PDUs. An Add Party Acknowledgment PDU is a local acknowledgment that the Add party PDU was received.
Add Party Reject PDUs	The number of Add Party Reject PDUs. An Add Party Reject PDU is used to reject an add party request.
Drop Party PDUs	The number of Drop Party PDUs. A Drop Party PDU is a PDU used to terminate a leaf from a point-to-multipoint connection.
Drop Party Acknowledge PDUs	The number of Drop Party Acknowledgment PDUs. A Drop Party Acknowledgment PDU is a local acknowledgment that the Drop Party PDU was received.

Table 7-20. Q.2931 Logical Port Summary Statistics (Continued)

Statistic	Description
Status Enquiry PDUs	The number of Status Enquiry PDUs. A Status Enquiry PDU is an unsolicited status request for a call. One endpoint signals that the connection seems valid and expects verification from the other endpoint.
Status PDUs	The number of Status PDUs. A Status PDU is a response to a Status Enquiry PDU. The PDU indicates the state of the call.
Restart PDUs	The number of Restart PDUs. A Restart PDU is used to restart a single call or the entire signaling VC.
Restart Acknowledge PDUs	The number of Restart Acknowledgment PDUs. A Restart Acknowledgment PDU is a local acknowledgment of a Restart PDU.
Notify PDUs	The number of Notify PDUs. A Notify PDU delivers notification when notification does not coincide with call/connection establishment procedures or call/connection clearing procedures. In addition, a Notify PDU is sent or received by the user or by the network only after the first response to a Setup PDU has been sent or received and before clearing of the call reference is initiated.
Progress PDUs	The number of Progress PDUs. Progress PDUs are used when a B-ISDN channel is used as a transit network for multiple ISDN networks.
Alerting PDUs	The number of Alerting PDUs. The user sends an Alerting PDU on a point-to-point SVC when it determines that sufficient call setup information has been received from the network and compatibility requirements have been satisfied. The network sends an Alerting PDU in response to an Alerting PDU from the user. If the network receives an Alerting PDU, but does not receive a Connect PDU or Release PDU prior to the expiration of T301 (or a corresponding internal alerting supervision timing function), then the network may initiate call clearing procedures toward the user.
Party Alerting PDUs	The number of Party Alerting PDUs. A Party Alerting PDU is sent on a point-to-multipoint circuit to indicate that alerting has begun at the called party. Party Alerting PDUs essentially perform the same function as Alerting PDUs. The difference is that Party Alerting PDUs are sent on point-to-multipoint circuits; Alerting PDUs are sent on point-to-point circuits.

Table 7-21 describes the statistics that appear when you select SAAL on the Logical Port Summary Statistics dialog box.

Table 7-21. SAAL Logical Port Summary Statistics

Statistic	Description
Discards	The number of discards.
Errors	The number of errors.
Begin PDUs	The number of Begin PDUs, which request establishment of SAAL connections.
Begin Acknowledge PDUs	The number of Begin Acknowledgment PDUs, which acknowledge the acceptance of connection requests (Begin PDUs).
Begin Reject PDUs	The number of Begin Reject PDUs, which reject SAAL connection requests.
End PDUs	The number of End PDUs, which terminate SAAL connections.
End Acknowledge PDUs	The number of End Acknowledgment PDUs, which confirm termination of SAAL connections.
Resynchronization PDUs	The number of Resynchronization PDUs, which resynchronize system resources and states on both endpoints if they are out-of-sync.
Resync. Acknowledge PDUs	The number of Resynchronization Acknowledgment PDUs, which acknowledge acceptance of Resynchronization PDUs.
Error Recovery PDUs	The number of Error Recovery PDUs, which are sent to correct protocol errors.
Error Recovery Ack. PDUs	The number of Error Recovery Acknowledgment PDUs, which acknowledge Error Recovery PDUs (acknowledge recovery from a protocol error).
Sequenced Data PDUs	The number of Sequenced Data PDUs, which are sequentially numbered PDUs containing user-provided information fields.
Poll PDUs	The number of Poll PDUs, which are sent as keep-alive signals for the SAAL connection. Poll PDUs request status information about the other end of the connection.
Status PDUs	The number of Status PDUs, which respond to Poll PDUs.
Unsolicited Status PDUs	The number of Unsolicited Status PDUs, which inform the sender of one or more missing Sequenced Data PDUs.
Unnumbered user PDUs and Unnumbered Mgmt PDUs	Not used.
Signaling Channel Octets	The number of octets transmitted or received on the SAAL connection.

Table 7-21. SAAL Logical Port Summary Statistics (Continued)

Statistic	Description
Transmit Window Depth	The current depth of the SAAL transmit window, which represents the current number of outstanding, unacknowledged Sequenced Data PDUs.

Table 7-22 describes the statistics that appear when you select ILMI on the Logical Port Summary Statistics dialog box.

Table 7-22. ILMI Statistics

Statistic	Description
Improper Format PDUs	The total number of PDUs that were received with an improper format.
UME Entity Polls	The total number of ILMI received status polls issued by the User Management Entity (UME) at this port.
Octets	The total number of octets received and transmitted by the port.
Proper Format PDUs	The total number of Protocol Data Units (PDUs) that were received with a proper format and transmitted.

When you select PNNI on the Logical Port Summary Statistics dialog box, only one row of statistics — *Link Hellos* — appears. This row tells you the number of Hello packets sent and received.

Viewing ATM Control Channel Statistics

You can view statistics that provide information on the performance of ATM control channels. You can view control channel statistics for the following types of ATM logical ports:

ATM UNI — ILMI and signaling control channel.

ATM Direct and OPTimum Trunks — Node and card channel.

ATM NNI (With Protocol Type of PNNI) — Routing Control Channel (RCC), ILMI and signaling control channel.

To view control channel statistics:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1 on page 6-2).
3. Select the appropriate logical port name from the list box on the left.
4. Depending on the type of ATM logical port selected, perform one of the following actions:
   - Select Options ⇒ Conf Ctrl Chan Stats for OPTimum trunk logical ports.
   - Select Options ⇒ Statistics for ATM Direct trunk logical ports, ATM UNI logical ports, or ATM NNI (with protocol type of PNNI) logical ports.
5. Select View. Depending on your action in the previous step, one of the following events occurs:
   - If you previously selected Options ⇒ Conf Ctrl Chan Stats, the Logical Port Control Channel Statistics dialog box appears, allowing you to view control channel statistics. Figure 7-17 shows a sample Logical Port Control Channel Statistics dialog box. See Table 7-23 for descriptions of these statistics.
   - If you previously selected Options ⇒ Statistics, the Logical Port Summary Statistics dialog box appears (see Figure 7-16 on page 7-41). This dialog box provides a Ctrl Chan Stats command, which allows you to display control channel statistics on the Logical Port Control Channel Statistics dialog box. Figure 7-17 shows a sample Logical Port Control Channel Statistics dialog box. See Table 7-23 for descriptions of these statistics.

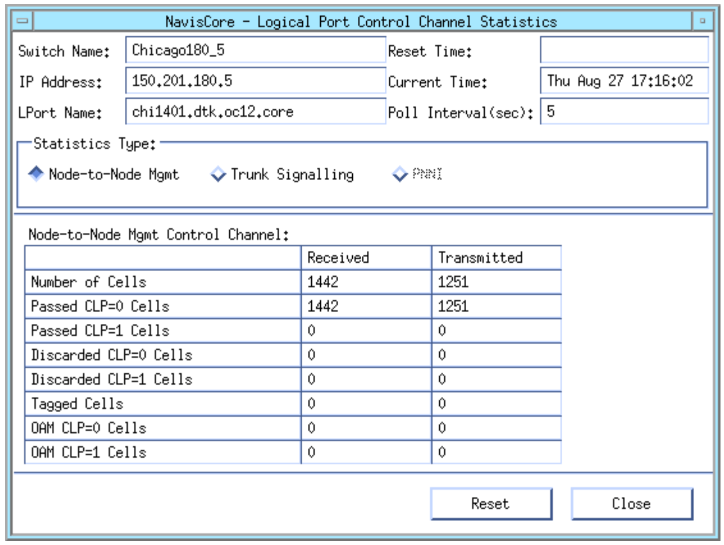


Figure 7-17. Sample Logical Port Control Channel Statistics Dialog Box

The exact appearance of the Logical Port Control Channel Statistics dialog box varies, depending on the type of logical port (for example, ATM Direct trunk ports versus ATM UNI ports). The Logical Port Control Channel Statistics dialog box allows you to toggle between statistics for the various control channels. For example, on the Logical Port Control Channel Statistics dialog box for ATM Direct trunk logical ports, you can toggle between node-to-node management channel and trunk signaling channel statistics. Or, for ATM UNI logical ports, you can toggle between ILMI and Signaling control channel statistics. For ATM PNNI logical ports, you can toggle between ILMI, Signaling, and PNNI (RCC) control channel statistics.

Table 7-23 describes the logical port control channel statistics.

Table 7-23. Logical Port Control Channel Statistics

Statistic	Description
Number of Cells	The total number of ATM cells received and transmitted on the control channel.
Passed CLP=0 Cells	The number of ATM CLP=0 cells that were received and transmitted on the control channel that passed UPC.
Passed CLP=1 Cells	The number of ATM CLP=1 cells that were received and transmitted on the control channel that passed UPC.
Discarded CLP=0 Cells	The number of ATM CLP=0 cells that were received on the control channel, but were discarded due to UPC failure. Ignore the value in the Transmitted column. If you notice that CLP=0 cells are discarded consistently, consider increasing the Maximum Burst Size (MBS) for the control circuit. See the *NavisCore ATM Configuration Guide* for more information on increasing the MBS.

Table 7-23. Logical Port Control Channel Statistics (Continued)

Statistic	Description
Discarded CLP=1 Cells	The number of ATM CLP=1 cells that were received on the control channel, but were discarded due to UPC failure. Ignore the value in the Transmitted column. If you notice that CLP=1 cells are discarded consistently, consider increasing the Maximum Burst Size (MBS) for the control circuit. See the *NavisCore ATM Configuration Guide* for more information on increasing the MBS.
Tagged Cells	The number of tagged ATM cells received. Ignore the value in the Transmitted column. If you notice that cells are tagged consistently, consider increasing the Maximum Burst Size (MBS) for the control circuit. See the *NavisCore ATM Configuration Guide* for more information on increasing the MBS.
OAM CLP=0 Cells	The number of ATM OAM CLP=0 cells transmitted. Ignore the value in the Received column.
OAM CLP=1 Cells	The number of ATM OAM CLP=1 cells transmitted. Ignore the value in the Received column.

Viewing All Management VPI/VCIs

To view status information for a management VPI/VCI connection, from the Monitor menu, select Ascend Objects ⇒ Show All Management VPI/VCIs. The Show All Management VPI/VCIs dialog box appears (see Figure 7-18).

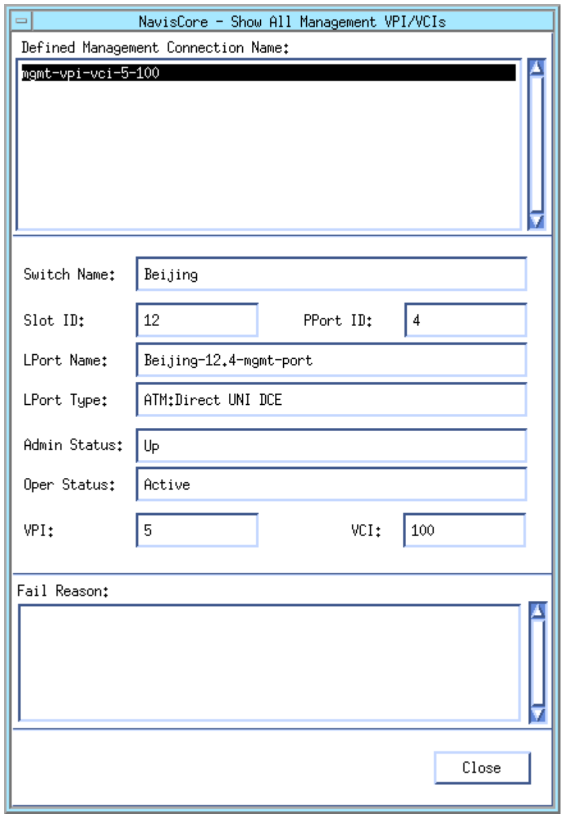


Figure 7-18. Show All Management VPI/VCIs Dialog Box

Table 7-24 describes the Show All Management VPI/VCI fields.

Table 7-24. Management VPI/VCI Fields

Field	Displays...
Switch Name	The name of the switch that connects to the router that serves as the interface for the network management VPI/VCI.
Slot ID	The number of the slot in which the IOM resides.
PPort ID	The port number for the physical port.
LPort Name	The name of the logical port.
LPort Type	The logical port type.

Table 7-24. Management VPI/VCI Fields (Continued)

Field	Displays...
Admin Status	*Up* or *Down* to indicate whether the management VPI/VCI connection is up or down.
Oper Status	The operational status of the management connection. Possible values include: *Active* – The connection is operational. *Inactive* – The connection is not operational. *Unknown* – The connection configuration is not contained within the calling node. *Invalid* – The calling node did not respond to the NMS request for the status of this connection.
VPI	The VPI that is used for the connection.
VCI	The VCI that is used for the connection.
Fail Reason	A reason code if the Operational Status is Inactive. See Table 13-3 on page 13-6 for more information.

8

Monitoring IP

This chapter describes how to retrieve status information about the various Ascend IP objects such as IP logical ports and associated parameters including OSPF, BGP, and RIP. Table 8-1 lists the sections in this chapter that describe each of the Monitor functions.

Table 8-1. Monitor Functions

To Monitor	See...
IP Logical Ports	"Viewing IP Logical Ports" on page 8-2
OSPF	"Viewing OSPF Information" on page 8-21
BGP	"Viewing BGP Information" on page 8-30
Network Filters	"Viewing Filters, Access Lists, and Route Maps" on page 8-42
Network Access Lists	"Viewing Network Access Lists" on page 8-46
Route Maps	"Viewing Route Maps" on page 8-48
Packet Filters	"Viewing IP Packet Filters" on page 8-50
QoS Profiles	"Viewing QoS Profiles" on page 8-58
Static Routes	"Viewing Static Routes" on page 8-62
ARP	"Viewing Static ARP Parameters" on page 8-63
IP Loopback Addresses	"Viewing IP Loopback Addresses" on page 8-65
MPT Path	"Viewing MPT Path Parameters" on page 8-66
RIP2	"Viewing RIP Information" on page 8-68
Multipoint-to-Point Operational Status	"Viewing MPT Point-to-Point Connection Status" on page 8-70
IP Routing Table	"Viewing the IP Routing Table" on page 8-73

Table 8-1. Monitor Functions (Continued)

To Monitor	See...
IP Servers	"Viewing IP Servers" on page 8-80
IP QoS PVCs	"Viewing IP QoS PVCs" on page 8-81

Viewing IP Logical Ports

IP logical ports support IP routing on B-STDX 8000/9000 switches and CBX 500 switches over ATM and Frame Relay links. To view an IP logical port:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All IP LPorts. The Show All IP LPorts dialog box appears (see Figure 8-1).

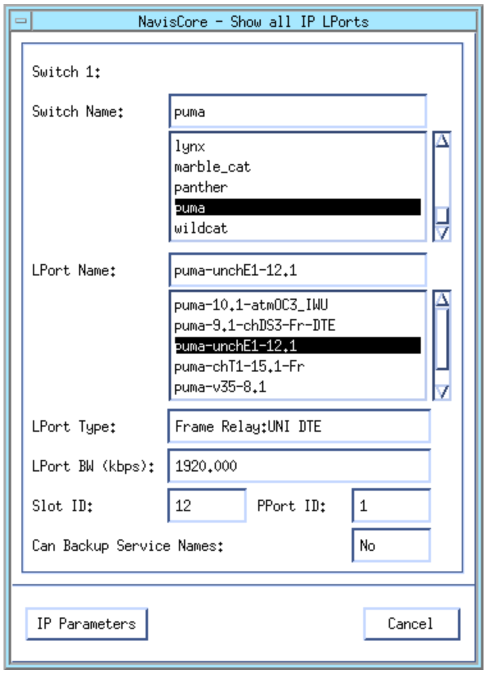


Figure 8-1. Show All IP LPorts

3. Select the IP Lport for which you want to view IP parameters.
4. Choose IP Parameters. The Show IP Parameters dialog box appears (see Figure 8-2).

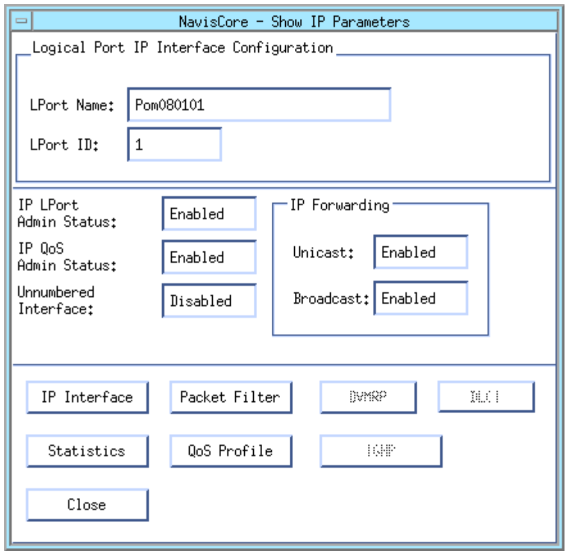


Figure 8-2. Show IP Parameters Dialog Box

Table 8-2 describes the Show IP Parameters buttons. Table 8-3 describes the IP Parameters fields.

Table 8-2. Show IP Parameters Buttons

Button	Function
IP Interface	View the IP interface address configuration.
Packet Filter	View inbound and outbound packet filters.
DLCI	*(For Frame Relay modules only)*. View the Data Link Connection Identifier (DLCI) for the logical port.
VPI/VCI	*(For ATM modules only)*. View the virtual path identifier (VPI) and virtual channel identifier (VCI) for the logical port.
Statistics	Access the IP Lport Statistics dialog box shown in Figure 8-10 on page 8-18. See "Viewing IP Logical Port Statistics" on page 8-18 for more information about IP logical port statistics.
QoS Profile	View the Quality of Service profiles.

Table 8-3. Show IP Parameter Fields

Field	Displays...
Lport Name	The name assigned to the LPort at configuration.
Lport ID	The ID number that uniquely identifies each logical port.
IP LPort Admin Status	One of the following: *Enable* – Port is activated for IP services. *Disable* – Port has never been activated for IP services or that the port is off-line for diagnostics. A logical port IOM with an IP LPort Admin Status of *Disable* is not operational for IP routing.
IP QoS Admin Status	One of the following: *Enable* – QoS flow profile is activated for the logical port. *Disable* – QoS flow profile is disabled.
Unnumbered Interface	One of the following: *Enable* – This IP logical port is not part of a subnet. It does not have a specific address and instead uses the router ID as its address. *Disable* – This IP logical port is part of a subnet.
Unicast	One of the following: *Enable* – IP forwarding is allowed from this logical port to a unicast address. *Disable* – IP forwarding is not allowed from this logical port to a unicast address. The unicast addresses are specified for each IP interface.
Broadcast	One of the following: *Enable* – IP forwarding is allowed from this logical port to a broadcast address. *Disable* – IP forwarding is not allowed from this logical port to a broadcast address. The broadcast addresses are specified for each IP interface.

Viewing an IP Interface Address

To view an IP interface address:

1. Access the Show IP Parameters dialog box (Figure 8-2) as described in "Viewing IP Logical Ports" on page 8-2.
2. Choose IP Interface. The Show IP Interface Addresses dialog box appears (Figure 8-3).

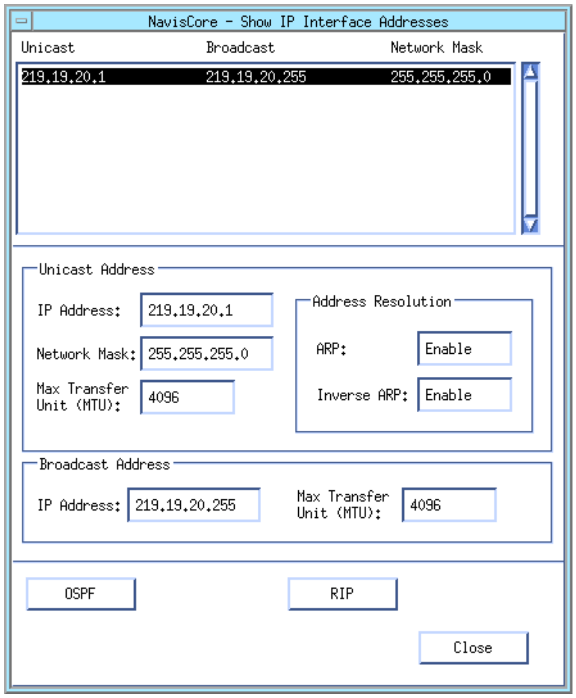


Figure 8-3. Show IP Interface Addresses Dialog Box

3. Select an interface from the list at the top of the dialog box. All fields report information on the selected interface.

Table 8-4 describes the Show IP Interface Addresses dialog fields and buttons.

Table 8-4. Show IP Interface Address Fields and Buttons

Field/Button	Displays.../Function
Unicast Address Fields	
IP Address	The IP address for this interface.
Network Mask	The mask used to determine the subnet of this IP interface.
Max Transfer Unit (MTU)	The maximum size of a packet that can be sent through the physical port. The default value for this field is 1500 bytes.

Table 8-4. Show IP Interface Address Fields and Buttons (Continued)

Field/Button	Displays.../Function
Address Resolution Fields	
ARP	One of the following: *Enable* – Address Resolution Protocol (ARP) is activated on the switch. *Disable* – ARP is disabled on the switch.
Inverse ARP *(Frame Relay Only)*	One of the following: *Enable* – Inverse Address Resolution Protocol (InARP) is activated on the switch. *Disable* – InARP is disabled on the switch.
Broadcast Address Fields	
IP Address	The address used by this interface for subnet broadcasting.
Max Transfer Unit (MTU)	The maximum size of a broadcast packet that can be sent through the physical port. The default value for this field is 1500 bytes.
Buttons	
OSPF	View the OSPF parameters for the logical port.
RIP2	View the RIP parameters for the logical port.

Viewing the Logical Port OSPF Interface

To view an OSPF interface for a logical port:

1. Access the Show IP Interface Addresses dialog box as described in "Viewing an IP Interface Address" on page 8-5.
2. Choose OSPF. The Show OSPF Interface dialog box appears (see Figure 8-4).

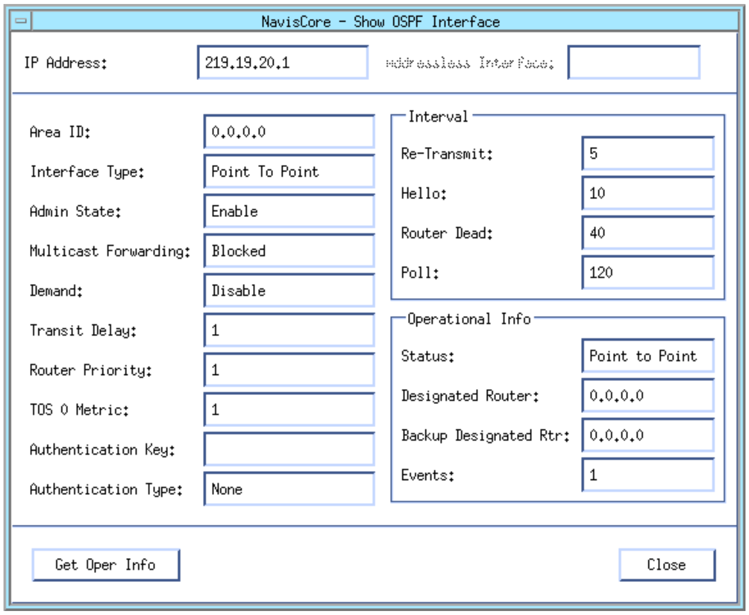


Figure 8-4. Show OSPF Interface Dialog Box

3. Choose Get Oper Info to display, in the Status field, the operational status of the selected logical port.

Table 8-5 describes the Show OSPF Interface dialog box fields.

Table 8-5. Show OSPF Interface Fields

Field	Displays...
Area ID	The ID (x.x.x.x) of the area in which this interface is located. Area 0.0.0.0 is the network backbone area. Areas are collections of networks, hosts, and routers. The area ID identifies the area. ***Note***: *Area 1 (0.0.0.1) is reserved for Ascend switches.*
Interface Type	The logical port interface type, which is one of the following: *Broadcast* – A broadcast network supports many routers and has a designated router that addresses a single physical message to all attached routers. The hello protocol dynamically discovers neighboring routers on these networks. *NBMA* – A non-broadcast multi-access (NBMA) network supports many routers, but does not have broadcast capability. This type of network requires full-mesh connectivity. *Point -to-Point* – A point-to-point network joins two routers together. The IP address of the neighboring router's interface is advertised. Hello packets are sent to the neighbor every *Hello Interval* seconds. *Point-to-Multipoint* – A point-to-multipoint network supports multiple router connections, which are treated like point-to-point connections. The IP addresses of the remote routers' interfaces are advertised. *Virtual Link* – A virtual-link network links areas that are not physically connected to the backbone and patches the backbone if a disconnect occurs in it.
Admin State	One of the following: *Enable* – OSPF is activated on this interface, and this interface can send or receive Hello packets. *Disable* – OSPF is disabled on this interface, and this interface cannot send or receive Hello packets.
Multicast Forwarding	Not Supported.
Demand	Not Supported.
Transit Delay	The estimated number of seconds it takes to transmit a link-state update packet over this interface. Any value between 0 and 3600 is valid; the default value is 1.
Router Priority	The priority of the router associated with this logical port. This value is used to elect the designated and backup designated routers. The router with the highest priority is considered the designated router. If all routers have the same priority, the router ID is used to determine the designated router. Any value between 0 and 255 is valid. A value of 0 indicates the router is not eligible to be the designated or backup designated router.
TOS 0 Metric	The type of service (TOS) cost. The lowest cost has the highest priority for routing. Any value between 1 and 65535 is valid.

Table 8-5. Show OSPF Interface Fields (Continued)

Field	Displays...
Authentication Type	The type of authentication that OSPF uses as a security measure to ensure that this logical port and router exchange information with correct neighbors. Options include: *None* – OSPF performs no authentication. *Simple Password* – OSPF uses a simple password authentication method that includes a password in all OSPF messages, on an interface-by-interface basis. When a router receives a message on an interface that uses simple password authentication, the router checks the incoming OSPF message to see if the password is included in the message. If the password is correct, the message is processed normally. If the password is not part of the incoming message, the message is dropped. *MD5* – OSPF uses the Message Digest Algorithm Version 5 (MD5) encryption method that converts the authentication key to a number. The number, rather than the actual key, is forwarded with the route.
Authentication Key	An authentication password, if the authentication type is *Simple Password* or *MD5*. This value is not required if authentication type is *None*.
Re-Transmit	The number of seconds to wait before resending a packet if no acknowledgment is received. Any value between 0 and 3600 is valid; the default value is 5 seconds.
Hello	The number of seconds between router Hello messages. This is a configurable parameter and controls the frequency of router Hello messages on an interface. Any value between 1 and 65535 is valid; the default value is 10 seconds.
Router Dead	The number of seconds a router waits to hear a Hello message from a neighbor before the router declares the neighbor “down.” The value that you specify can affect OSPF operation. If the interval is too short, neighbors are considered down when they are reachable. If the interval is too long, routers that are unreachable are not considered down soon enough for OSPF to properly reroute data. Any value is greater than or equal to 0 is valid; the default value is 40 seconds. This value is a multiple of the Hello interval. For example, if the Hello interval is set to 10, the router dead interval should be configured at 20, 30, 40, etc. Specify this parameter if you have bad connections or if a link in the network is down.
Poll	The time, in seconds, between Hello packets sent to an inactive NBMA neighbor. Any value greater than or equal to 0 is valid; the default value is 120.

Table 8-5. Show OSPF Interface Fields (Continued)

Field	Displays...
Status	The state of OSPF communication on the interface. The following are options for point-to-point, point-to-multipoint, broadcast, and virtual-link networks: *Up* – The network interface is operational. *Point-to-Point* – The interface is at the highest level of connection. In this state, the interface is operational and connects either to a physical point-to-point network or to a virtual link. Upon entering this state, the router attempts to form an adjacency with the neighboring router. Hello packets are sent to the neighbor based on the setting of the Hello interval. *Init* – The neighbor sees a Hello packet. However, bidirectional communication has not been established with the neighbor. All neighbors in this state are listed in the Hello packets sent from the associated interface. *Down* – The interface is not usable, and no protocol traffic can be sent or received. The following are options for NBMA networks: *Loopback* – The router's interface to the network is "looped back." The interface may be looped back in hardware and software. While in loopback, the interface is not available for regular data traffic. *Waiting* – The router tries to determine the backup designated router's identity. To do this, the router monitors received Hello packets. The router cannot elect a designated router or backup designated router until it leaves the waiting state. This prevents any unnecessary changes to the backup designated router. *Designated Router* – The router is the designated router on the attached network. The router establishes adjacencies to all other routers attached to the network. The router must also originate network link advertisements for the network node. The advertisement provides link information to all routers (including the designated router itself) attached to the network. *Backup Designated Router* – The router is the backup designated router on the attached network. When the designated router fails, this router takes over and performs all tasks of the designated router. The router establishes adjacencies to all other routers attached to the network. *Other* – The router forms adjacencies to both the designated router and the backup designated router.
Designated Router	The 32-bit IP address of the designated router for this network as seen by the advertising router. An IP address of 0.0.0.0 indicates that a designated router has not been specified for this network. If all routers have the same Router Priority, the router ID is used to specify the designated router.
Backup Designated Rtr	The 32-bit IP address of the backup designated router for this network as seen by the advertising router. An IP address of 0.0.0.0 indicates that a backup designated router has not been specified for this network.
Events	The number of times this OSPF interface changed its state, or the number of times an error occurred.

Viewing the Logical Port RIP Parameters

To view the RIP parameters for a logical port:

1. Access the Show IP Interface Addresses dialog box as described in "Viewing an IP Interface Address" on page 8-5.
2. Choose RIP. The Show RIP dialog box appears (see Figure 8-5).

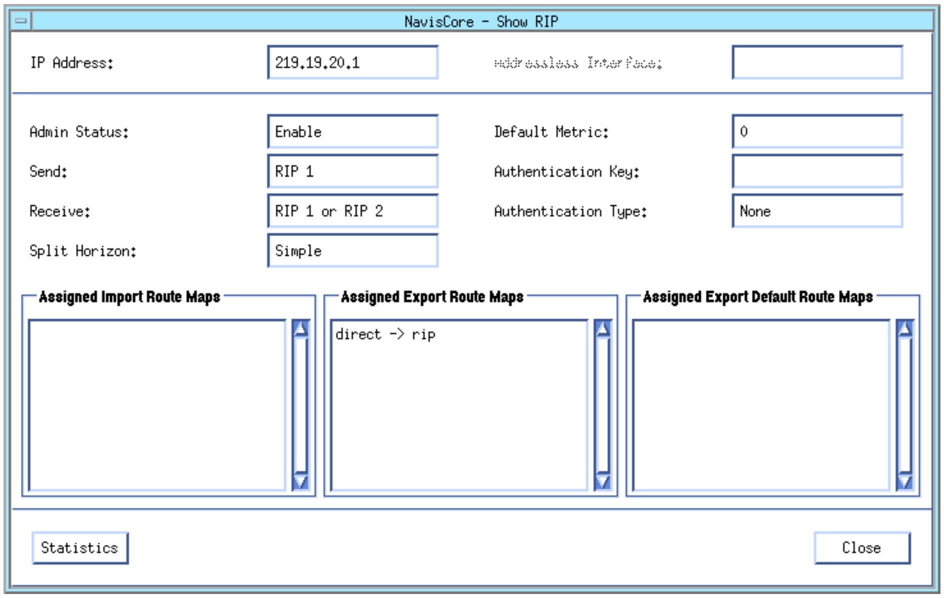


Figure 8-5. Show RIP Dialog Box

Table 8-6 describes the RIP fields.

Table 8-6. Show RIP Fields

Field	Displays...
Admin Status	One of the following: *Enable* – RIP is activated on the logical port and RIP packets can be exchanged over this logical port. *Disable* – RIP has never been activated on the logical port or the logical port is off-line for diagnostics. An IP interface with an Admin Status of *Disable* cannot exchange RIP packets.
Send	One of the following possible values: *Disable*, *RIP 1*, *RIP 1 Compatible*, or *RIP 2*.
Receive	One of the following possible values: *RIP 1*, *RIP 2*, *RIP 1 or RIP 2*, or *Disable*.

Table 8-6. Show RIP Fields (Continued)

Field	Displays...
Split Horizon	One of the following: *Disable* – Split horizon is not used. *Simple* – Split horizon is in use. The simple form of split horizon specifies that if a router learns of a route from an update received on the link, it does not advertise that route on updates that it transmits to the link. *Poison Reverse* – Split horizon is in use in a stronger form. In this form, a router does not omit destinations learned from an interface. Instead, it includes these destinations, but advertises an infinite cost to reach them. This option increases the size of routing updates, but provides a positive indication that a specific location is not reachable through a router. Note that split horizon is a method for avoiding common situations that require counting to infinity.
Default Metric	The metric that is used for the default route entry in RIP updates that originate on this interface. A value of zero indicates that no default route should be originated.
Authentication Key	The authentication password if the authentication type is *Simple* or *MD5*. This field is blank if the authentication type is *None*.
Authentication Type	The type of authentication that RIP uses as a security measure to ensure that this logical port and router are exchanging information with proper neighbors. Possible values are *None*, *Simple*, or *MD5*. *None* – RIP performs no authentication. *Simple* – RIP performs a simple password authentication, which enables you to designate a password that is part of all RIP messages, on an interface-by-interface basis. When a router receives a message on an interface that is using simple password authentication, it checks the incoming RIP message to ensure that the proper password is included in the message. If the password is correct, the message is processed normally. If the password is not part of the incoming message, or an incorrect password is used, the message is dropped. *MD5* – RIP performs MD5 authentication, which is similar to the simple password method; however, the password is not transmitted. Instead, the router uses the MD5 algorithm to create a message digest of the password. The message digest is sent instead of the password. This method prevents the password from being read during transmission.
Assigned Import Route Maps	The import route maps that are assigned to this RIP interface. All incoming routes on this RIP interface are filtered using the assigned route maps in the listed sequence. To display the parameters for any listed route map, double-click on the map.
Assigned Export Route Maps	The export route maps that are assigned to this RIP interface. All outgoing routes on this RIP interface are filtered using the assigned route maps in the listed sequence. To display the parameters for any listed route map, double-click on the map.

Table 8-6. Show RIP Fields (Continued)

Field	Displays...
Assigned Export Default Route Maps	The export default route maps that are assigned to this RIP interface. All outgoing routes on this RIP interface are filtered using the assigned route maps in the listed sequence. To display the parameters for any listed route map, double-click on the map.

Viewing RIP Statistics

To view RIP statistics:

1. Access the Show RIP dialog box as described in "Viewing the Logical Port RIP Parameters" on page 8-11.
2. Choose Statistics. The RIP2 Statistics dialog box appears (see Figure 8-6).

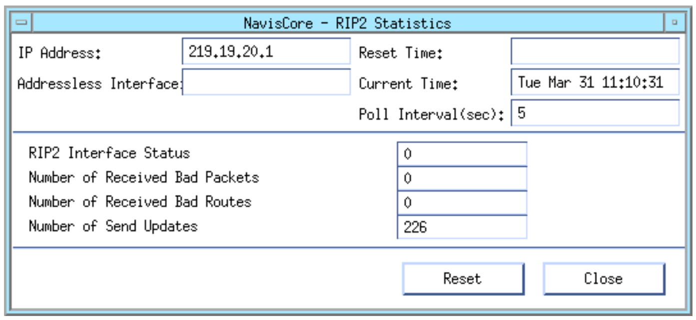


Figure 8-6. RIP2 Statistics Dialog Box

> A warm boot clears all of the cumulative statistics and resets the counters.

3. Choose Reset to clear all statistics counters.

Table 8-7 describes the RIP2 Statistics fields.

Table 8-7. RIP2 Statistics

Field	Displays...
Identifying Fields	
IP Address	The Ethernet IP address of the switch on the subnet. For unnumbered interfaces, the system displays a value of 0.0.0.N where the least significant 24 bits (N) represent the ifIndex for the IP interface.
Addressless Interface	A value that identifies an addressless interface. If the interface has an IP address, the field is blank. If the interface is addressless, the value is the internal router ID.
Reset Time	The time of the last counter reset.
Current Time	The current system time.
Poll Interval (sec)	The time interval for the collection of statistical data. See "Setting the Polling Interval" on page 3-2 for information about setting the poll interval.
Cumulative Statistics	
RIP2 Interface Status	The status of the RIP2 logical port interface.
Number of Received Bad Packets	The number of RIP response packets received by the RIP process that were discarded for any reason (for example, a version 0 packet or an unknown command type).
Number of Received Bad Routes	The number of routes (in valid RIP packets) that were ignored for any reason (for example, an unknown address family or an invalid metric).
Number of Send Updates	The number of triggered RIP updates sent from this interface. This counter does not include full updates that were sent containing new information.

Viewing Packet Filters

> You must be logged on to access this function.

To view the packet filters that are currently assigned to a logical port:

1. Access the Show IP Parameters dialog box as described in "Viewing IP Logical Ports" on page 8-2.
2. Choose Packet Filter. The Assign Logical Port IP Filter dialog box appears (see Figure 8-7). The Available Filters column lists the packet filters that are available for use with this logical port. The Assigned Filters column lists the packet filters assigned to this logical port.

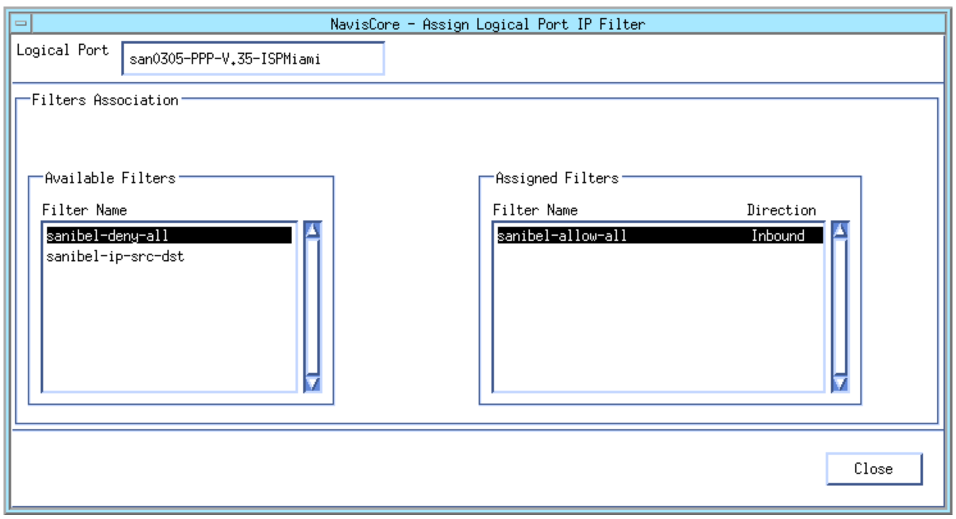


Figure 8-7. Assign Logical Port IP Filter Dialog Box

Viewing a DLCI Data Link ID

To view a DLCI:

1. Access the Show IP Parameters dialog box as described in "Viewing IP Logical Ports" on page 8-2.
2. Choose DLCI. The Show IP Interface Data Link ID dialog box appears (see Figure 8-8).

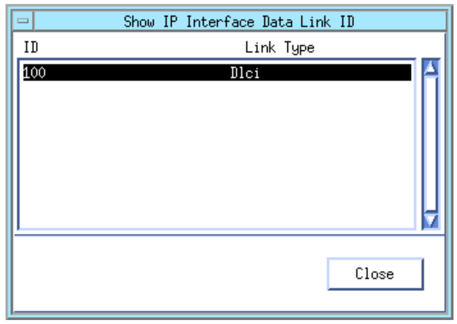


Figure 8-8. Show IP Interface Data Link ID Dialog Box (DLCI)

Table 8-8 describes the Show IP Interface fields.

Table 8-8. Show IP Interface Data Link ID Fields (DLCI)

Field	Displays...
ID	The DLCI value for this IP interface. The DLCI value identifies the Frame Relay link that IP uses to send and receive data.
Link Type	Displays DLCI, indicating that the logical port uses a Frame Relay link.

Viewing a VPI/VCI Data Link ID

To view a VPI/VCI:

1. Access the Show IP Parameters dialog box as described in "Viewing IP Logical Ports" on page 8-2.
2. Choose VPI/VCI. The Show IP Interface Data Link ID dialog box appears (see Figure 8-8).

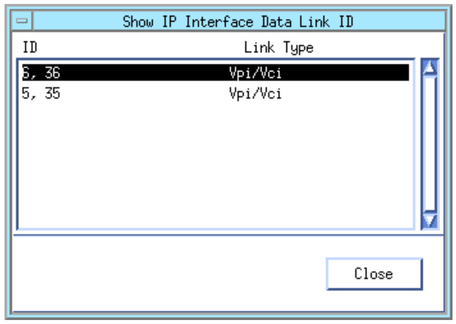


Figure 8-9. Show IP Interface Data Link ID Dialog Box (VPI/VCI)

Table 8-8 describes the Show IP Interface fields.

Table 8-9. Show IP Interface Data Link ID Fields (VPI/VCI)

Field	Displays...
ID	The VPI/VCI identifier of the ATM link that IP uses to send and receive data. The virtual path identifier (VPI) is the first number. The virtual channel identifier (VCI) is shown after the comma.
Link Type	Displays VPI/VCI, indicating that the logical port uses an ATM link.

Viewing IP Logical Port Statistics

The IP LPort Statistics dialog box displays information about the transmission and receipt of data on the logical port. Cumulative Statistics list the number of each type of packet (received, transmitted, or tagged due to an error). Throughput fields display the bits and packets per second for the logical port.

To view IP logical port statistics:

1. Access the Show IP Parameters dialog box as described in "Viewing IP Logical Ports" on page 8-2.
2. Choose Statistics. The IP LPort Statistics dialog box appears (see Figure 8-10).

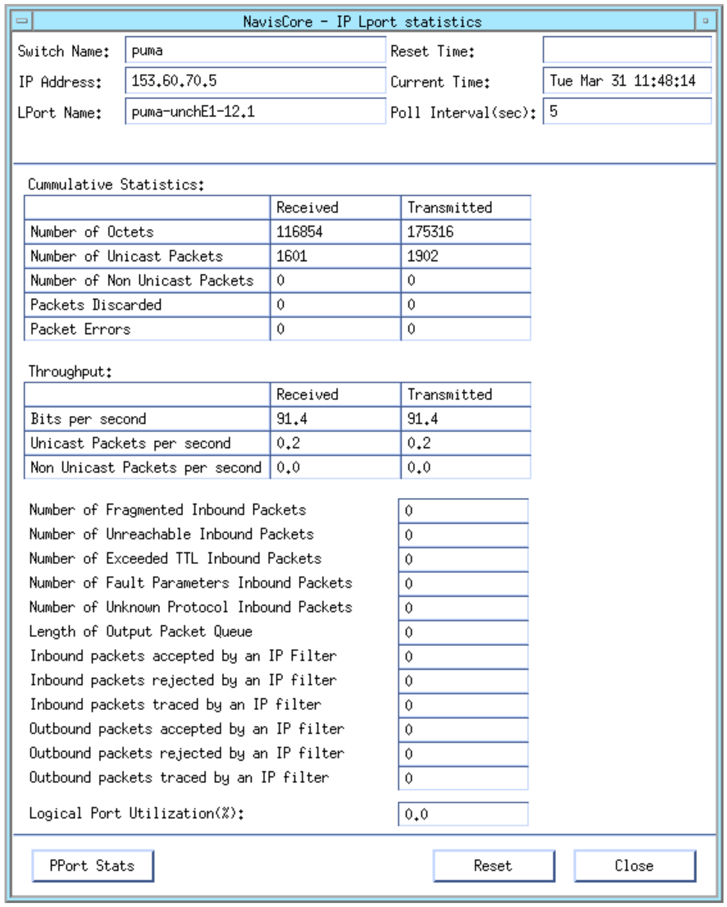


Figure 8-10. IP LPort Statistics Dialog Box

> The Logical Port Utilization field measures the traffic queued for transmission on a logical port as a percentage of the logical port speed. It does not measure the amount of logical port bandwidth. Therefore, the Logical Port Utilization field value can exceed 100%.
>
> A warm boot clears all of the cumulative statistics and resets the counters.

3. Choose Reset to clear the statistics counters.
4. Choose PPort Stats to display the physical port statistics for the logical port. For more information about physical port statistics, see Chapter 3, "Generating Physical Port Statistics."

Table 8-10 describes the IP logical port statistics fields.

Table 8-10. IP LPort Statistics

Statistic	Description
Cumulative Statistics	
Number of Octets	The number of octets received since the last reset.
Number of Unicast Packets	The number of unicast packets received since the last reset.
Number of Non Unicast Packets	The number of nonunicast packets received since the last reset.
Packets Discarded	The number of packets (frames) received and discarded since the last reset.
Packet Errors	The number of packet errors received since the last reset.
Throughput Statistics	
Bits per Second	The total number of bits received and transmitted each second.
Unicast Packets per Second	The total number of unicast packets received and transmitted each second.
Non Unicast Packets per Second	The total number of nonunicast packets received and transmitted each second.
Number of Fragmented Inbound Packets	The number of received IP packets that were fragmented because the packet size was greater than the transmit Maximum Transit Unit (MTU) size.

Table 8-10. IP LPort Statistics (Continued)

Statistic	Description
Number of Unreachable Inbound Packets	The number of inbound packets that had a *destination unreachable* condition. The router had no route to the IP destination indicated by the Destination Address (DA) in the IP packet.
Number of Exceeded TTL Inbound Packets	The number of inbound packets that had a *Time-to-Live (TTL) Exceeded* condition. This counter is decremented at each hop. If the counter equals zero, the packet is discarded. The purpose of TTL is to prevent packets from endlessly circulating on the network.
Number of Fault Parameters Inbound Packets	The number of inbound packets that had a *Parameter Errors* condition. A parameter error is any value in the header that either appears incorrectly or cannot be interpreted.
Number of Unknown Protocol Inbound Packets	The number of unknown protocol inbound packets. This counter does not apply to traffic that passes through the router (or Ascend switch). Instead, it applies to traffic destined for any IP entity (such as a router or an end station). This counter is incremented when the IP protocol stack has no packet destination (because there is no IP entity that is interested in this protocol).
Length of Output Packet Queue	The length of the transmit queue, that indicates the level of congestion on the logical port.
Inbound packets accepted by an IP filter	The number of packets that arrived at the port with inbound IP filters and were accepted because the IP filter matched the packet and specified acceptance of the packet as a result of the match.
Inbound packets rejected by an IP filter	The number of packets that arrived at the port with inbound IP filters and were rejected because the IP filter matched the packet and specified rejection of the packet as a result of the match.
Inbound packets traced by an IP filter	The number of packets that arrived at the port with inbound IP filters and were traced because the IP filter matched the packet and specified packet tracing as a result of the match.
Outbound packets accepted by an IP filter	The number of packets that arrived at the port with outbound IP filters and were accepted because the IP filter matched the packet and specified acceptance of the packet as a result of the match.
Outbound packets rejected by an IP filter	The number of packets that arrived at the port with outbound IP filters and were rejected because the IP filter matched the packet and specified rejection of the packet as a result of the match.
Outbound packets traced by an IP filter	The number of packets that arrived at the port with outbound IP filters and were traced because the IP filter matched the packet and specified packet tracing as a result of the match.

Table 8-10. IP LPort Statistics (Continued)

Statistic	Description
Utilization Statistic	
Logical Port Utilization	The amount of traffic queued for transmission on a logical port as a percentage of the committed information rate (CIR). This statistic does not measure the amount of bandwidth of the logical port. For this reason, the displayed value can exceed 100%.

Viewing OSPF Information

This section describes how to view the following objects:

- IP parameters
- Neighbors
- Area aggregates
- Virtual links

Viewing IP Parameters

To view IP parameters:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show IP Parameters. The Show IP Parameters dialog box appears (see Figure 8-12).

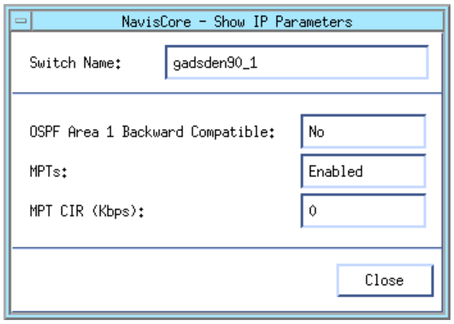


Figure 8-11. Show IP Parameters Dialog Box

Table 8-11 describes the IP parameters fields.

Table 8-11. Show IP Parameters Field Descriptions

Field	Displays...
OSPF Area 1 Backward Compatible	Whether the switch is OSPF Area 1 backward compatible (*Yes* or *No*). If the field displays *Yes*, the switch: • Can communicate with other Ascend switches running pre-5.0 switch software. • Can communicate with other Ascend switches running 5.0 switch software. • **Cannot** communicate with other vendor routers. If the field displays *No*, the switch: • Cannot communicate with other Ascend switches running pre-5.0 switch software. • Can communicate with other Ascend switches running 5.0 switch software. • **Can** communicate with other vendor routers.
MPT	Whether the Multipoint-to-Point (MPT) administrative value for the switch is enabled. This field must be set to *Enabled* in order for the switch to process MPT tunnels. The setting of the MPT administrative value determines how the switch uses MPTs: • If MPTs are enabled and no IP interfaces are defined, the switch does not establish MPTs. • If MPTs are enabled and IP interfaces are defined, the switch establishes MPTs as a means of forwarding IP traffic. • If MPTs are disabled and IP interfaces are defined, the switch does not establish MPTs as a means of forwarding IP traffic, but instead uses a hop-by-hop transmission method. • If MPTs are disabled and no IP interfaces are defined, the switch does not establish MPTs.
MPT CIR (Kbps) (Multipoint-to-Point Tunneling Committed Information Rate)	The rate in Kbps at which the MPT transfers data, averaged over a minimum increment of time. In addition, this value enables the switch to reserve bandwidth for MPTs that the switch originates. ***Note:*** *This value applies to all links in the MPT.*

Viewing OSPF Neighbors

To view OSPF neighbors:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All OSPF ⇒ Show All OSPF Neighbors. The Show All OSPF Neighbors dialog box appears (see Figure 8-12).

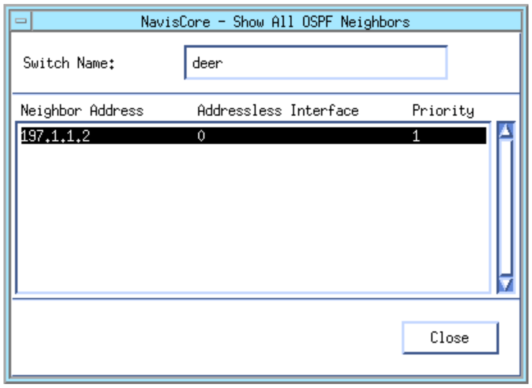


Figure 8-12. Show All OSPF Neighbors Dialog Box

Table 8-12 describes the OSPF Neighbor fields.

Table 8-12. Show OSPF Neighbor Fields

Field	Displays...
Neighbor Address	The IP address this neighbor uses in its IP source address. On addressless links, the address is the address of the neighbor's interface.
Addressless Interface	The addressless interface. If the interface has an IP address, the value is 0.0.0.0. If the interface is addressless, the value is the internal router ID.
Priority	A value between 0 and 255. The neighbor with the highest priority is the designated router. This field only applies to NBMA and broadcast networks. The value zero signifies the neighbor cannot be the designated router on this network.

Viewing OSPF Area Aggregates

To view an OSPF area aggregate:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All OSPF ⇒ Show All OSPF Area Aggregates. The Show All OSPF Area Aggregates dialog box appears (see Figure 8-13).

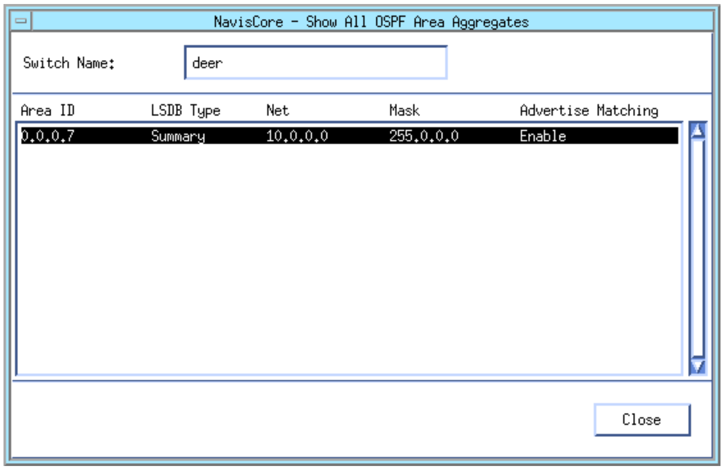


Figure 8-13. Show All OSPF Area Aggregates Dialog Box

Table 8-13 describes OSPF Area Aggregate fields.

Table 8-13. Show All OSPF Area Aggregates Fields

Field	Displays...
Area ID	The ID (x.x.x.x) of the area in which the node is located. Area 0.0.0.0 is the network backbone. Areas are collections of networks, hosts, and routers. The area ID identifies the area. ***Note***: *Area 1 is reserved for Ascend switches.*
LSDB Type	The link state database (LSDB) type to which this address aggregate applies. Options include: *Summary* – Area border routers generate summary link advertisements, which describe inter-area routes (routes between areas) to networks. *NSSA External* – Not So Stubby Area (NSSA) external link advertisements allow an AS border router within a stub area and the routers within that area to learn about the external networks accessible through the AS border router in the area.
Net	The IP address of the net or subnet.
Mask	The subnet mask that pertains to the net or subnet.

Table 8-13. Show All OSPF Area Aggregates Fields (Continued)

Field	Displays...
Advertise Matching	One of the following: *Enable* – The net/mask combination specified for the given area is “leaked” (i.e., advertised). *Disable* – The net/mask combination specified for the given area is hidden.

Viewing OSPF Virtual Links

To view an OSPF switch’s virtual links:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All OSPF ⇒ Show All OSPF Virtual Links. The Show All OSPF Virtual Links dialog box appears (see Figure 8-14).

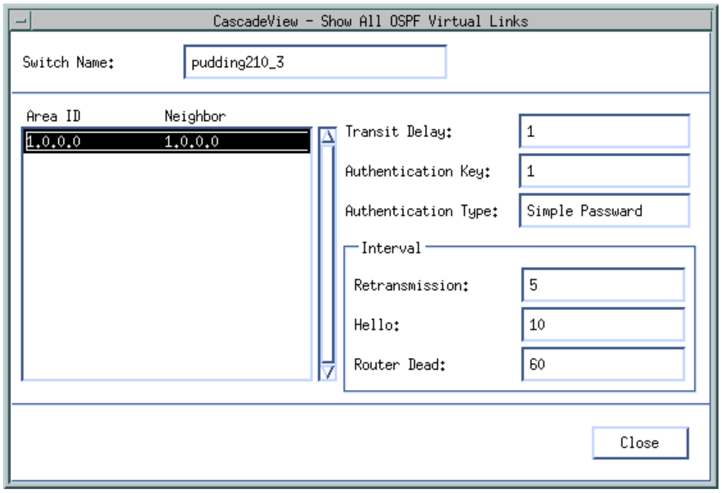


Figure 8-14. Show All OSPF Virtual Links Dialog Box

Table 8-14 describes the OSPF Virtual Link fields.

Table 8-14. Show All OSPF Virtual Link Fields

Field	Displays...
Area ID	The area ID (x.x.x.x) in which you want to locate the neighbor. Area 0.0.0.0 is the network backbone area. Areas are collections of networks, hosts, and routers. The area ID identifies the area. ***Note**: Area 1 is reserved for Ascend switches.*
Neighbor	The IP address this neighbor uses in its IP source address. On addressless links, the address is the address of the neighbor's interface.
Transit Delay	The estimated number of seconds it takes to transmit a link-state update packet over this interface. Any value between 0 and 3600 is valid; the default value is 1.
Authentication Key	The authentication password, if used with *Simple* or *MD5* as the authentication type. This field is blank if the authentication type is *None*.
Authentication Type	The type of authentication that OSPF uses as a security measure to ensure that this logical port and router exchange information with correct neighbors. Options include: *None* – OSPF performs no authentication. *Simple Password* – OSPF uses a simple password authentication method that includes a password in all OSPF messages, on an interface-by-interface basis. When a router receives a message on an interface that uses simple password authentication, the router checks the incoming OSPF message to see if the password is included in the message. If the password is correct, the message is processed normally. If the password is not part of the incoming message, the message is dropped. *MD5* – OSPF uses the MD5 encryption method that converts the authentication key to a number. The number, rather than the actual key, is forwarded with the route.
Interval	
Retransmission	The number of seconds to wait before resending a packet if no acknowledgment is received. Any value between 0 and 3600 is valid; the default value is 5 seconds.
Hello	The number of seconds between router Hello messages. This is a configurable parameter and controls the frequency of router Hello messages on an interface. Any value between 1 and 65535 is valid; the default value is 10 seconds.

Table 8-14. Show All OSPF Virtual Link Fields (Continued)

Field	Displays...
Router Dead	The number of seconds a router waits to hear a Hello message from a neighbor before the router declares the neighbor "down." The value that you specify can affect OSPF operation. If the interval is too short, neighbors are considered down when they are reachable. If the interval is too long, routers that are unreachable are not considered down soon enough for OSPF to properly reroute data. Any value is greater than or equal to 0 is valid; the default value is 40 seconds. This value is a multiple of the Hello interval. For example, if the Hello interval is set to 10, the router dead interval should be configured at 20, 30, 40, etc. Specify this parameter if you have bad connections or if a link in the network is down.

Viewing OSPF Route Maps

To view an OSPF route map:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All OSPF ⇒ Show All OSPF Route Maps. The Show All OSPF Route Maps dialog box appears (see Figure 8-15).

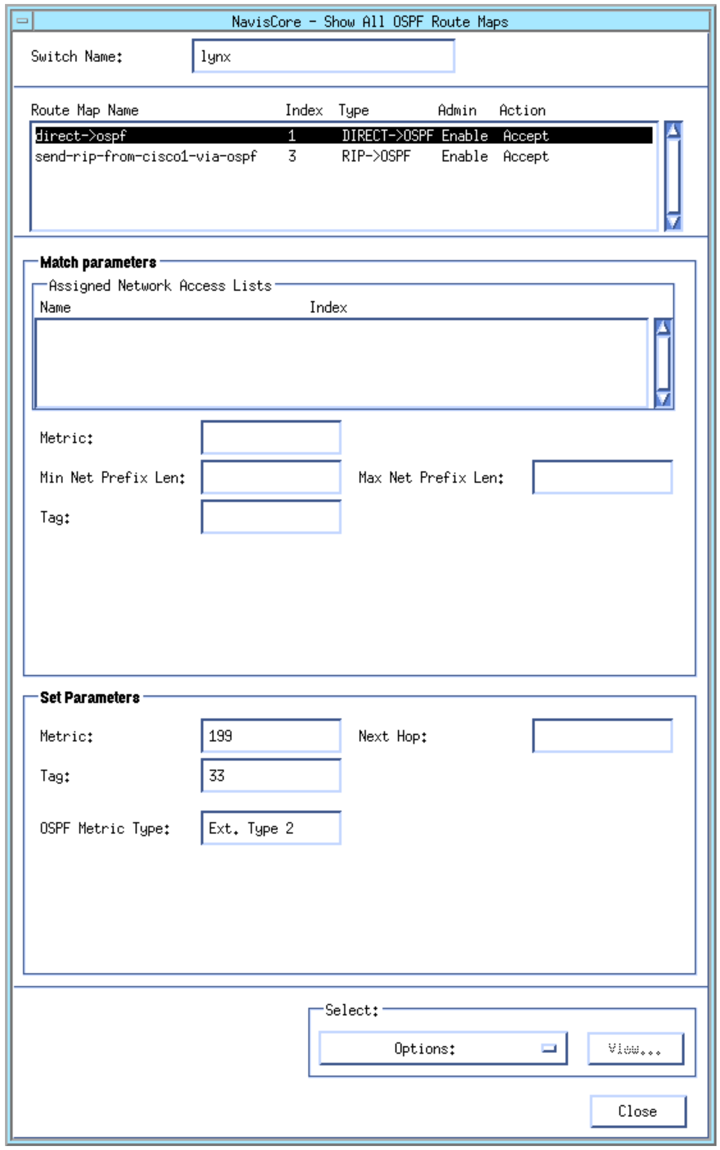


Figure 8-15. Show All OSPF Route Maps Dialog Box

Note that the Match parameters and Set parameters vary depending on the type of route map that you are defining. See the *NavisCore IP Navigator Configuration Guide* for information about the Match and Set parameters for each route map type.

Table 8-15 describes each of the common fields shown at the top of the Show All OSPF Route Maps dialog box.

Table 8-15. Show All OSPF Route Maps Common Values

Field	Displays...
Route Map Name	A name that uniquely identifies the route map.
Index	The index field, which is generated by NavisCore and is unique within the switch.
Type	The From protocol and To protocol that identify the route distribution type.
Admin	One of the following: *Enable* – The route map is administratively enabled and can be used. *Disable* – The route map is administratively disabled and cannot be used.
Action	One of the following: *Accept* – All routes that match the specified Match parameters are accepted. *Deny* – All routes that match the specified Match parameters are denied. *Originate Default* – The match parameters that define where to send a default route heading are configurable. This option is used for the following types of route maps: • BGP to BGP • ANY to BGP • RIP to RIP

Viewing BGP Information

This section describes how to view the following objects:

- Switch parameters
- Neighbors
- Neighbor connection statistics
- Aggregates
- BGP path attributes

Viewing BGP Switch Parameters

To view a BGP switch:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All BGP ⇒ Show All BGP Parameters. The Show BGP dialog box appears (see Figure 8-16).

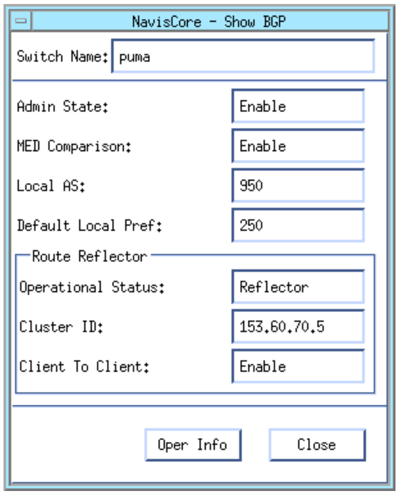


Figure 8-16. Show BGP Dialog Box

3. Choose Oper Info to display, in the Operational Status field, a status message for the selected port.

Table 8-16 describes the BGP fields.

Table 8-16. Show BGP Fields

Field	Displays...
Admin State	One of the following: *Enable* – The selected switch is communicating using BGP. *Disable* – The selected switch is not communicating using BGP.
MED Comparison	One of the following: *Enable* – A multi-exit discriminator (MED) is being used in the route selection process. MED allows BGP to communicate preferred path information to external neighbors when the autonomous system has multiple exits to another autonomous system. *Disable* – MED is not being used the route selection process.
Local AS	The switch's autonomous system (AS) number. Any value between 1 and 65535 is valid.
Default Local Pref	The value sent to internal neighbors, used for ranking a route according to its importance. The local preference is compared to other routes that have the same destination. A higher local preference indicates the route is preferred. Any value between 1 and 4294967295 is valid; the default is 100.
Route Reflector	
Operational Status	Whether or not this peer is a route reflector. If it is, the peer forwards route information to all clients. The route reflector is implicitly defined when you define any of its peers to be a route reflector client.
Cluster ID	The internal IP address of the selected switch, if the switch is a route reflector in a cluster that contains more than one route reflector. A cluster is a group of client peers that communicate with a BGP route reflector. A cluster ID specifies the cluster.
Client To Client (For IBGP peers only)	One of the following: *Enable* – Any routes that are received by the selected switch from a client are sent to all other clients (the default). *Disable* – Any routes that are received by the selected switch from a client are not sent to all other clients.

Viewing BGP Neighbors

To view a BGP neighbor:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All BGP ⇒ Show All BGP Neighbors. The Show All BGP Neighbors dialog box appears (see Figure 8-17).

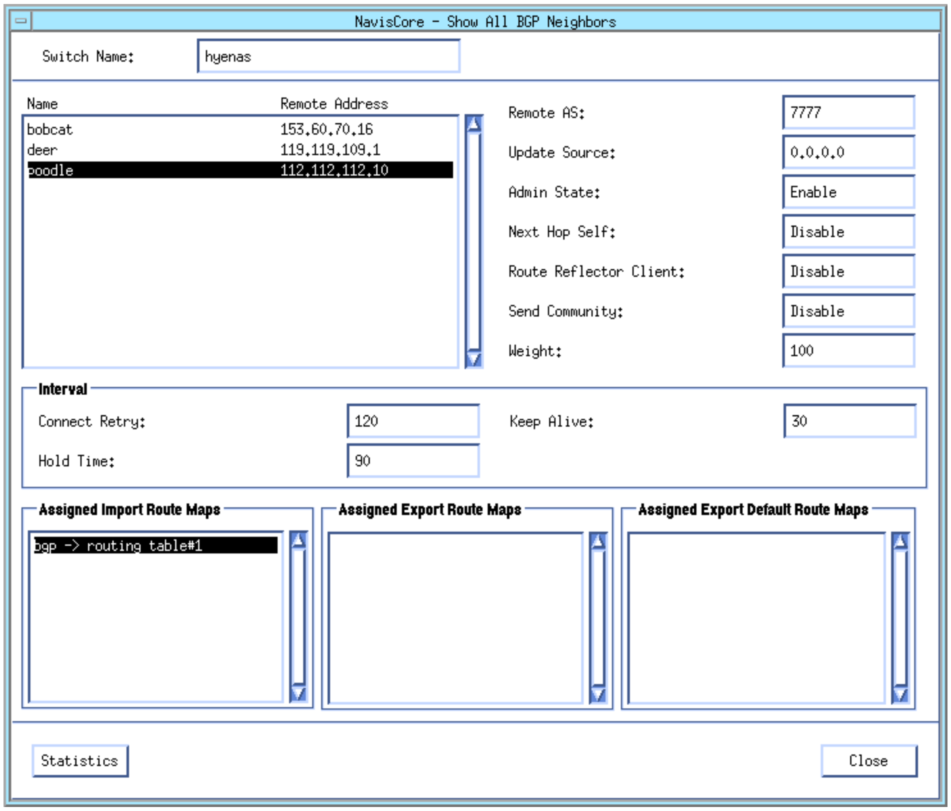


Figure 8-17. Show All BGP Neighbors Dialog Box

3. Use the Statistics button to display BGP peer connection statistics. For more information, see "Viewing BGP Connection Statistics" on page 8-34.

Table 8-17 describes the BGP Neighbor fields.

Table 8-17. BGP Neighbor Fields

Field	Displays...
Name	The name of the BGP neighbor.
Remote Address	The IP address of the BGP neighbor.
Remote AS	The neighbor's remote AS number. Any value between 1 and 65535 is valid.
Update Source	A valid IP address for the Update Source address, which is the source address for the BGP TCP connection.
Admin State	One of the following: *Enable* – The connection between the selected switch and this BGP neighbor is active. *Disable* – The connection between the selected switch and this BGP neighbor is deactivated.
Next Hop Self	One of the following: *Enable* – For IBGP peers, BGP must advertise the local address of the BGP connection as the next hop. For EBGP peers, BGP always advertises the local address as the next hop; therefore you do not need to enable next hop self for EBGP peers. *Disable* – BGP determines the next hop.
Route Reflector Client	One of the following: *Enable* – The selected switch's neighbor is defined as a route reflector client, implicitly making the selected switch a route reflector. *Disable* – The selected switch's neighbor is not defined as a route reflector client. In addition, if you disable this parameter on all of the selected switch's BGP neighbors, the selected switch is not defined as a route reflector. However, if the route reflector client is enabled on at least one BGP neighbor, the selected switch is still considered a route reflector.
Send Community	One of the following: *Enable* – Sends community attributes of all updates to this neighbor. A community is a group of destinations that share some common property. A community is not restricted to one network or autonomous system; it has no physical boundaries. You use community attributes to simplify routing policies by identifying routes based on the logical property rather than IP prefix or AS number. *Disable* – Community attributes of all updates are not sent to this neighbor.
Weight	The path weight (received by the neighbor) that is applied to every route. IP Navigator applies the weight value to EBGP routes only. It does not use the weight value for IBGP routes. Any value between 0 and 65535 is valid; the default value is zero.
Connect Retry	The time, in seconds, that BGP waits before it tries to connect to this neighbor. The number of connection retries due to errors are generated with no regard to this value. The initial value is 60 seconds; the value is doubled with each retry.

Table 8-17. BGP Neighbor Fields (Continued)

Field	Displays...
Hold Time	The time, in seconds, BGP waits before considering the connection to be down if messages are not received from this neighbor. A value of 0 or a range of 3 to 65535 is valid; the default is 90. The value 0 indicates not to use hold time with this neighbor.
Keep Alive	The time, in seconds, between consecutive keep-alive messages sent to this neighbor. This event occurs after a connection is established. Keep-alive messages are sent periodically between BGP neighbors to ensure that the connection is still alive. Any value between 0 and 21845 is valid; the default is 30.
Assigned Import Route Maps	The import route maps that are assigned to this BGP neighbor. All incoming routes on this BGP neighbor are filtered using the assigned route maps in the listed sequence. To display the parameters for any listed route map, double-click on the map.
Assigned Export Route Maps	The export route maps that are assigned to this BGP neighbor. All outgoing routes on this BGP neighbor are filtered using the assigned route maps in the listed sequence. To display the parameters for any listed route map, double-click on the map.
Assigned Export Default Route Maps	The export default route maps that are assigned to this BGP neighbor. All outgoing routes on this BGP neighbor are filtered using the assigned route maps in the listed sequence. To display the parameters for any listed route map, double-click on the map.

Viewing BGP Connection Statistics

To view BGP connection statistics:

1. Access the Show All BGP Neighbors dialog box as described in "Viewing BGP Neighbors" on page 8-32.
2. Choose Statistics. The BGP Peer Connection Statistics dialog box appears (see Figure 8-18).

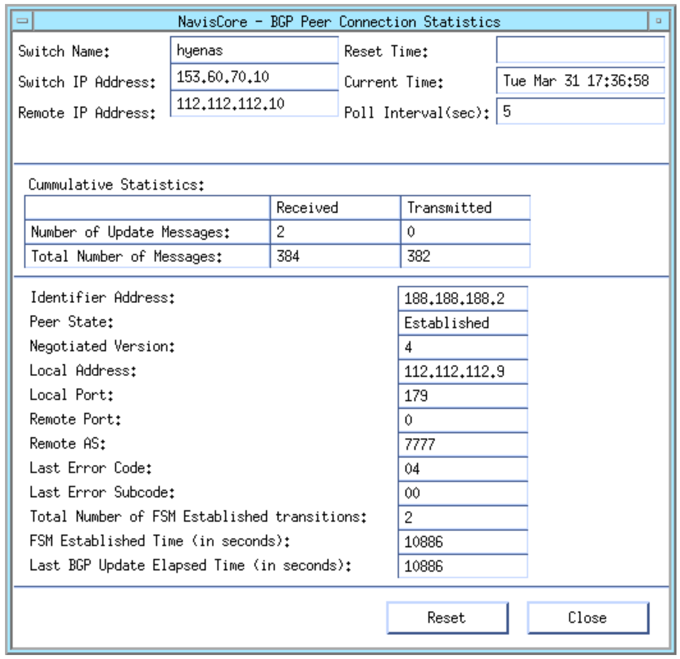


Figure 8-18. BGP Peer Connection Statistics Dialog Box

The BGP Peer Connection Statistics dialog box displays data in separate columns to reflect the transmission and receipt of data on the switch. **Cumulative Statistics** list the number of each type of packet (received, transmitted, or tagged due to an error).

3. Choose Reset to clear the statistics counters.

Table 8-18 describes each of the BGP Peer Connection Statistics.

Table 8-18. BGP Peer Connection Statistics

Field	Displays...
Cumulative Statistics	
Number of Update Messages	The number of BGP update messages this connection transmitted or received.
Total Number of Messages	The total number of messages this connection transmitted to or from a remote peer.
Identifier Address	The 4-byte unsigned integer that indicates the sender’s ID.

Table 8-18. BGP Peer Connection Statistics (Continued)

Field	Displays...
Peer State	One of the BGP peer connection states: *Idle* – BGP waits for the operator to initiate a start event. BGP initiates a TCP connection and listens for a connection, which may be initiated by a peer. After BGP is initialized, it advances to the Connect state. *Connect* – BGP waits for TCP to complete. If the TCP connection completes, BGP advances to the Opensent state. If the TCP connection fails, BGP advances to the Active state. *Active* – BGP tries to establish peering through a TCP connection. If the connection is successful, BGP transmits an Open message and advances to the Opensent stage. If the TCP connection retry timer expires, BGP restarts the connection timer and retreats to the Connect state. *Opensent* – BGP sends an Open message to its peer and waits for an Open message. Once the message is received, the message is checked for correctness, which includes the router ID, BGP version, AS number, and hold timer. If errors occur, the system sends an error notification message and returns to the Idle state. If there are no errors, BGP sends keep-alive messages. *Openconfirm* – BGP waits for keep-alive messages from its peer. If the message is received, the session advances to the Established state. *Established* – The final state of the BGP connection state.
Negotiated Version	The negotiated version of BGP running between two peers.
Local Address	The local IP address of this entry's BGP connection.
Local Port	The local port that establishes a TCP connection between the BGP peers.
Remote Port	The remote port that establishes a TCP connection between the BGP peers.
Remote AS	The remote AS number.
Last Error Code	The last error code seen by this peer. An error code is part of the notification message that is sent whenever an error occurs. See Table 8-19 for more information on last error codes.
Last Error Subcode	The last error subcode seen by this peer. An error subcode is part of the notification message. The last error subcode provides more specific information about the nature of the error. See Table 8-19 for more information on last error subcodes.
Total Number of FSM Established transitions	The total number of times the BGP Finite State Machine (FSM) transitioned into the Established state. The BGP FSM is a process BGP goes through to determine its connection state.

Table 8-18. BGP Peer Connection Statistics (Continued)

Field	Displays...
FSM Established Time	This timer indicates, in seconds, one of the following: • How long this peer has been in the Established state. • How long since this peer was last in the Established state. The timer is set to zero when you configure a new peer or you boot the router.
Last BGP Update Elapsed Time	The number of seconds since this peer received the last BGP update message.

Table 8-19. BGP Error Codes

Last Error Code	Last Error Subcode
1 – Message Header Error	1 – Connection Not Synchronized
	2 – Bad Message Length
	3 – Bad Message Type
2 – OPEN Message Error	1 – Unsupported Version Number
	2 – Bad Peer AS
	3 – Bad BGP Identifier
	4 – Unsupported Optional Parameter
	5 – Authentication Failure
	6 – Unacceptable Hold Timer

Table 8-19. BGP Error Codes (Continued)

Last Error Code	Last Error Subcode
3 – UPDATE Message Error	1 – Malformed Attribute List
	2 – Unrecognized Well-Known Attribute
	3 – Missing Well-Known Attribute
	4 – Attribute Flags Error
	5 – Attribute Length Error
	6 – Invalid Origin Attribute
	7 – AS Routing Loop
	8 – Invalid NEXT_HOP Attribute
	9 – Optional Attribute Error
	10 – Invalid Network Field
	11 – Malformed AS_path
4 – Hold Timer Expired	Not applicable
5 – Finite State Machine Error (for errors detected by the FSM)	Not applicable
6 – Cease (for fatal errors besides the ones already listed)	Not applicable

Viewing BGP Aggregates

To view a BGP area aggregate:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All BGP ⇒ Show All BGP Aggregates. The Show All BGP Aggregates dialog box appears (see Figure 8-19).

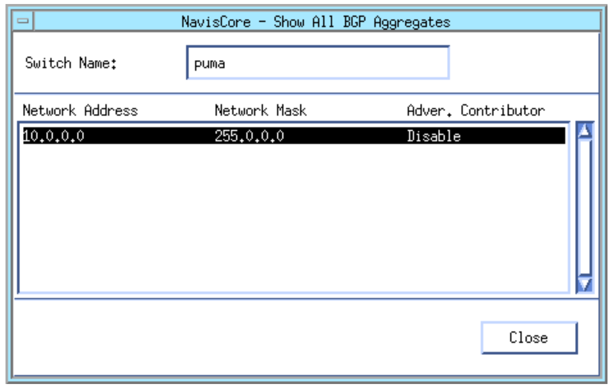


Figure 8-19. Show All BGP Aggregates

Table 8-20 describes the BGP Aggregate fields.

Table 8-20. BGP Aggregate Fields

Field	Description
Network Address	The aggregate network IP address.
Network Mask	The aggregate network mask.
Adver. Contributor	One of the following: *Enable* – Advertises components of the aggregate network. *Disable* – Components of the aggregate network are not advertised.

Viewing BGP Path Attributes

BGP attributes are parameters that describe characteristics of a route. The BGP decision process uses these attributes to select the best routes. This section describes BGP switch path attributes.

To view a BGP switch's path attributes:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All BGP ⇒ Show All BGP Path Attributes. The Show All BGP Path Attributes dialog box appears (see Figure 8-20).

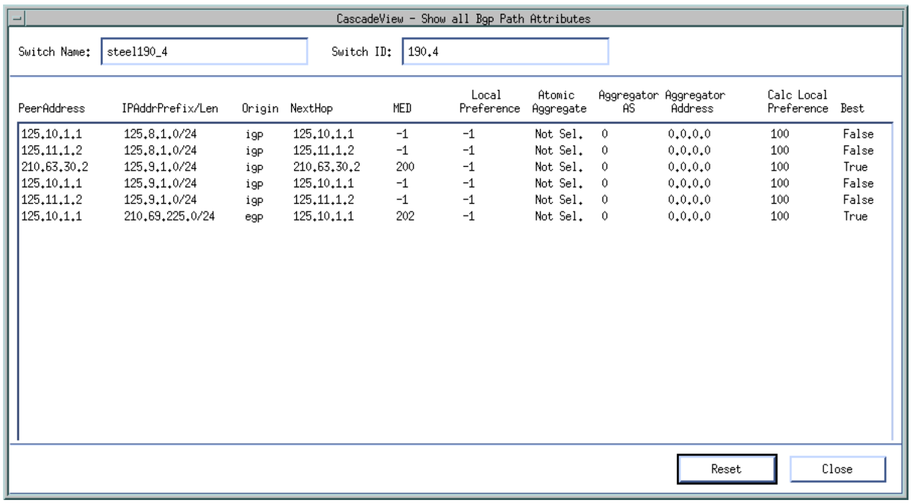


Figure 8-20. Show All BGP Path Attributes Dialog Box

3. Choose Reset to clear each of the counters.

Table 8-21 describes the fields on the Show All BGP Path Attributes dialog box.

Table 8-21. Show All BGP Path Attributes Fields

Field	Displays...
Peer Address	The IP address of the peer that sent the route information.
IPAddrPrefix/Len	The IP address prefix in the network layer reachability information field, separated by a slash (/), from the length, in bits, of the IP address prefix in the network reachability information field. Possible values are between 0 and 32.
Origin	The origin of the path information. Possible values are: *igp* – Networks learned through interior gateway protocol. *egp* – Networks learned through exterior gateway protocol. *incomplete* – Undetermined.

Table 8-21. Show All BGP Path Attributes Fields (Continued)

Field	Displays...
NextHop	The IP address of the border router that is used for the destination network.
MED	The multi-exit discriminator (MED) metric. BGP uses MED to communicate preferred path information to external neighbors when the autonomous system has multiple exits to another autonomous system. Possible values are between -1 and 2147483647. A value of -1 indicates that this attribute does not apply.
Local Preference	The original BGP speaker's preference for an advertised route. Possible values are between -1 and 2147483647. A higher local preference indicates the route is preferred. A value of -1 indicates that this attribute does not apply.
Atomic Aggregate	The BGP speaker uses this parameter to inform other BGP speakers that the local system selected a less specific route without selecting a more specific route. A BGP speaker is a router in an Autonomous System (AS). Possible values are: • Not Selected • Selected
Aggregator AS	The AS number of the last BGP speaker that performed route aggregation. A value of 0 indicates this attribute does not apply.
Aggregator Address	The IP address of the last BGP speaker that performed route aggregation. A value of 0.0.0.0 indicates this attribute does not apply.
Calc Local Preference	The BGP speaker's preference for an advertised route. Possible values are between -1 and 2147483647. A value of -1 indicates this attribute does not apply.
Best	Indicates if this route was chosen as the best BGP route. Possible values are: *False* – Not chosen as best route. *True* – Chosen as best route.

Viewing Filters, Access Lists, and Route Maps

This section describes how to view the following IP objects:

- Network filters
- Network access lists
- Route maps

You can monitor network filters, access lists, and route maps by using one of the following methods:

- Double-clicking on the network filter, access list, or route map when you see it in a pick list on the RIP Interface, BGP Neighbor, or any Route Map dialog box.
- Accessing the functions from the monitor menu.

Double-Clicking on an Object in a Pick List

You can double-click on an access list or route map while you are defining a RIP interface, BGP neighbor, or route map. For example, if you double-click on one of the route maps listed in the Assigned Export Maps pick list shown in Figure 8-21, the system displays the Show Route Map Configuration dialog box (see Figure 8-22) for the selected map.

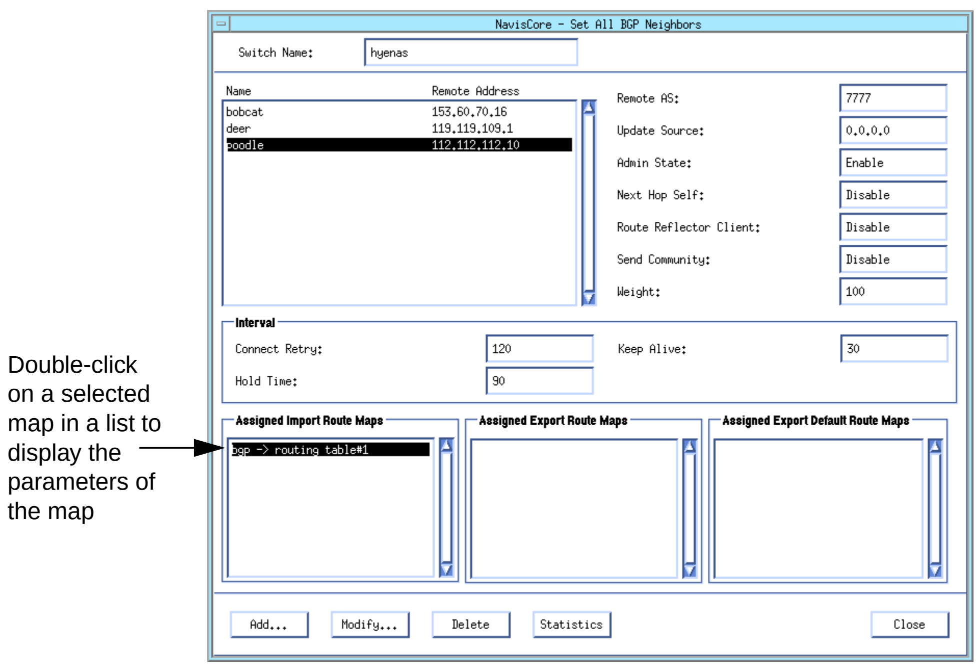
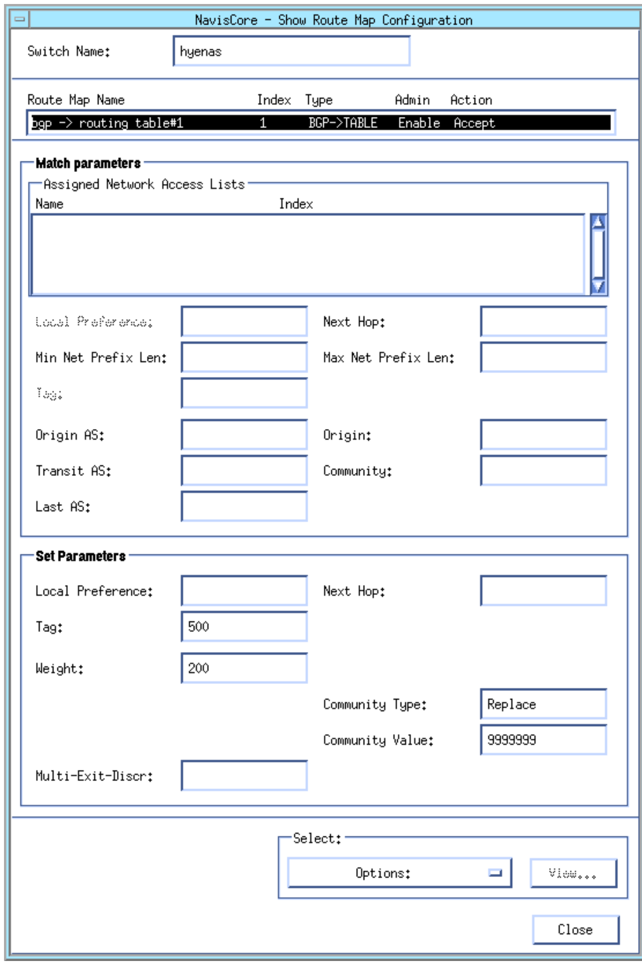


Figure 8-21. Double-clicking on a Route Map in a Pick List



Parameters display after you double-click on a selected map.

Figure 8-22. Show Route Map Configuration

Viewing Network Filters

To view the network filters defined for a node:

1. On the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show Route Policies ⇒ Show Network Filters. The Show All Network Filters dialog box appears (see Figure 8-23).

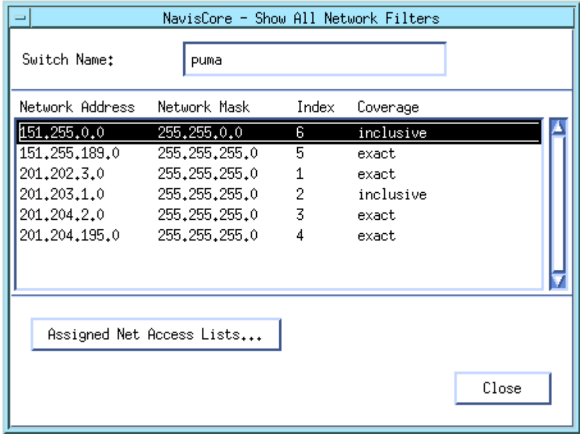


Figure 8-23. Show All Network Filters Dialog Box

Table 8-22 describes the Network Filter fields.

Table 8-22. Show All Network Filter Fields

Field	Displays...
Network Address	The network address for this filter. For example, 0.0.0.0 specifies all network addresses.
Network Mask	The network mask for this filter.
Index	The index field generated by NavisCore and unique within the switch.
Coverage	One of the following: *inclusive* – Allow all networks that match the specified network address (including addresses that may be more specific). *exact* – Allow only the network that is specified in the network address and the network mask.

Viewing Assigned Network Access Lists

To view the network access lists assigned to a selected network filter:

1. Choose Assigned Net Access Lists from the Show All Network Filters dialog box (see Figure 8-23).
2. The Network Access Lists Using a Network Filter dialog box appears (see Figure 8-24).

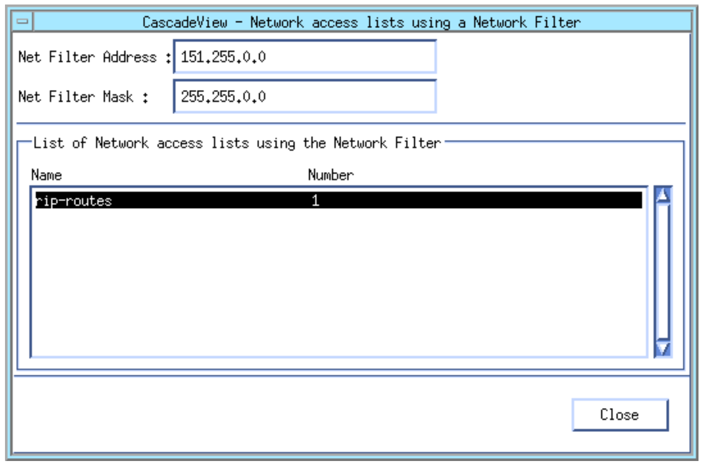


Figure 8-24. Network Access Lists Using a Network Filter Dialog Box

This dialog box displays the name and internally assigned number of each network access list assigned to a selected network filter.

Viewing Network Access Lists

To view the network access lists defined for a node:

1. On the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All Route Policies ⇒ Show All Network Access Lists. The Show All Network Access Lists dialog box appears (see Figure 8-25).

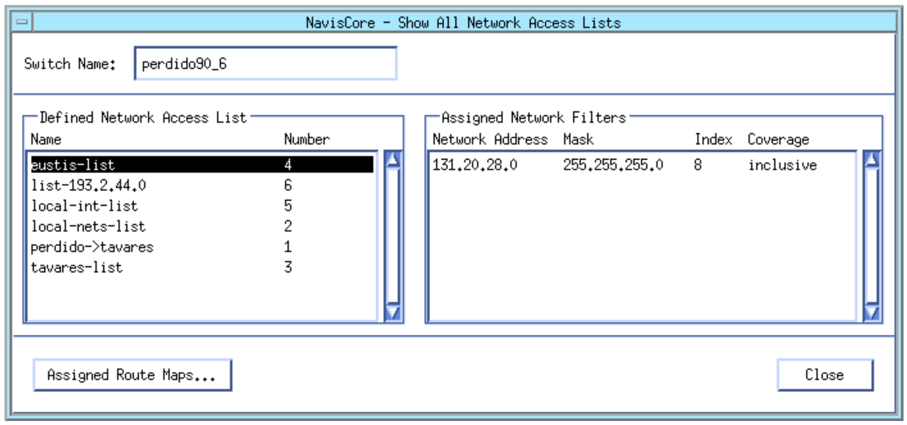


Figure 8-25. Show All Network Access Lists Dialog Box

Table 8-23 describes of each of the Network Access List fields. Note that the dialog box lists the network filters that are currently included in the network access list. Up to 300 filters can be included in the access list.

Table 8-23. Show All Network Access List Fields

Field	Displays...
Defined Network Access List	
Name	A unique network access list name.
Number	An internally assigned number.
Assigned Network Filters	
Network Address	The network address for the filter.
Mask	The network mask for the filter.
Index	The index field generated by NavisCore and unique within the switch.
Coverage	One of the following: *Inclusive* – Allows all networks that match the specified network address (including addresses that may be more specific. *Exact* – Allows only the network that is specified in the network address.

Viewing Assigned Route Maps

To view the route maps assigned to a selected network access list:

1. Choose Assigned Route Maps from the Show All Network Access Lists dialog box (see Figure 8-25).
2. The Route Maps Using Network Access List dialog box appears (see Figure 8-26).

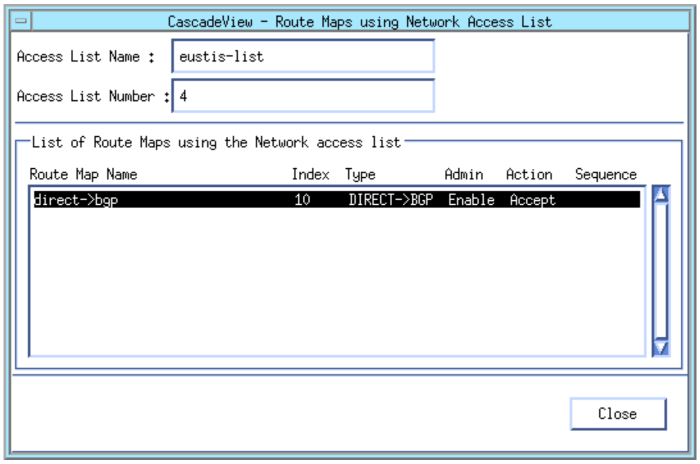


Figure 8-26. Route Maps Using Network Access List Dialog Box

Viewing Route Maps

To view the route maps defined for a node:

1. On the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All Route Policies ⇒ Show All Route Maps. The Show All Route Maps dialog box appears (see Figure 8-27).

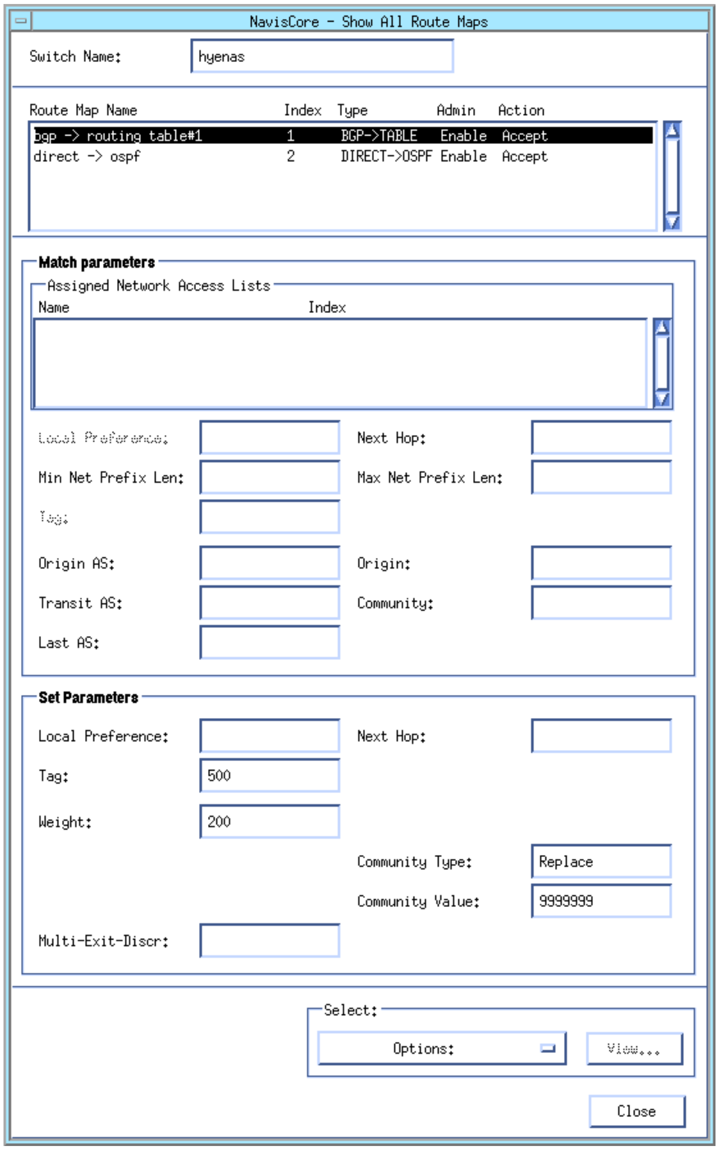


Figure 8-27. Show All Route Maps Dialog Box

Table 8-24 describes each of the common fields shown at the top of the Show All Route Maps dialog box. Note that the Match parameters and Set parameters vary depending on the type of route map that you are defining. See the *NavisCore IP Navigator Configuration Guide* for information about the Match and Set parameters for each route map type.

Table 8-24. Show All Route Maps Common Values

Field	Displays...
Route Map Name	A name that uniquely identifies the route map.
Index	The index field generated by NavisCore and unique within the switch.
Type	The From protocol and To protocol that identify the route distribution type.
Admin	One of the following: *Enable* – The route map is administratively enabled and can be used. *Disable* – The route map is administratively disabled and cannot be used.
Action	One of the following: *Accept* – All routes that match the specified Match parameters are accepted. *Deny* – All routes that match the specified Match parameters are denied. *Originate Default* – The match parameters that define where to send a default route heading are configurable. This option is used for the following types of route maps: • BGP to BGP • ANY to BGP • RIP to RIP

Viewing IP Packet Filters

This section describes how to view IP packet filters, and list IP packet filters assigned to logical ports and to hosts.

Viewing IP Packet Filters

To view IP Packet filter parameters:

1. From the network map, select the appropriate switch object.

2. From the Monitor menu, select Ascend IP Objects ⇒ Show All Packet Filters ⇒ Show All Packet Filters. The Show All Packet Filters dialog box appears (see Figure 8-28).

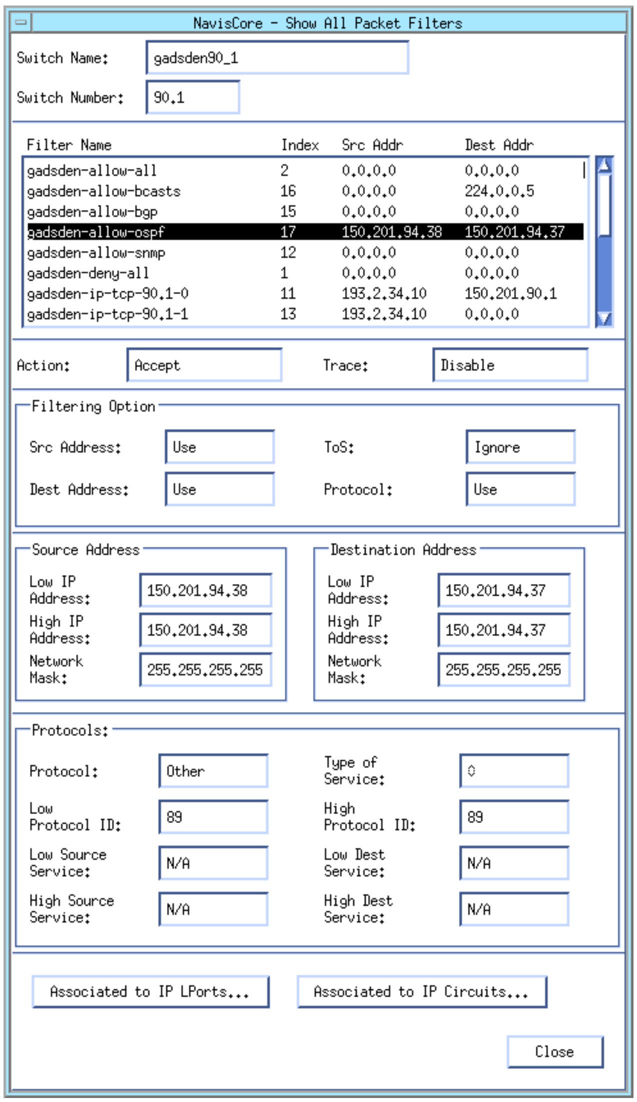


Figure 8-28. Show All Packet Filters Dialog Box

3. Select a packet filter from the list at the top. The filter criteria appear in the fields on the dialog box.

Table 8-25 describes the packet filter parameter fields.

Table 8-25. Show All Packet Filter Fields

Field	Displays...
Filter Name	The name that identifies the filter.
Index	The index field generated by NavisCore and unique within the switch.
Src Addr	The source address specified for the filter (if applicable). An address of 0.0.0.0 means that no source address was specified.
Dest Addr	The destination address specified for the filter (if applicable). An address of 0.0.0.0 means that no destination address was specified.
Action	One of the following: *Accept* – The switch accepts packets that match the filtering criteria. *Reject* – The switch rejects packets that match the filtering criteria.
Trace	One of the following: *Enable* – The switch passes matched packets to the trace manager. *Disable* – The switch does not pass matched packets to the trace manager.
Filtering Option	
Src Address	One of the following: *Use* – The switch filters packets based on the source address field in the IP packet header. *Ignore* – The switch ignores filtering based on the source address field in the IP packet header. In addition, the Source Address fields are grayed out.
Dest Address	One of the following: *Use* – The switch filters packets based on the destination address field in the IP packet header. *Ignore* – The switch ignores filtering based on the destination address field in the IP packet header. In addition, the Destination Address fields are grayed out.
ToS	One of the following: *Use* – The switch filters packets based on the ToS field in the IP packet header. *Ignore* – The switch ignores filtering based on the ToS field in the IP packet header. In addition, the Type of Service field is grayed out.

Table 8-25. Show All Packet Filter Fields (Continued)

Field	Displays...
Protocol	One of the following: *Use* – The switch filters packets based on the protocol (e.g., TCP). *Ignore* – The switch ignores filtering based on the protocol. In addition, the Protocols fields are grayed out.
Source Address	
Low IP address	The low IP address of the node that sends the packet. When you enter this value, you enter the beginning address in a range between this value and the high IP address. If the packet's source address is between the low and high IP address, there is a match. ***Note:*** *If you want to filter packets coming from one IP address, specify the IP address in the low IP address field. You do not have to specify a value in the high IP address field.*
High IP Address	The high IP address of the node that sends the packet (the default is high IP address=low IP address). When you enter this value, you enter the ending address in a range between the low IP address and this value. If the packet's source address is between the low and high IP address, there is a match.
Network Mask	The Network Mask that applies to the source address.
Destination Address	
Low IP Address	The low IP address of the node that receives the packet. When you enter this value, you enter the beginning address in a range between this value and the high IP address. If the packet's destination address is between the low and high IP address, there is a match. ***Note:*** *If you want to filter packets going to one IP address, specify the IP address in the low IP address field. You do not have to specify a value in the high IP address field.*
High IP Address	The high IP address of the node that receives the packet. The default is high IP address=low IP address. When you enter this value, you enter the ending address in a range between the low IP address and this value. If the packet's destination address is between the low and high IP address, there is a match.
Network Mask	The network mask that applies to the destination address.

Table 8-25. Show All Packet Filter Fields (Continued)

Field	Displays...
Protocols	
Protocol	The packet's transport protocol type: *TCP* – Transmission Control Protocol. *UDP* – User Datagram Protocol. *Others* – Protocol IDs in the low and high protocol ID fields. Transport refers to the protocol (TCP, UDP, or Others) that enables the packet to be delivered to the correct destination protocol.
Low Protocol ID	The low protocol ID, if you selected *Others* in the Protocol field. See *RFC 1700* for protocol ID numbers. When you enter this value, you enter the beginning protocol ID in a range between this value and the high protocol ID. If the packet's protocol ID is between the low and high protocol ID, there is a match.
Low Source Service	The low source service port number, if *Other* was specified for service when the packet filter was configured. See *RFC 1700* for the port numbers. Otherwise, this field displays "N/A." When you enter this value, you enter the beginning source service port number in a range between this value and the high source service port number. If the packet's source service port number is between the low and high source service port numbers, there is a match. See the *NavisCore IP Navigator Configuration Guide* for more information on configuring service port numbers.
High Source Service	The high source service port number, if *Other* was specified for service when the packet filter was configured. See *RFC 1700* for the port numbers. Otherwise, this field displays "N/A." When you enter this value, you enter the ending source service port number in a range between the low source service port number and this value. If the packet's source service port number is between the low and high source service port numbers, there is a match. See the *NavisCore IP Navigator Configuration Guide* for more information on configuring service port numbers.
Type of Service	The value that identifies the type of service (ToS). Protocols use this value to specify the packet's priority. Any value between 0 and 254 is valid.
High Protocol ID	The high protocol ID, if you selected *Others* in the Protocol field. See *RFC 1700* for protocol ID numbers. When you enter this value, you enter the ending protocol ID in a range between the low protocol ID and this value. If the packet's protocol ID is between the low and high protocol ID, there is a match.

Table 8-25. Show All Packet Filter Fields (Continued)

Field	Displays...
Low Dest Service	The low destination service port number, if *Other* was specified for service when the packet filter was configured. See *RFC 1700* for the port numbers. Otherwise, this field displays "N/A." When you enter this value, you enter the beginning destination service port number in a range between this value and the high destination service port number. If the packet's destination service port number is between the low and high destination service port numbers, there is a match. See the *NavisCore IP Navigator Configuration Guide* for more information on configuring service port numbers.
High Dest Service	The high destination service port number, if *Other* was specified for service when the packet filter was configured. See *RFC 1700* for the port numbers. Otherwise, this field displays "N/A." When you enter this value, you enter the ending destination service port number in a range between the low destination service port number and this value. If the packet's destination service port number is between the low and high destination service port numbers, there is a match. See the *NavisCore IP Navigator Configuration Guide* for more information on configuring service port numbers.

Viewing IP Logical Ports That Use the Packet Filter

To view a list of IP logical ports that use the packet filter:

1. From the Show All Packet Filters dialog box (see Figure 8-28 on page 8-50), select a packet filter from the list at the top.
2. Choose Associated to IP LPorts. A list of logical ports that use the packet filter appears.

Viewing IP Circuits That Use the Packet Filter

To view a list of IP circuits that use the packet filter:

1. From the Show All Packet Filters dialog box (see Figure 8-28 on page 8-50), select a packet filter from the list at the top.
2. Choose Associated to IP Circuits. A list of logical ports that use the packet filter appears.

Viewing IP Packet Filters Assigned to Logical Ports

To view IP packet filters assigned to a logical port:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All Packet Filter ⇒ Show All Logical Port Filters. The Show All Logical Port Filters dialog box appears (see Figure 8-29).

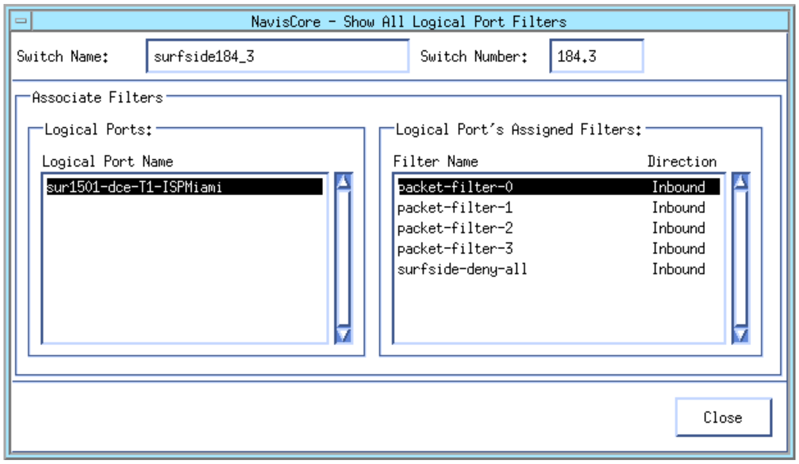


Figure 8-29. Show All Logical Port Filters Dialog Box

3. Select a logical port from the Logical Ports list on the left. The filters assigned to the logical port appear in the Logical Port's Assigned Filters list on the right. The direction of network traffic to which each filter applies (e.g., Inbound) also appears.

Viewing IP Packet Filters Assigned to Hosts

To view IP packet filters assigned to hosts:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All Packet Filter ⇒ Show All Host Filters. The Show All Host Filters dialog box appears (see Figure 8-30).

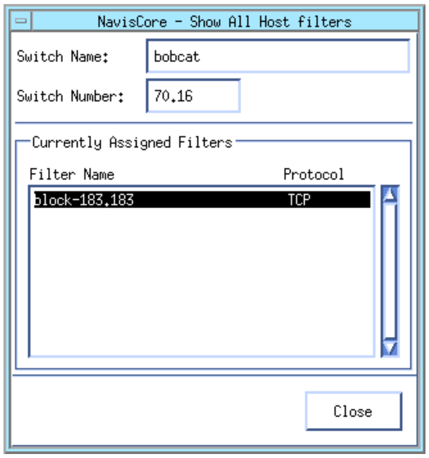


Figure 8-30. Show All Host Filters Dialog Box

The Show All Host Filters dialog box displays a list of filters configured for the switch in the Filter Name column and a list of protocols associated with the filters in the Protocol column.

Viewing IP Packet Filters Assigned to Circuits

To view IP packet filters assigned to circuits:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All Packet Filters ⇒ Show All IP Circuit Filters. The Show All IP Circuit Filters dialog box appears (see Figure 8-31).

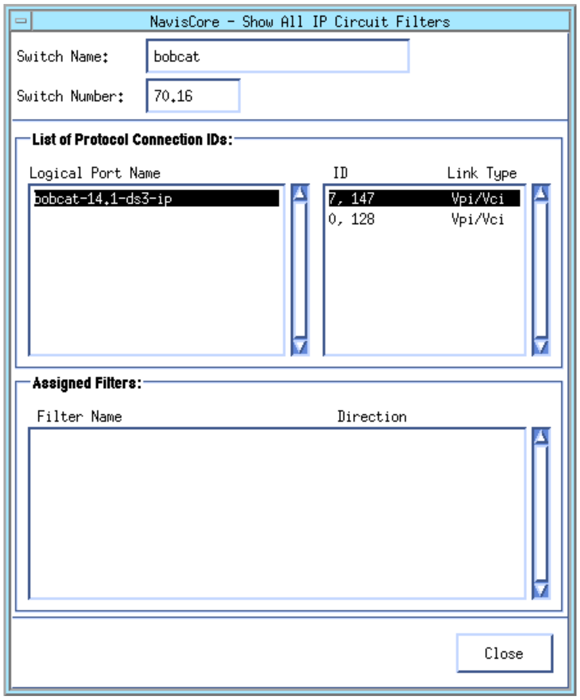


Figure 8-31. Show All IP Circuit Filters Dialog Box

3. Select an IP logical port from the Logical Port Name list on the left. A list of IP circuits appears to the right. Each IP circuit is identified by its DLCI (Frame Relay circuits) or by its VPI/VCI (ATM circuits).
4. Select an IP circuit. The filters assigned to the IP circuit appear in the Assigned Filters list at the bottom of the dialog box. The direction of network traffic to which each filter applies (e.g., Inbound) also appears.

Table 8-26 describes the Show All IP Circuit Filters fields.

Table 8-26. Show All IP Circuit Filter List Fields

Field	Displays...
Logical Port Name	The IP logical port name.
ID	The IP circuit's DLCI (Frame Relay circuits) or VPI/VCI (ATM circuits).
Link Type	One of the following: *Dlci* – The value in the ID field is a DLCI. *Vpi/Vci* – The value in the ID field is a VPI/VCI.
Filter Name	The name of the filter.
Direction	The direction of network traffic to which the filter applies (e.g., Inbound).

Viewing QoS Profiles

This section describes how to view:

- QoS flow profiles
- QoS filters assigned to logical ports
- QoS filter statistics

Viewing QoS Flow Profiles

To view IP QoS PVC flow profiles:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All QoS Profiles ⇒ Show All QoS Profiles. The Show All QoS Profiles dialog box appears (see Figure 8-32).

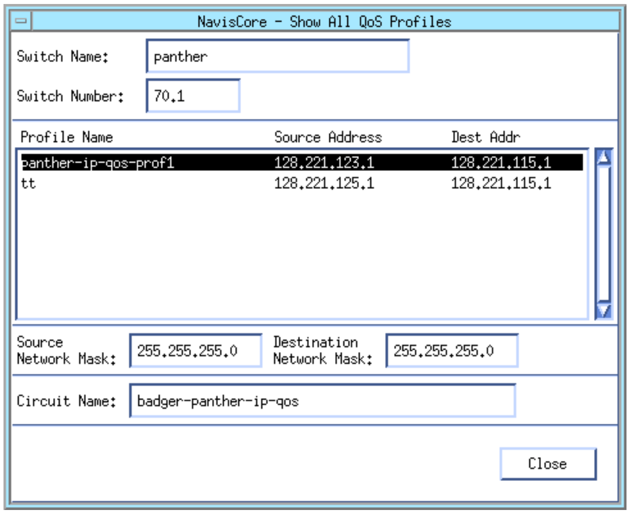


Figure 8-32. Show All QoS Profiles Dialog Box

3. Select a profile from the list.

Table 8-27 describes QoS Profile fields.

Table 8-27. Show All QoS PVC Flow Profile Fields

Field	Displays...
Profile Name	The profile name.
Source Address	The IP address of the network or host that sends the packet.
Dest Addr	The IP address of the network or host that receives the packet.
Source Network Mask	The network mask that applies to the source address.
Destination Network Mask	The network mask that applies to the destination address.
Circuit Name	The PVC to which the IP QoS PVC flow profile is assigned.

Viewing IP QoS Profiles Assigned to a Logical Port

To view IP QoS profiles assigned to a logical port:

1. From the network map, select the appropriate switch object.

2. From the Monitor menu, select Ascend IP Objects ⇒ Show All QoS Profiles ⇒ Show All Logical Port QoS Profiles. The Show All Logical Port QoS Profiles dialog box appears (see Figure 8-33).

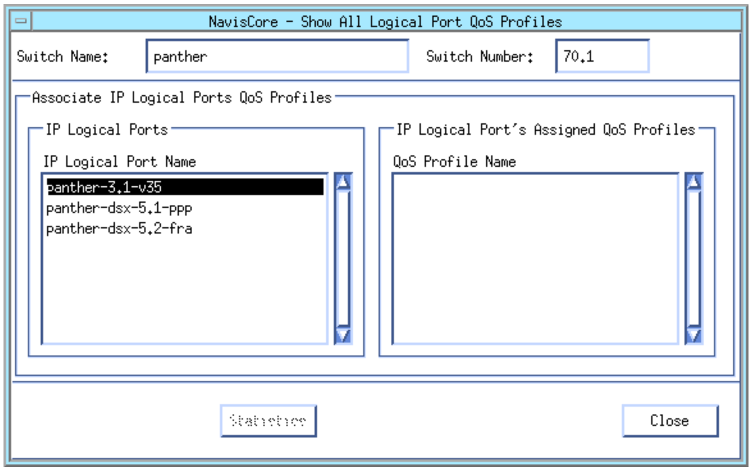


Figure 8-33. Show All Logical Port QoS Profiles Dialog Box

3. Select a logical port from the IP Logical Port Name list. The IP QoS profiles assigned to the logical port appear in the QoS Profile Name list.

4. Choose the Statistics button to display LPort QoS filter statistics. For more information, see "Viewing IP QoS Filter Statistics" on page 8-60.

Viewing IP QoS Filter Statistics

To view a logical port's IP QoS filter statistics:

1. Select a logical port and associated QoS filter as described in "Viewing IP QoS Profiles Assigned to a Logical Port."

2. Choose Statistics. The LPort QoS Filter Statistics dialog box appears (see Figure 8-34).

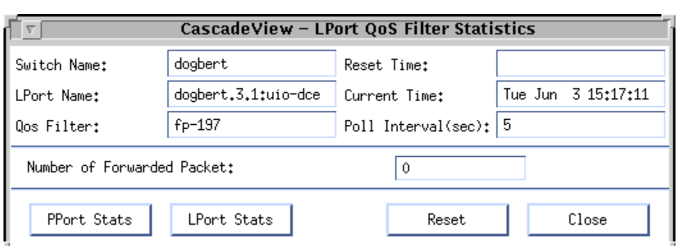


Figure 8-34. LPort QoS Filter Statistics Dialog Box

Table 8-28 describes LPort QoS Filter Statistics fields.

Table 8-28. LPort QoS Filter Statistics

Statistic	Description
Switch Name	The name of the switch.
LPort Name	The name of the selected logical port.
QoS Filter	The name of the QoS profile.
Reset Time	The time of the last counter reset.
Current Time	The current system time.
Poll Interval(sec)	The time interval for the collection statistics. See "Setting the Polling Interval" on page 3-2 for information about setting the poll interval.
Number of Forwarded Packet	The number of packets forwarded over the IP QoS PVC processed by the IP QoS profile and associated logical port.

3. Choose Reset to clear the statistics counters.
4. Choose PPort Stats to display the physical port statistics. Choose LPort Stats to display the logical port summary statistics. For more information, see Chapter 3, "Generating Physical Port Statistics."

Viewing Static Routes

To view static route parameters:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All Static Routes. The Show All Static Route dialog box appears (see Figure 8-35).

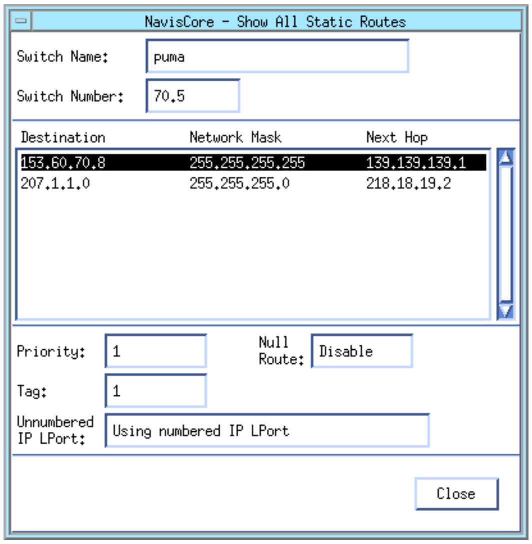


Figure 8-35. Show All Static Routes Dialog Box

3. Select a route.

   Table 8-29 describes the Static Route fields.

Table 8-29. Show All Static Routes Fields

Field	Displays...
Destination	The IP address of the destination network.
Network Mask	The network mask associated with the destination IP address.
Next Hop	The IP address of the next hop. This field is disabled for unnumbered IP logical ports or if null route is enabled.
Priority	A value from 1 to 20 which specifies the static route priority. The highest number is the preferred priority. The priority of the static route is in relation to other route protocols.
Tag	The tag value, which you use to group multiple static route entries together.

Table 8-29. Show All Static Routes Fields (Continued)

Field	Displays...
Null Route	One of the following: *Enable* – Packets destined for this network are discarded. In addition, the next hop is disabled. *Disable* – Packets destined for this network are forwarded.
Unnumbered IP LPort	Whether the route uses a numbered or unnumbered IP logical port.

Viewing Static ARP Parameters

To view static ARP parameters:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All Static ARP Entries. The Show All Static ARP Entries dialog box appears (see Figure 8-36).

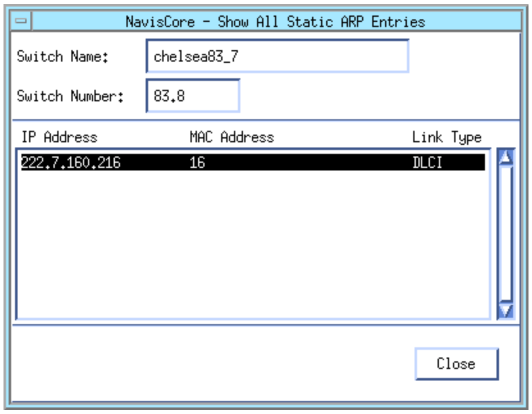


Figure 8-36. Show All Static ARP Entries Dialog Box

Table 8-30 describes the ARP Entries fields.

Table 8-30. Show All Static ARP Entries Fields

Field	Displays...
IP Address	The IP address of the neighbor.
MAC Address	The MAC Address used for the neighbor. The MAC address that appears depends on the link type: **Frame Relay Circuit –** The MAC address is the DLCI number identifying the circuit that connects the switch and the neighbor. The DLCI number may range from 0 through 937. **ATM Circuit** – The MAC address is the VPI/VCI number identifying the circuit that connects the switch and the neighbor. A VPI is an 8-bit field in the ATM cell header that is used as an addressing identifier to route cell traffic. A VCI is a 16-bit field in the ATM cell header that is used as an addressing identifier to route cell traffic. **Ethernet LAN** – The MAC address is the LAN card address.
Link Type	One of the following: *DLCI* – A Frame Relay circuit connects the switch and the neighbor. *VPI-VCI* – An ATM circuit connects the switch and the neighbor. *Ethernet* – An Ethernet LAN connects the switch and the neighbor.

Viewing IP Loopback Addresses

To view a list of IP loopback addresses:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show All IP Loopback Addresses. The Show All IP Loopback Addresses dialog box appears (see Figure 8-37).

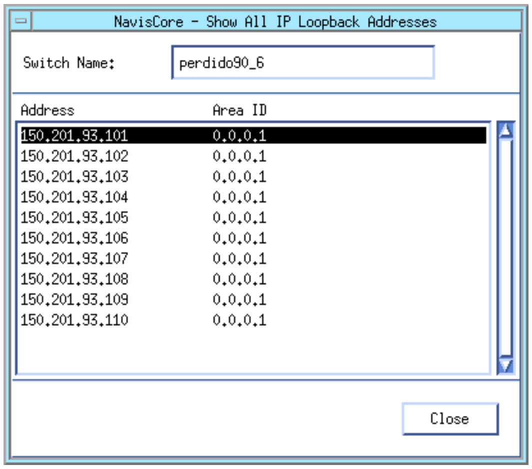


Figure 8-37. Show All IP Loopback Addresses Dialog Box

The Show All IP Loopback Addresses dialog box displays the IP address and Area ID of each loopback address. Loopback addresses identify virtual interfaces that are up at all times on the switch. If the physical interfaces that BGP neighbors use to exchange routing updates are unstable, the neighbors can use virtual interfaces (that is, interfaces that are not dependent on physical interfaces) to exchange the updates. Otherwise, routing update sessions between the neighbors may become unstable.

Viewing MPT Path Parameters

To view MPT path parameters:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show MPT Path. The Show MPT Path dialog box appears (see Figure 8-38).

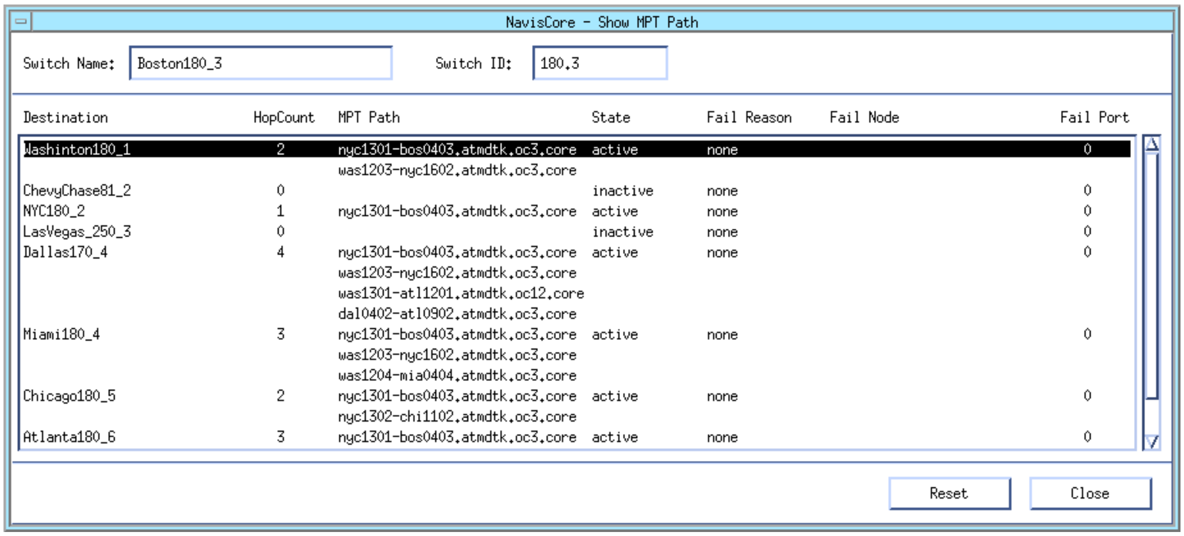


Figure 8-38. Show MPT Path Dialog Box

3. Choose Reset to clear the path information.

Table 8-31 describes MPT path fields.

Table 8-31. Show MPT Path Fields

Field	Displays...
Destination	The MPT destination node's switch name.
Hop Count	The MPT destination node path's hop counts.
MPT Path	The trunk name that represents the MPT circuit path.

Table 8-31. Show MPT Path Fields (Continued)

Field	Displays...
State	The current status of the MPT destination node path. Possible states are: *retry* – The MPT process is waiting until the local timer expires to call. *calling* – The MPT process is waiting for the local timer of a message, which rejects or confirms a call. *active* – The MPT process successfully calls and waits for keep-alive events. *inactive* – The MPT process is waiting for the grooming process (to locate a better path in the network), which activates the MPT leaf node. *wcinact* – The MPT process clears when the call is terminated. *wcdel* – The MPT process calls, then deleted is when the calling is over. ***Note:*** *The MPT process maintains the state of each end-to-end path that is sent by OSPF.*
Fail Reason	The reason why the MPT path failed. Possible causes of failure are: *none* – Problems were not encountered. *tpcalling* – An mptTport is calling. An mptTport is a data record that describes an MPT ingress port at any given merge point. *vcalling* – A VC_ENTRY is calling. *tpdead* – The connection is dead. *routelookup* – The route lookup failed. *confirmtimeout* – The confirm timer expired. *pathclear* – OSPF is notifying MPT that the path is no longer preferred. *trunkdown* – The trunk is down. *dead* – Hello packets are no longer received. *grooming* – A better path exists in the network. *pathregister* – The path is not registered with OSPF. *impurepath* – A shorter path of mixed cells and frames exists. *rvcdied* – The RVC is dead. An RVC is a data structure that reassembles frames into ATM cells.
Fail Node	The last switch associated with the failed MPT path.
Fail Port	The interface number on the failed node that is associated with the failed MPT path.

Viewing RIP Information

This section describes how to view RIP information.

Viewing RIP Peer Information

The switch communicates with a RIP peer, such as a remote host or router, via the Routing Information Protocol (RIP).

To view the RIP peer information:

1. On the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show Rip2 ⇒ Show Rip2 Peers. The RIP2 Active Peer Table dialog box appears (see Figure 8-39).

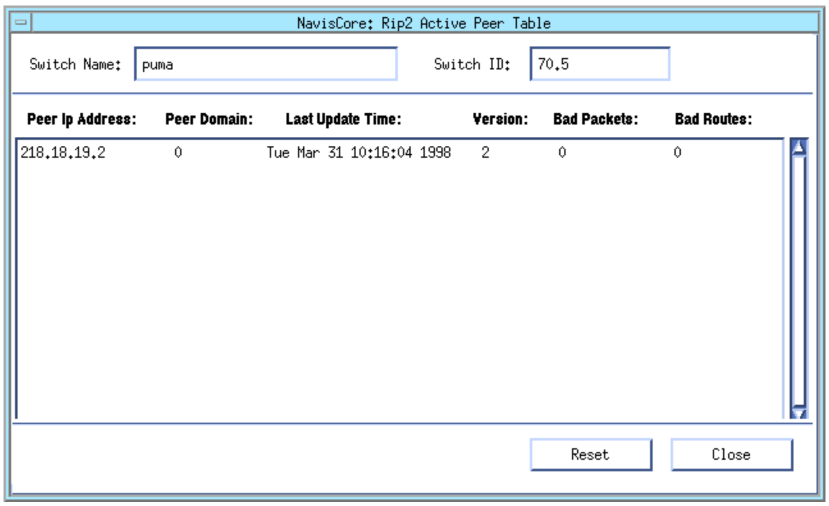


Figure 8-39. RIP2 Active Peer Table Dialog Box

3. Choose Reset to clear the peer information.

Table 8-32 describes the RIP2 Active Peer Table fields.

Table 8-32. RIP Active Peer Table Fields

Field	Displays...
Peer IP Address	The IP address that the peer uses as its source address. On an unnumbered interface, this address may not be a member of any subnet on the system.
Peer Domain	The value in the Routing Domain field in RIP packets received from the peer. As domain support is lowered, this value must be zero.
Last Update Time	The time that the most recent RIP update was received.

Table 8-32. RIP Active Peer Table Fields (Continued)

Field	Displays...
Version	The RIP version number in the header of the last RIP packet received.
Bad Packets	The number of RIP response packets from this peer that were discarded as invalid.
Bad Routes	The number of routes from this peer that were ignored because the entry format was invalid.

Viewing RIP Global Counters

To view the RIP counters:

1. On the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show Rip2 ⇒ Show Rip2 Global Counters. The Rip2 Global Counters dialog box appears (see Figure 8-40).

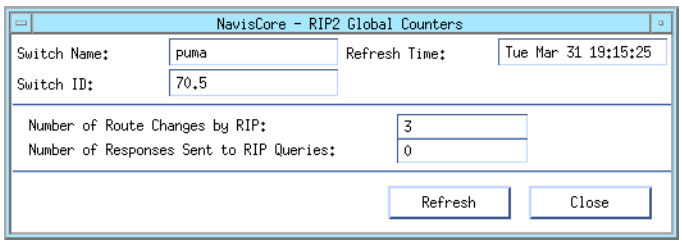


Figure 8-40. RIP2 Global Counters Dialog Box

The RIP2 Global Counters dialog box displays the number route changes that RIP has made and the number of responses that RIP has sent to RIP queries. Choose Refresh to update these counters.

Viewing MPT Point-to-Point Connection Status

To view MPT point-to-point connection status:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show MPT Point-to-Point Paths. The Show All MPT Point-to-Point Connections dialog box appears (see Figure 8-41).

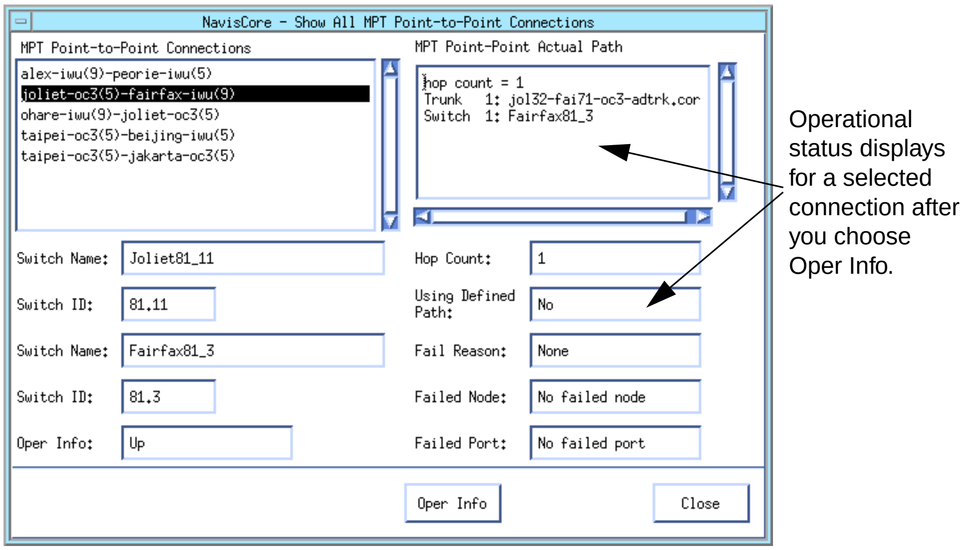


Figure 8-41. Show All MPT Point-to-Point Connections Dialog Box

3. Select an MPT point-to-point connection from the MPT Point-to-Point Connections list. Information about the connection appears in the fields on the dialog box.

Table 8-33 describes the MPT Point-to-Point Connections fields.

Table 8-33. Show All MPT Point-to-Point Connections Field Descriptions

Field	Displays...
MPT Point-to-Point Connections	All of the defined MPT point-to-point connections in your network.
MPT Point-Point Actual Path	The actual path for a selected MPT point-to-point connection.
Switch Name	The two switch name fields. Each field displays one of the switch endpoints of a selected MPT point-to-point connection.
Switch ID	The two switch ID fields. Each field displays a unique identifier that is assigned to a switch endpoint of a selected MPT point-to-point connection. (This value is the last two bytes of the switch IP address.)

Table 8-33. Show All MPT Point-to-Point Connections Field Descriptions (Continued)

Field	Displays...
Oper Info	*Up*, *Down*, or *Unknown* to indicate the current operational status of a selected MPT point-to-point connection.
Hop Count	The number of hops used in the path for a selected MPT point-to-point connection.
Using Defined Path	One of the following: *Yes* – The point-to-point connection uses a user-defined path. *No* – The path uses the point-to-point connection that was automatically defined by the Virtual Network Navigator (VNN). *Unknown* – The point-to-point connection has no path.
Fail Reason	The cause of the failure or *None* if no failure exists. These fail reasons are reported by the switch to the NMS. Table 8-34 displays a list of possible fail reasons.
Failed Node	*No failed node* if no failure exists or the node ID in the event of a failure.
Failed Port	*No failed port* if no failure exists or the logical port interface number (that MPT is using to access the switch) in the event of a failure.

Table 8-34. MPT Point-to-Point Connection Failure Reasons

Reason	Description
None	No failure condition exists.
Unknown	The error condition that the switch reported does not match any of the error conditions in this table.
Tpcalling	VNN detected an MPT port calling error.
Vcalling	VNN detected a circuit endpoint calling error.
Tpdead	A dead MPT port exists.
Route Lookup	A route lookup failure exists.
Confirm Timeout	The confirm timer has expired.
Path Clear	An OSPF Path clear condition exists.
Trunk Down	A trunk down condition exists.
Dead	Hello packets are no longer being received.
Grooming	A better path exists in the network.
Path Registering	The switch failed to register a path with OSPF.

Table 8-34. MPT Point-to-Point Connection Failure Reasons (Continued)

Reason	Description
Impure path	A shorter path of mixed cells and frames exists.
Receiver died	The Reassembly Virtual Circuit (RVC) has died.
Invalid Trunk	An invalid trunk was found in the path.
VPC Allocate	VNN could not allocate a VPC.
VCC Allocate	VNN could not allocate a VCC.
ADD RVC	VNN could not add a reassembly virtual circuit (RVC).
NO RIDS	No more RIDs are available at this node.
FE Calling	VNN encountered an MPT Forwarding Engine (FE) calling error.
FE Dead	VNN was notified of a dead MPT Forwarding Engine (FE).
FE Active	VNN was notified of an active MPT Forwarding Engine (FE).
Invalid FE ID	An invalid Forwarding Engine (FE) ID exists at the leaf.

To display the operational status for an MPT Point-to-Point connection path:

1. Select the connection from the MPT Point-to-Point Connections list of the Show All MPT Point-to-Point Connections dialog box.
2. Choose Oper Info. The system then displays the MPT Point-to-Point path in the upper right portion of the dialog box.

Viewing the IP Routing Table

The following sections describe how to view the IP routing table. You can view the routing table as a whole or you can filter routes based on the following criteria:

- Destination IP address
- Mask
- Type
- Protocol

To view the IP routing table:

1. From the network map, select the appropriate switch object.
2. From the Monitor menu, select Ascend IP Objects ⇒ Show IP Routing Table. The Show IP Routing Table dialog box appears (see Figure 8-42).

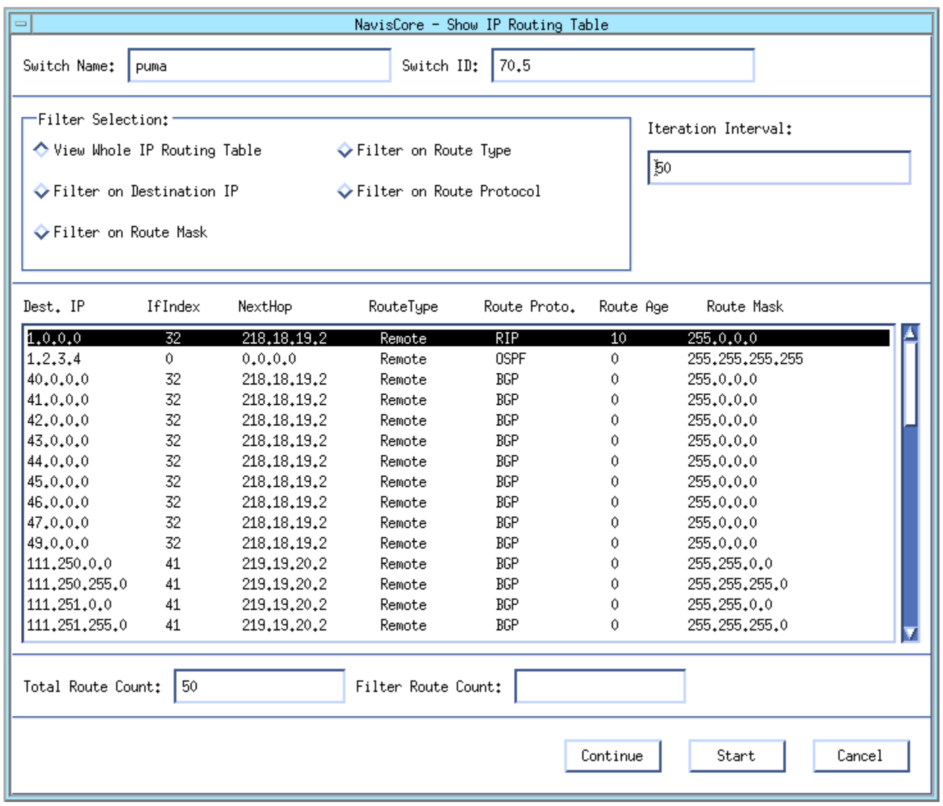


Figure 8-42. Show IP Routing Table Dialog Box

If the routing table is too large, the fields in the filter selection box enable you to view particular routes. You can select one of the filter selections to decrease the size of the routing table. This enables you to view routes based on a particular parameter. For example, if you select Filter on Destination IP, you only view the destination IP portion of the routing table.

Table 8-35 describes each field in the Filter Selection box.

Table 8-35. Filter Selection Fields

Field	Displays...
View Whole IP Routing Table	The whole routing table (see Table 8-36).
Filter on Destination IP	Destination IP address information in the routing table.
Filter on Route Mask	Route mask information in the routing table.
Filter on Route Type	Route type information in the routing table.
Filter on Route Protocol	Route protocol information in the routing table.

Viewing the Whole IP Routing Table

To view the whole IP routing table:

1. Select *View Whole IP Routing Table* in the Filter Selection box.

The Show IP Routing Table dialog box appears (see Figure 8-42). Table 8-36 describes each of the View Whole IP Routing Table fields.

Table 8-36. View Whole IP Routing Table Fields

Field	Action/Description
Iteration Interval	The number of routes you want to view. The default is 50.
Dest. IP	The IP network that is pointed to by this route entry.
IfIndex	The value that identifies the local interface for reaching the next hop.
NextHop	The address of the next system en route on remote routes. Otherwise, the value is 0.0.0.0.
Route Type	One of the following: *Local* – The next hop is the final destination. *Remote* – The next hop is not the final destination. *Invalid* – The entry is not used to forward IP packets.
Route Proto.	The routing protocol that indicates how the route was learned.

Table 8-36. View Whole IP Routing Table Fields (Continued)

Field	Action/Description
Route Age	The number of seconds since this route was updated or determined to be correct.
Route Mask	The mask that applies to the corresponding entry in the destination IP column.
Total Route Count	The total routes counter.
Filter Route Count	The filter routes counter.
Starting IP Address (with *Filter on Destination IP* selected)	Enter the starting IP address. When you enter this value, you specify the beginning address in a range between this value and the ending IP address. The range filters out IP addresses that are not in the specified range.
Ending IP Address (with *Filter on Destination IP* selected)	Enter the ending IP address. When you enter this value, you specify a range between the starting IP address and this value. The range filters out IP addresses that are not in the specified range.
Mask Value (with *Filter on Route Mask* selected)	Enter a value between 1 and 32. This value filters on masks between 1 and 32 bits.
Filtering on Routing Type (with *Filter on Route Type* selected)	Filters based on the route type. Select one of the following: *Other Route* – Not specified by this MIB. *Reject Route* – Rejected routes. *Local Route* – Locally configured networks. *Remote* – Routes learned through routing protocols (e.g., BGP, OSPF, RIP).
Filtering on Routing Protocol (with *Filter on Route Protocol* selected)	Filters based on route protocol. Select one of the following protocols: *Local* – Not specified. *Network Management* – Static route. *ICMP* – Result of ICMP Redirect. *EGP* – Exterior Gateway Protocol. *GGP* – Gateway-Gateway Protocol. *Hello* – FuzzBall HelloSpeak. *RIP* – Berkeley RIP or RIP-II. *IS-IS* – Dual IS-IS. *ES-IS* – ISO 9542. *ciscoIgrp* – Cisco IGRP. *bbnSpfIgp* – BBN SPF IGP. *OSPF*– Open Shortest Path First. *BGP* – Border Gateway Protocol. *Other* – Undefined protocol.

2. Choose Start to display information based on your filtering criteria.
3. Choose Continue to scroll through the list of routes.

Filtering Routes Based on Destination IP Address

To filter routes based on destination IP address:

1. Select Filter On Destination IP in the Filter Selection box. The Show IP Routing Table dialog box appears (see Figure 8-43). Table 8-36 on page 8-74 describes each of the Filter on Destination IP fields.

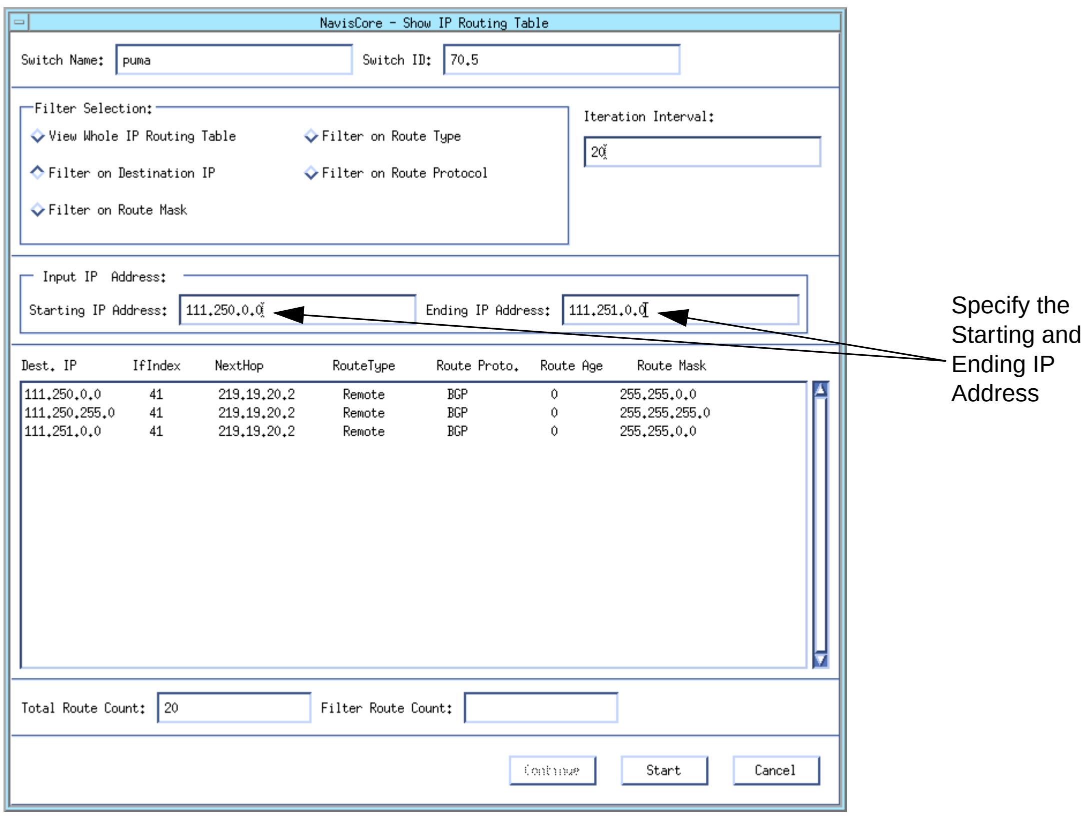


Figure 8-43. Filtering the Routing Table on the Destination IP Address

2. In the Iteration Interval field, specify the number of routes you want to view.
3. In the Input IP Address field, enter the starting IP address and the ending IP address.
4. Choose Start to view the routes.
5. Choose Continue to scroll through the list of routes.

Filtering Routes Based on Mask

To filter routes based on the route mask:

1. Select Filter on Route Mask in the Filter Selection box.

The Show IP Routing Table dialog box appears (see Figure 8-44). Table 8-36 on page 8-74 describes each of the Filter on Route Mask fields.

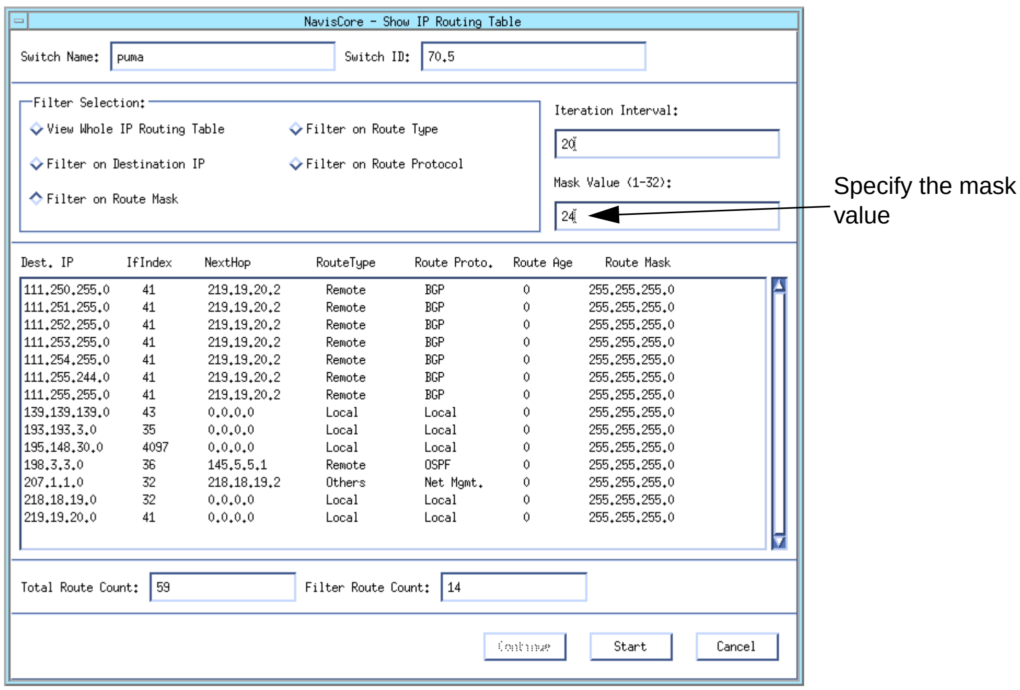


Figure 8-44. Filtering the Routing Table on the Route Mask

2. In the Iteration Interval field, specify the number of routes you want to view.

3. In the Mask Value field, enter the number bits you want the masks displayed to contain.

4. Choose Start to view the routes.

5. Choose Continue to scroll through the list of routes.

Filtering Routes Based on Type

To filter routes based on route type:

1. Select Filter on Route Type in the Filter Selection box.

The Show IP Routing Table dialog box appears (see Figure 8-45). Table 8-36 on page 8-74 describes each of the Filter on Route Type fields.

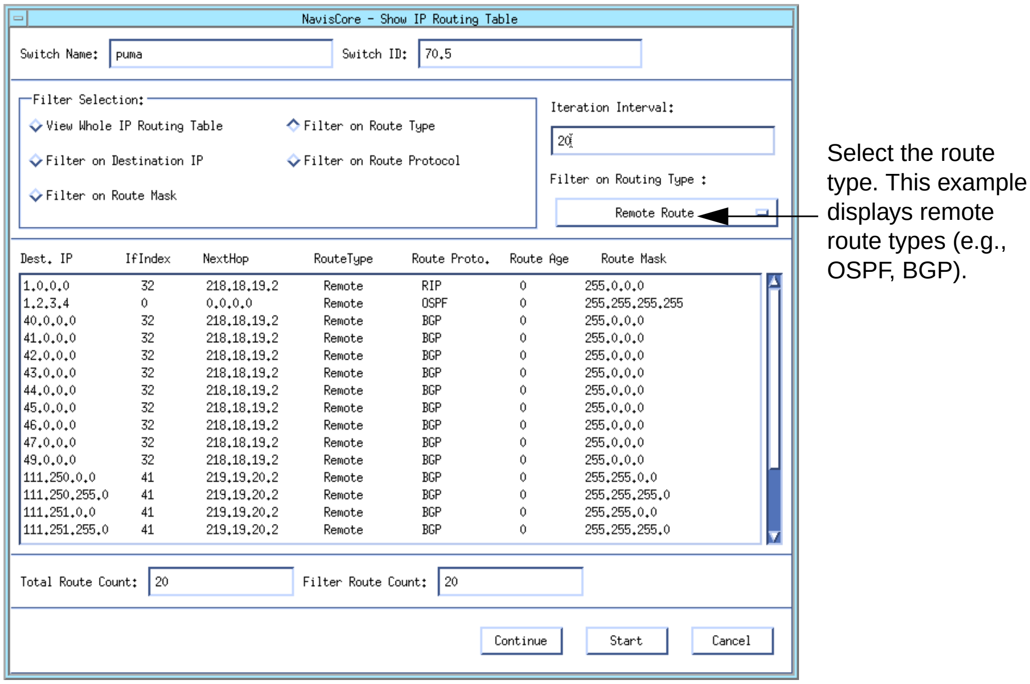


Figure 8-45. Filtering the Routing Table on the Route Type

2. In the Iteration Interval field, specify the number of routes you want to view.

3. In the Filter on Route Type field, select the route type.

4. Choose Start to view the routes.

5. Choose Continue to scroll through the list of routes.

Filtering Routes Based on Protocol

To filter routes based on protocol:

1. Select Filter on Route Protocol in the Filter Selection box.

   The Show IP Routing Table dialog box appears (see Figure 8-46). Table 8-36 on page 8-74 describes each of the Filter on Route Protocol fields.

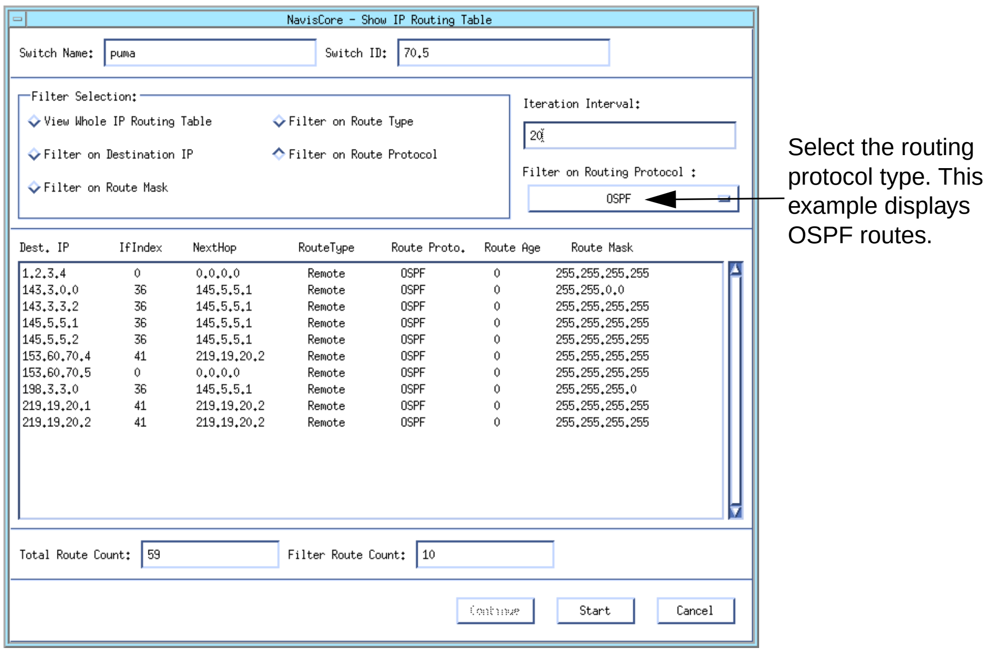


Figure 8-46. Filtering the Routing Table On the Route Protocol

2. In the Iteration Interval field, specify the number of routes you want to view.
3. In the Filter on Routing Protocol field, select the routing protocol type.
4. Choose Start to view the routes.
5. Choose Continue to scroll through the list of routes.

Viewing IP Servers

You can monitor IP server logical port and PVC activity. IP server logical ports provide a method of accepting or transmitting IP traffic on a CBX 500 cell-based I/O module. For more information on IP servers, see the *NavisCore IP Navigator Configuration Guide*.

Viewing IP Server Logical Ports

To view IP Server logical ports:

1. From the Monitor menu, select Ascend IP Objects ⇒ Show IP Servers ⇒ Show IP Server Lports. The Show IP Servers dialog box appears (see Figure 8-47).

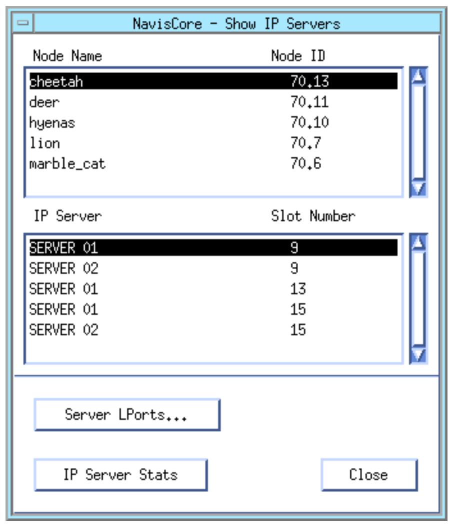


Figure 8-47. Show IP Servers Dialog Box

2. Select a CBX 500 switch in the top list box of node names. The IP servers for the switch appear in the bottom list box.

3. Select an IP server in the bottom list box.

4. Choose one of the following buttons:

   Server Lports — Allows you to view the logical port configured for the selected IP server. Viewing IP Server logical ports is similar to viewing ATM logical ports. See Chapter 7, "Monitoring ATM Logical Ports" for more information.

   IP Server Stats — Allows you to view physical port summary statistics for the IP server. See "Viewing Physical Port Summary Statistics" on page 3-2 for more information on interpreting physical port summary statistics.

Viewing IP Server PVCs

To view IP server PVCs, from the Monitor menu, select Ascend IP Objects ⇒ Show IP Servers ⇒ Show IP Server PVCs. The Show All IP Server PVCs on Map dialog box appears. This dialog box allows you to view all the ATM PVCs between ATM logical ports and IP server logical ports.

Viewing ATM PVCs that carry IP traffic is almost identical to viewing point-to-point ATM PVCs that carry other types of traffic. See "Viewing Point-to-Point ATM PVCs" on page 13-1 for information on viewing point-to-point ATM PVCs.

Viewing IP QoS PVCs

To view IP QoS PVCs, from the Monitor menu, select Ascend IP Objects ⇒ Show IP QoS PVCs. The Show All IP QoS PVCs on Map dialog box appears. This dialog allows you to view all the IP QoS PVCs in the network.

IP QoS PVCs use point-to-point Frame Relay PVCs. Viewing IP QoS PVCs is almost identical to viewing point-to-point Frame Relay PVCs. See "Viewing Frame Relay PVCs" on page 14-1 for information on viewing point-to-point Frame Relay PVCs.

Viewing Ethernet Logical Ports

To view Ethernet logical ports:

1. Select the switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 8-48).

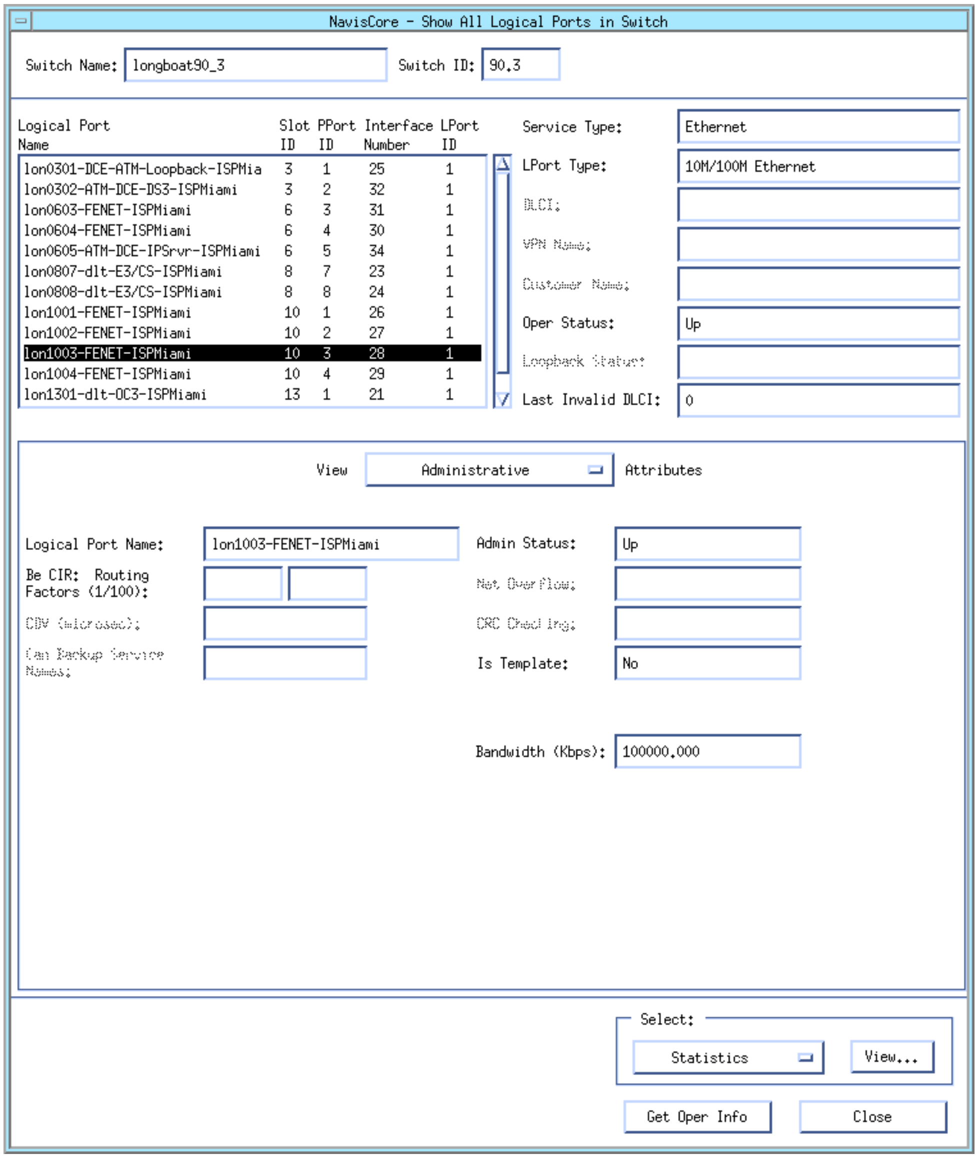


Figure 8-48. Show All Logical Ports in Switch Dialog Box (Ethernet Port)

3. Select an Ethernet logical port.

Using the View Attributes pull-down menu choices, you can view the following attributes:

Administrative — See "Viewing Administrative Attributes" on page 6-7 for information on Administrative attributes.

Trap Control — See "Viewing Trap Control Attributes" on page 6-12 for information on Trap Control attributes.

Ethernet Frame — Displays the Ethernet framing type configured for the logical port: Ethernet II (the original Ethernet framing standard) or IEEE-SNAP (the IEEE Ethernet standard). All nodes on the Ethernet LAN must share the same framing method.

The Options option menu allows you to view IP parameters configured for the logical port and statistics on logical port activity.

Viewing Ethernet Logical Port IP Parameters

To view Ethernet logical port IP parameters:

1. From the Show All Logical Ports in Switch dialog box (see Figure 8-48 on page 8-82), select Options ⇒ IP Parameters.
2. Choose Set. The Show IP Parameters dialog box appears (see Figure 8-2 on page 8-3). See "Viewing IP Parameters" on page 8-21 for more information.

Viewing Ethernet Logical Port Statistics

To view statistics on Ethernet logical port activity:

1. From the Show All Logical Ports in Switch dialog box (see Figure 8-48 on page 8-82), select Options ⇒ IP Parameters.
2. Choose View. The Fast Ethernet Logical Port Statistics dialog box appears.

The Fast Ethernet Logical Port Statistics dialog **b**ox displays statistics defined in the Ascend MIB as well as Internet-standard MIBs RFC1213-MIB-II and RFC1643-EtherLike-MIB. These MIBs are supplied with OpenView.

Table 8-37 describes the Fast Ethernet logical port statistics.

Table 8-37. Fast Ethernet Logical Port Statistics

Statistic	Description
Unicast Packets	Cumulative inbound and outbound statistics for unicast packets: *Inbound* – The total number of subnetwork-unicast packets delivered to a higher-level protocol. *Outbound* – The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Non-unicast Packets	Cumulative inbound and outbound statistics for non-unicast packets: *Inbound* – The total number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-level protocol. *Outbound* – The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
Max Datagram Size (in bytes)	The size of the largest datagram that can be sent or received on the Ethernet interface, in bytes.
Inbound Unknown Protocol	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Alignment Errors	The number of received frames that are not an integral number of octets in length and do not pass the FCS check.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Late Collision Frames	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
SQE Test Errors	The number of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Internal Mac Xmit Errors	The number of frames for which transmission on a particular interface fails due to an internal Media Access Control (MAC) sublayer transmit error.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.
Ethernet Chip Set	The chip set that the interface uses.
Congestion State	One of the following congestion states for the logical port: Normal (1), Mild (2), Severe (3), or Absolute (4).

Table 8-37. Fast Ethernet Logical Port Statistics (Continued)

Statistic	Description
Severely Congested State Count	Number of times that the logical port's congestion state has changed from Mild to Severe since the last reset.
Absolutely Congested State Count	Number of times that the logical port's congestion state has changed from Severe to Absolute since the last reset.
% of Sev/Abs Congested State	The rate of entering Severe or Absolute congested states in the last one minute interval.
SysUpTime Last Error Detected	The amount of time the Ethernet interface had been up when the last error was detected.
Unicast Packets (Throughput in Packets per Second)	Throughput inbound and outbound statistics for unicast packets: *Inbound* – The number of subnetwork-unicast packets delivered to a higher-level protocol per second. *Outbound* – The number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address per second, including those that were discarded or not sent.
Non-unicast Packets (Throughput in Packets Per Second)	Throughput inbound and outbound statistics for non-unicast packets: *Inbound* – The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-level protocol per second. *Outbound* – The number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address per second, including those that were discarded or not sent.
Physical Address	The Ethernet address of the interface.
Outbound Queue Length in Pkts	The length of the outbound packet queue in number of packets.
FCS Errors	The number of frames received that are an integral number of octets (bytes) in length but do not pass the Frame Check Sequence (FCS) check.
Multiple Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
Excessive Collision Frames	The number of frames for which transmission on a particular interface fails due to excessive collisions.
Deferred Xmit Frames	The number of frames for which the first transmission attempt is delayed because the medium is busy.
Internal Mac Rcv Errors	The number of frames for which reception fails due to an internal Media Access Control (MAC) sublayer error.

Table 8-37. Fast Ethernet Logical Port Statistics (Continued)

Statistic	Description
Frame Too Long	The number of frames received that exceeded the maximum frame size.
Priority-1 – Priority-4 Queue Length (pkts)	The transmit queue length, in number of packets, for each priority transmit queue.
Error Type Last Seen	The type of error last detected on the Ethernet interface. Errors include: *1* – Frame too short. *2* – Abort. *3* – Residual bit. *4* – CRC Error. *5* – Receive long. *6* – Receive overrun. *7* – Transmit underrun. *8* – Unknown error.

Troubleshooting IP Problems

As described in "Troubleshooting Network Problems" on page 1-12, you need a proven troubleshooting process to deal with the kinds of complex problems you may encounter in your network. You should base the troubleshooting process for your network problems on the following guidelines:

1. Identify the problem.
2. Verify the problem.
3. Isolate the problem.
4. Take corrective action.

Table 8-38 illustrates how you can apply these guidelines to IP environments.

Table 8-38. Troubleshooting IP Problems

Guideline	Application
Identify the problem.	Look for traps, changes in network map object colors, LEDs changing from green to red, and user complaints. For example, a trap might indicate that a physical port is down, or a user running PING or TRACEROUTE might find a problem.
Verify the problem.	Based on your identification of the problem, use the NMS and console commands to verify it. Check the status of physical ports, logical ports, and PVCs, and determine whether these network objects are sending and receiving data properly. Some key things to look for include: **Physical Ports** – Is the physical port's operational status Up or Down? Is it sending and receiving data? See "Reviewing Physical Port Status" on page 2-44 and "Viewing Physical Port Summary Statistics" on page 3-2. **Logical Ports** – Is the logical port's operational status Up or Down? Is it sending and receiving data? See "Viewing Logical Port Status" on page 6-1. For Frame Relay logical ports that transmit IP traffic, is LMI Operator Status Up or Down? Is the correct DLCI configured? See "Troubleshooting a Frame Relay Logical Port" on page 9-28. For ATM logical ports that transmit IP traffic, is the correct VPI/VCI configured? See "Viewing ATM-Specific Logical Port Attributes" on page 7-1. For Ethernet logical ports, is data being sent and received on the LAN? Is the collision rate high? If so, this indicates a busy LAN. Is the proper framing type configured (Ethernet II or IEEE-SNAP)? See "Viewing Ethernet Logical Ports" on page 8-81. **PVCs** – Is the PVC's operational status Up or Down? Is data being sent and received on the PVC? See "Viewing Point-to-Point ATM PVCs" on page 13-1 for information on viewing ATM PVCs and see "Viewing Frame Relay PVCs" on page 14-1. **IP Configuration Parameters** – Check configuration parameters such as IP addresses and masks for IP, BGP, OSPF, etc.
Isolate the problem.	Use foreground and background diagnostics to isolate physical port and logical port problems (see Chapter 5, "Testing Modules, Ports, and Channels"). Use OAM loopbacks to isolate ATM PVC problems (see "Testing ATM Circuits" on page 13-90). Use PVC loopback to isolate Frame Relay PVC problems (see "Testing Frame Relay PVCs" on page 14-54). Traditional IP troubleshooting tools such as PING and TRACEROUTE can also help you to isolate problems. When isolating the problem, it is important to consult other administrative personnel. For example, you may determine that the source of the problem lies with CPE equipment at a customer site, and you need the assistance of administrative personnel at that site to correct the problem.
Take corrective action.	Corrective action can come in many forms, ranging from re-configuring various parameters to replacing faulty hardware.

9

Monitoring Frame Relay Logical Ports

This chapter describes Frame Relay logical port attributes and statistics (including encapsulated FRAD logical ports and Frame Relay trunk logical ports). For information about monitoring Frame Relay circuits, see Chapter 14, "Monitoring Frame Relay Circuits."

Viewing Frame Relay Logical Port Attributes

You can access the dialog boxes for viewing Frame Relay logical port attributes in two ways:

- From the Monitor menu. This chapter presents this method of accessing Frame Relay logical port attribute dialog boxes.
- From the View Physical Port Attributes dialog box for the physical port to which the Frame Relay logical port is mapped. See "Reviewing Physical Port Status" on page 2-44 for information on this method of accessing logical port attribute dialog boxes.

To view Frame Relay logical port attributes:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1 on page 6-2).
3. Select the appropriate logical port name from the list box on the left.
4. Choose the View Attributes option menu to view various attributes for the selected logical port. Only the selections that apply to the selected logical port appear.

   See Chapter 6, "Monitoring Logical Ports" for information on attributes that are not specific to Frame Relay (administrative, congestion control, and trap control attributes).

Table 9-1 identifies each of the different Frame Relay-specific attribute types you can select, along with a reference to the table that describes the attribute fields.

Table 9-1. Frame Relay-Specific Logical Port Attribute Types

For Information About	See...
Link Management	Table 9-2 on page 9-3
Priority Frame	Table 9-3 on page 9-6
Frame Relay SVC	Table 9-4 on page 9-7
SVC Parameters	Table 9-6 on page 9-10
SVC Routing Priorities	Table 9-7 on page 9-13

Viewing Link Management Attributes

To view link management logical port attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View Link Management Attributes. The Link Management attributes fields appear (see Figure 9-1).

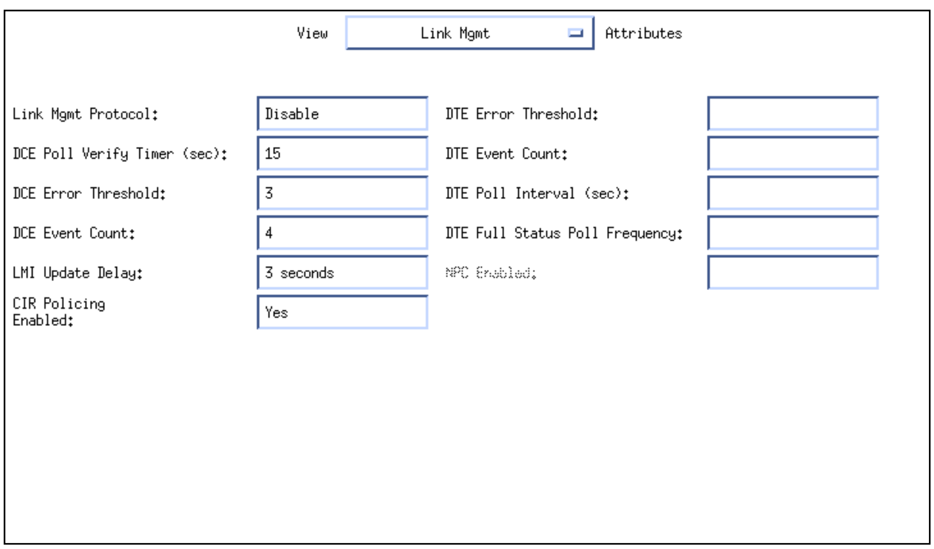


Figure 9-1. Frame Relay Link Management Attributes Fields

Table 9-2 describes the link management attributes fields.

Table 9-2. Link Management Attributes Fields

Field	Displays...
Link Mgmt Protocol	One of the following values to identify the type of link management protocol defined for the selected logical port: *ANSI T1.617 Annex D (default)* – Indicates that the network uses DLCI 0 for link management. *LMI Rev1* – Indicates that the network uses DLCI 1023 for link management. *CCITT Q.933 Annex A* – For international standard (European) use only, indicates that the network uses DLCI 0 for link management. *Auto Detect* – Sets the logical port to automatically detect which protocol is in use. Used only if the attached customer premise equipment (CPE) provides the link management protocol. *Disabled* – Used only if the attached CPE does not support link management or if you need to disable link management for troubleshooting.
DCE Poll Verify Timer (sec)	The value of the T392 timer which specifies the length of time the network should wait between Status Enquiry messages. If no Status Enquiry message is received within the number of seconds specified by the T392 timer, the network records an error. The default is 15 seconds.
DCE Error Threshold	The parameter used in conjunction with the DCE Event Count (N393) parameter. The Local Management protocol monitors the specified number of events for the DCE Event Count. If the number of events found in error exceeds the specified DCE Error Threshold, the link is declared inactive. The default value is 3.
DCE Event Count	The number of events in a sliding window of events monitored by the network. An event is the receipt of a valid or an invalid Status message, or the expiration of the DCE Poll Verify timer. For example, suppose you use the default DCE Error Threshold value of 3 (N392) and the default DCE Event Count of 4 (N393). If N392 of the last N393 events are found in error, the link is declared inactive. The link remains inactive until N393 consecutive error-free events are detected. The default is 4.

Table 9-2. Link Management Attributes Fields (Continued)

Field	Displays...
LMI Update Delay	A value from 1 to 9 seconds to enable asynchronous LMI updates. The default is 3 seconds. The setting of this timer causes the switch to send a signal (known as an event) to notify other network equipment (such as CPE) when a circuit on this logical port goes up or down. If the circuit recovers within this delay, no event is issued. Instead of a specific timer value, one of the following parameters can be set: *No Updates* – The switch does not send a signal to the CPE. *No Delay* – The switch sends an update immediately to the CPE. For example, if the network takes a significant amount of time to recover from trunk outages, you can increase the LMI Update Delay. This delay introduces a time element, which can minimize end-user visibility to a self-recoverable outage.
CIR Policing Enabled	One of the following: *Yes* – CIR policing is enabled. *No* – CIR policing is disabled.
DTE Error Threshold	The parameter used in conjunction with the DTE Event Count (N393) parameter. The Local Management protocol monitors the specified number of events for the DTE Event Count. If the number of events found in error exceeds the specified DTE Error Threshold, the link is declared inactive. The default value is 3.
DTE Event Count	The number of events in a sliding window of events monitored by the network. An event is the receipt of a valid or an invalid Status message, or the non-receipt of a Status Enquiry message after the number of seconds specified by the DTE Poll Interval. For example, suppose you use the default DTE Error Threshold value of 3 (N392) and the default DTE Event Count of 4 (N393). If N392 of the last N393 events are found in error, the link is declared inactive. The link remains inactive until N393 consecutive error-free events are detected. The default is 4.
DTE Poll Interval (sec)	The number of seconds between the transmission of Status Enquiry messages. The default is 10 seconds.
DTE Full Status Poll Frequency	The number of polling cycles between full Status Enquiry messages. The default is 6.
NPC Enabled (NNI, IISP, PNNI Lports only)	One of the following: *Enabled* – The Network Parameter Control (NPC) function, which helps you communicate with other networks, is enabled. Frames that do not conform to the traffic parameters are dropped or tagged as they come into the port. *Disabled* – NPC is disabled. All traffic, including non-conforming traffic, passes in through the port.

Viewing Priority Frame Attributes

Priority frame provides ATM-like Quality of Service for Frame Relay traffic. The following service classes are supported:

Variable Frame Rate Real-Time (VFR-RT) — Provides committed bandwidth, low delay, low delay variation, and low frame loss, enabling service providers to accommodate delay-sensitive traffic such as SNA and voice.

Variable Frame Rate Non-Real Time (VFR-NRT) — Resembles traditional Frame Relay offerings. VFR-NRT provides committed bandwidth and low frame loss, but has a higher delay than VFR-RT. VFR-NRT is designed for LAN-to-LAN and business-class Internet/Intranet access services. This service also provides configurable congestion control.

Unspecified Frame Rate (UFR) — Offers no guarantees except for throughput. UFR provides a best-effort service using any remaining bandwidth. UFR is designed for e-mail, file transfer, and residential Internet access services.

To view priority frame logical port attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View Priority Frame Attributes. The Priority Frame attributes fields appear (see Figure 9-2).

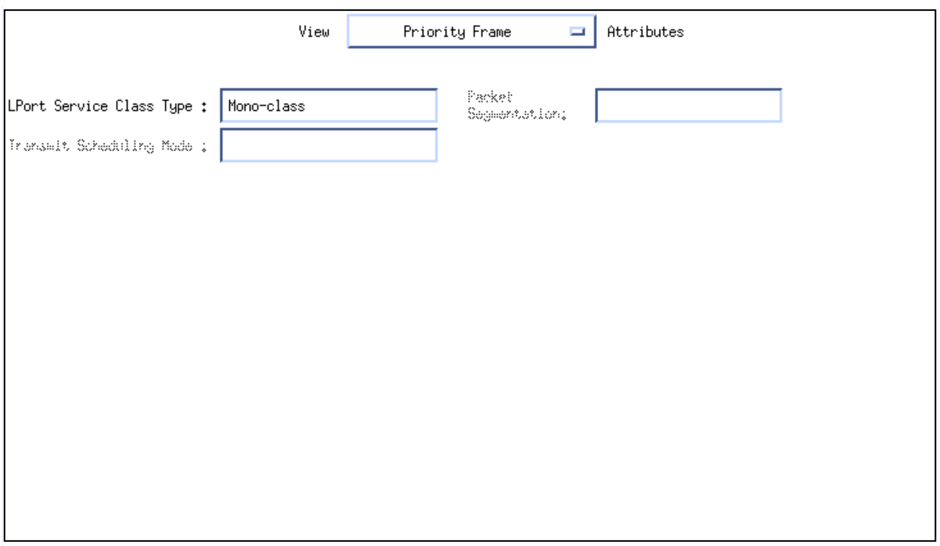


Figure 9-2. Frame Relay Priority Frame Attributes Fields

Table 9-3 describes the priority frame attributes fields.

Table 9-3. Priority Frame Attribute Fields

Field	Displays...
LPort Service Class Type	One of the following logical port service class types: *Mono-class* – Multiple priority bandwidth QoS classes are not supported for the logical port. All traffic is treated as VFR-NRT. *Multi-class* – Multiple priority bandwidth QoS classes (VFR-RT, VFR-NRT, and UFR) are supported for the logical port. For information on viewing the QoS classes and associated parameters configured for the logical port, see “Viewing QoS Parameters” on page 6-13.
Transmit Scheduling Mode	One of the following configured transmit scheduling modes: *Fixed Priority* – Transmit scheduling is according to strict priority in the following order: 1. Control 2. VFR-RT 3. VFR-NRT 4. UFR *Weighted Round Robin* – Control traffic is scheduled “at the head of the line,” and the weighted round robin algorithm is used to schedule VFR-RT and VFR-NRT traffic. A best effort attempt is made for UFR traffic (which has the lowest priority). This field is blank if LPort Service Class Type is *mono-class*.
Packet Segmentation	The segmentation feature of a trunk port: *On* – The port cuts user packets into fixed-length segments for delivery over the trunk. *Off* – The port delivers user packets without segmenting them. If the port service class type is configured as *multi-class*, the default is *On*. If the port service class type is configured as *mono-class*, the default is *Off*.

Viewing Frame Relay SVC Attributes

To view Frame Relay SVC logical port attributes:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View Frame Relay SVC Attributes. The Frame Relay SVC attributes fields appear (see Figure 9-3).

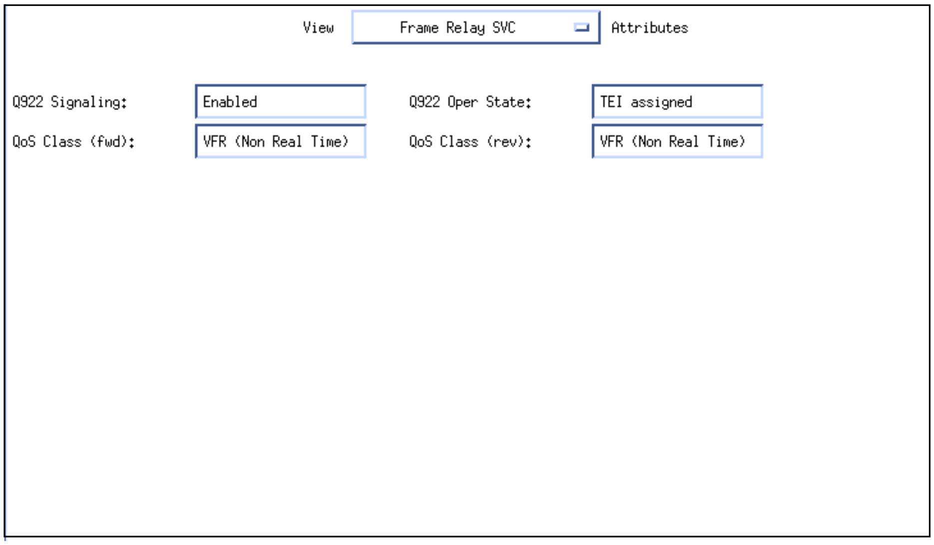


Figure 9-3. Frame Relay SVC Attributes Fields

Table 9-4 describes the Frame Relay SVC attributes fields. For more information on these fields, see the *NavisCore Frame Relay Configuration Guide*.

Table 9-4. Frame Relay SVC Attributes

Field	Displays...
Q922 Signaling	The state of Q.922 signalling, *Enabled* or *Disabled*. Q.922 must be enabled for the logical port to support SVCs.
QoS Class (fwd)	The QoS class for forward traffic on SVCs originating on this logical port.
Q922 Oper State	The current state of Q.922 signaling, if Q.922 signalling is enabled (see Table 9-5).
QoS Class (rev)	The QoS class for reverse traffic on SVCs originating on this logical port.

Table 9-5 describes the states that may appear in the Q.922 Oper State field.

Table 9-5. Q.922 Signaling Operating States

State	Description
Uninitialized	Indicates that Q.922 signaling is disabled.
TEI-Unassigned	A DLCI has not been assigned to the link and no connection has been established. A connection cannot be established until a DLCI is assigned. At this point, the connection establishment procedure can be initiated in two ways: • One side of the connection can issue a unit data request. The unit data request asks that a DLCI be assigned to the link. The issuance of a unit data request changes the state to Assign-Awaiting and then to TEI-Assigned once the DLCI is assigned. While the link is in the TEI-Assigned state, one side of the connection can issue an establish request to establish the connection, at which point the connection enters the Awaiting-Establishment state. • One side of the connection can issue an establish request. The state then changes to Establish-Awaiting until the DLCI is assigned, at which point the state changes to Awaiting-Establishment.
Assign-Awaiting	One side of the connection issued a unit data request, thereby requesting a DLCI for the link. The state changes to TEI-Assigned when the DLCI is assigned to the link.
TEI-Assigned	A DLCI has been assigned to the link but the link has not been established.
Establish-Awaiting	One side of the connection issued an establish request. The DLCI has not been assigned. The state will change to Awaiting-Establishment once the DLCI is assigned.
Awaiting-Establishment	The DLCI has been assigned and both sides of the connection are waiting for the connection to be established.
Multiple-Frame-Established	The link is established. Acknowledged data transfer requests can take place.
Timer-Recovery	The link enters Timer-Recovery state when timer T200 expires. The connection will return to the Multiple-Frame-Established state once the timer recovery procedure is complete.
Awaiting-Release	One side issued a connection release request. The connection then returns to the TEI-Unassigned state.

Viewing Frame Relay SVC Parameters

To view SVC parameters for the logical port:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View SVC Parameters Attributes. The SVC parameters fields appear (see Figure 9-4).

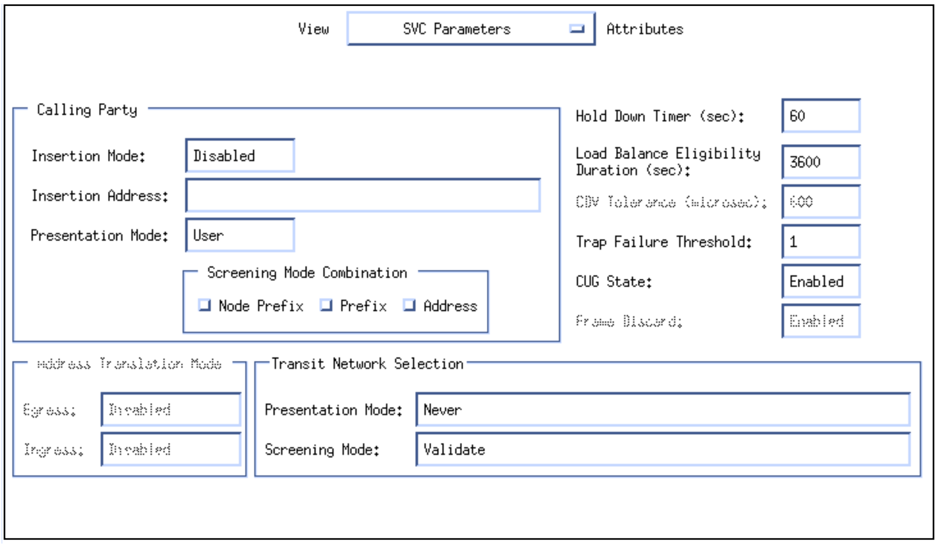


Figure 9-4. Frame Relay SVC Parameters

Table 9-6 describes the Frame Relay SVC parameters.

Table 9-6. Frame Relay SVC Parameters

Field	Displays...
Calling Party Fields	
Insertion Mode	One of the following insertion mode options: *Disabled* – The logical port does not insert or replace the calling party address. *Insert* – If the logical port receives a call that does not have a calling party information element, it inserts the address from the Calling Party Insertion Address field. *Replace* – The logical port takes one of the following actions when it receives a call: • If there is no calling party address, the logical port inserts the calling party address specified in the Calling Party Insertion Address field. • If there is a calling party address, the logical port overwrites the existing calling party information element with the address specified in the Calling Party Insertion Address field.
Insertion Address	The calling party insertion address.
Presentation Mode	One of the following presentation modes: *User* – The logical port includes the calling party address on outgoing calls based on the Presentation Indicator in the SETUP message of the user’s call. *Always* – The logical port always includes the calling party address on outgoing calls, regardless of the Presentation Indicator in the SETUP message of the user’s call. *Never* – The logical port never includes the calling party address on outgoing calls, regardless of the Presentation Indicator in the SETUP message of the user’s call.
Screening Mode Combination	The criteria that an ingress call must match in order to be processed. For example, if Node Prefix and Address are indicated, all ingress calls must match either a valid node prefix or a valid port address.
General Fields	
Hold Down Timer (sec)	The number of seconds to wait before the network initiates call clearing when a trunk has gone down.
Load Balance Eligibility Duration (sec)	The number of seconds an SVC must be established before a call is eligible for load balance rerouting.

Table 9-6. Frame Relay SVC Parameters (Continued)

Field	Displays...
Trap Failure Threshold	The number of failures that must occur during the current 15-minute time period before the switch generates a trap. The internal counter is reset every 15 minutes. The default value of one means that if one SVC failure occurs on a logical port, the switch issues a trap. The switch issues no additional traps until the next 15-minute period expires. If you change the threshold value to 100, it means that 100 SVC failures must occur in a 15-minute window before the switch generates a trap.
CUG State	One of the following: *Enabled* – The logical port supports closed user group (CUG) processing. *Disabled* – The logical port does not support CUG processing.
Transit Network Selection	
Presentation Mode	One of the following egress presentation modes for the logical port: *Never* – Never signal transit network selection (TNS) in egress calls. *Present Signaled TNS Only* – Signal TNS in egress calls only if TNS was signaled by the user in the ingress call. *Signaled or Source Default* – Signal TNS in egress calls only if TNS was signaled by the user in the ingress call or a source default network ID was provisioned at the ingress user's logical port.
Screening Mode	One of the following screening modes for the logical port: *Ignore* – Ignore the signaled TNS. *Accept* – Always accept the signaled TNS. *Validate* – Screen the signaled TNS and ignores it if there is no match.

Viewing SVC Routing Priorities

SVC routing priorities enable you to assign bandwidth and bumping priority to SVCs based on ingress QoS class. The network routes SVCs originating from this logical port according to the SVC ingress QoS class you select.

To view SVC routing priorities attributes for the logical port:

1. Access the Show All Logical Ports in Switch dialog box (see Figure 6-1 on page 6-2).
2. Choose View SVC Routing Priorities Attributes. The SVC routing priorities fields appear (see Figure 9-5).

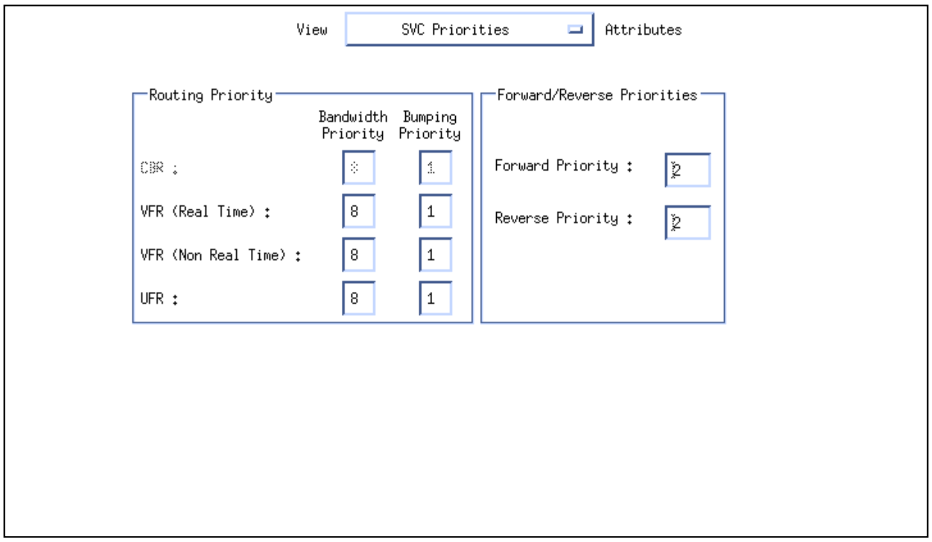


Figure 9-5. Frame Relay SVC Routing Priorities Fields

For each QoS class, the Frame Relay SVC Routing Priorities dialog box displays the *bandwidth priority* and the *bumping priority*. In the event of provisioning, trunk failure recovery, or load balance re-routing, PVCs and SVCs use the combination of bandwidth priority and bumping priority to preserve proper routing priority.

Bandwidth priority is a value from 0 to 15, where 0 is the highest priority. Bumping priority is a value from 0 to 7, where 0 is the highest priority.

Bandwidth priority supersedes bumping priority. The priority routing algorithm favors VCs with lower bandwidth priorities over VCs with higher bandwidth priorities, regardless of their respective bumping priorities.

If both VCs have an equal bandwidth priority, then the priority routing algorithm favors the VC with the lower bumping priority. For example, suppose that two VCs that traverse an optimal path have a bandwidth priority of two, but one VC has a bumping priority of three and the other VC has a bumping priority of four. In the event of a trunk failure, the VC assigned the bumping priority of three will be favored, and the VC assigned the bandwidth priority of four will be forced on to a non-optimal path.

There are additional rules that govern priority routing. See the *NavisCore Frame Relay Configuration Guide* for more information.

Table 9-7 describes the Frame Relay SVC priority routing attributes fields. See "Viewing Priority Frame Attributes" on page 9-5 for a description of the service classes mentioned in the table.

Table 9-7. Frame Relay SVC Priority Routing Attributes

Field	Displays...
VFR (Real Time)	The bandwidth priority and the bumping priority for the VFR-RT QoS.
VFR (Non Real Time)	The bandwidth priority and the bumping priority for the VFR-NRT QoS.
UFR	The bandwidth priority and the bumping priority for the UFR QoS.
Forward Priority	The discard priority level (from one to three) in the forward direction (caller to callee) for SVCs that originate at this logical port. When a particular service category's output queue becomes congested, it must discard cells. The value in this field sets the discard priority for the SVC in the forward direction. The lower the number, the higher the priority (for example, a value of one sets a higher priority than a value of two).
Reverse Priority	The discard priority level (from one to three) in the reverse (callee to caller) direction for SVCs that originate at this logical port. When a particular service category's output queue becomes congested, it must discard cells. The value in this field sets the discard priority for the SVC in the reverse direction. The lower the number, the higher the priority (for example, a value of one sets a higher priority than a value of two).

Viewing Frame Relay Logical Port Summary Statistics

You can access the dialog boxes for viewing Frame Relay logical port summary statistics in two ways:

- From the Monitor menu. This chapter presents this method of accessing Frame Relay logical port summary statistics dialog boxes.
- From the View Physical Port Attributes dialog box for the physical port to which the Frame Relay logical port is mapped. See "Reviewing Physical Port Status" on page 2-44 for information on this method of accessing logical port summary statistics dialog boxes.

To view Frame Relay logical port summary statistics:

1. Select the appropriate switch object on the network map.

2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1 on page 6-2).

3. Select the appropriate logical port name from the list box on the left.

4. Select Options ⇒ Statistics.

5. Choose View. The Logical Port Summary statistics dialog box appears.

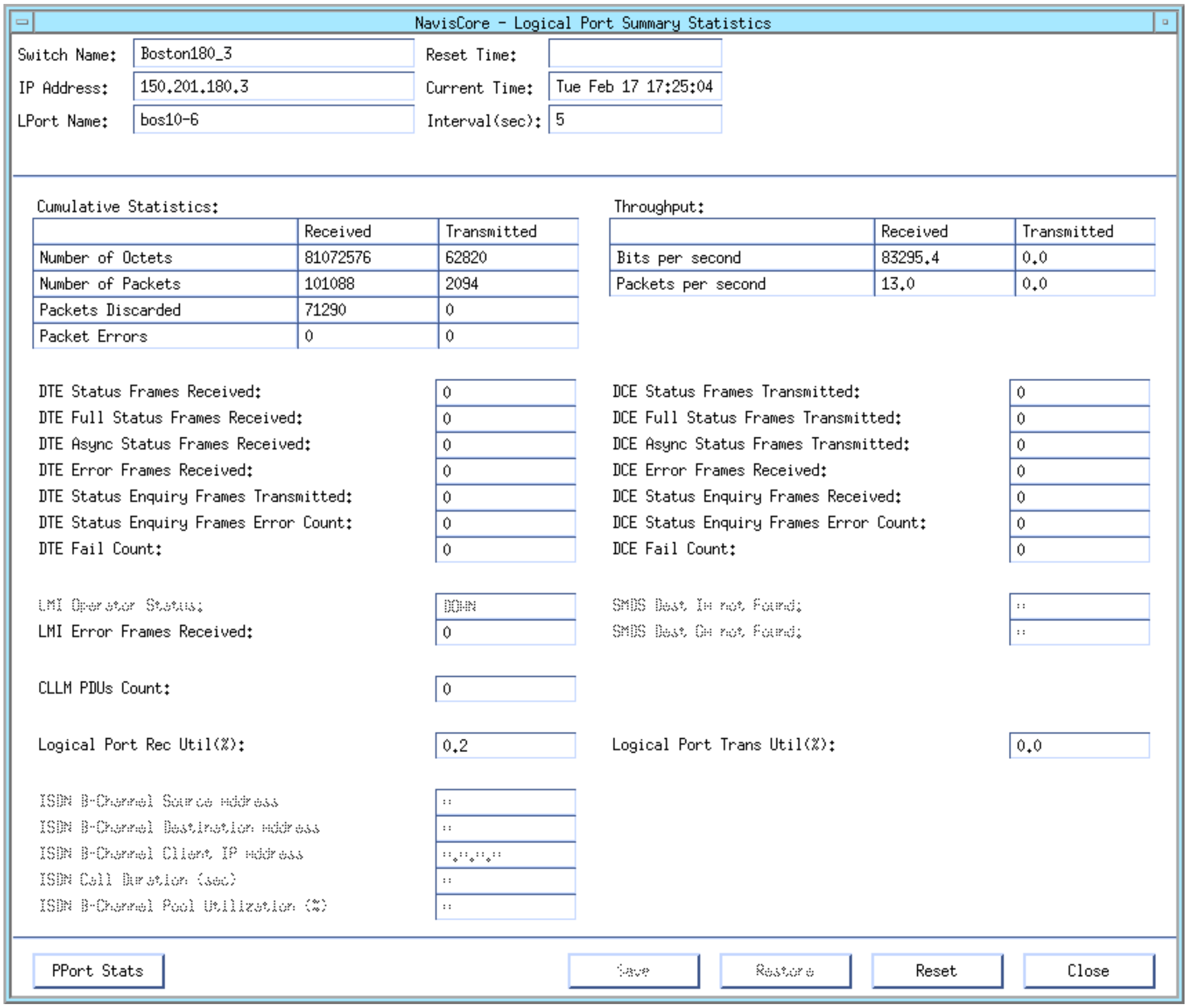


Figure 9-6. Logical Port Summary Statistics Dialog Box

Table 9-8 describes the Logical Port Summary Statistics dialog box buttons.

Table 9-8. Logical Port Summary Statistics Dialog Box Buttons (Frame Relay)

Button	Function
PPort Stats	Displays the Physical Port Summary Statistics dialog box. For details, see "Viewing Physical Port Summary Statistics" on page 3-2.
Reset	Clears the current statistics and updates the time in the Reset Time field.
Close	Closes the dialog box.

The type of statistics that the system displays for a logical port depends on the type of logical port:

UNI-NNI logical port — The system displays both DTE and DCE statistics.

UNI-DCE logical port — The system displays only DCE statistics.

UNI-DTE logical port — The system displays only DTE statistics.

If the link management interface (LMI) protocol is disabled, the system does not display any DTE or DCE statistics for a logical port. You set the LMI interface protocol when you define the parameters for a logical port. See the *NavisCore Frame Relay Configuration Guide* for more information about defining the LMI protocol.

Table 9-9 lists and describes the Frame Relay logical port summary statistics shown in Figure 9-6. Table 9-9 includes DTE as well as DCE statistics.

Table 9-9. Frame Relay Logical Port Summary Statistics

Statistic	Description
Identifying Fields	
Switch Name	The name of the switch associated with the logical port.
IP Address	The internal IP address of the switch.
LPort Name	The name that identifies this logical port.
Reset Time	The time of the last reset of the statistics.
Current Time	The current system time.
Interval (sec)	The time interval for the collection of statistical data. The default is 5. See “Setting the Polling Interval” on page 3-2 for details about how to set this value.
Cumulative Statistics	
Number of Octets	The number of octets (bytes) received and transmitted since the last reset.
Number of Packets	The number of packets (frames) received and transmitted since the last reset.
Packets Discarded	The number of packets (frames) discarded since the last reset.
Packet Errors	The number of packet (frame) errors since the last reset.
Throughput Statistics	
Bits per second	The number of bits received and transmitted each second.
Packets per second	The number of packets (frames) received and transmitted each second.

Table 9-9. Frame Relay Logical Port Summary Statistics (Continued)

Statistic	Description
DTE Statistics	
DTE Status Frames Received	The number of LMI Status frames received on this logical port from the DCE device. This only includes Status frames with a report type of LIV (link integrity verification).
DTE Full Status Frames Received	The number of LMI Status frames received on this logical port from the DCE device. This only includes Status frames with a report type of full. Full Status frames include the status (for example, active or inactive) of each PVC configured on the DCE device for this link.
DTE Async Status Frames Received	The number of Asynchronous LMI Status frames received on this logical port from the DCE device. For logical ports configured for ANSI Annex D or CCITT Annex A, this count includes only Status frames with a report type of Async. For logical ports configured for LMI Revision 1, this count includes only the number of Update Status messages received from the DCE device.
DTE Error Frames Received	The number of LMI Status frames received (either LIV or Full) which contained either an invalid receive sequence number (Nr) or an invalid send sequence number (Ns). Any value other than zero in this field indicates a problem.
DTE Status Enquiry Frames Transmitted	The number of LMI Status Enquiry frames transmitted on this logical port. This includes both LIV and Full Status Enquiry messages.
DTE Status Enquiry Frames Error Count	The total number of LMI errors on this logical port. These errors include the following: • Error frames received from the DCE device. • The number of times a Status frame (LIV and Full) wasn't received in response to a Status Enquiry. An error is counted each time a Status Enquiry is transmitted, if a Status message was not received since the last Status Enquiry was sent. Any value other than zero in this field indicates a problem.
DTE Fail Count	The number of times the LMI protocol declares the link to be down. The protocol declares the link as down if N392 out of N393 events are in error. The DTE Status Enquiry Frames Error Count statistic outlines the reasons for counting a condition as an error. See Table 9-2 on page 9-3 for an explanation of N392 and N393.
DCE Statistics	
DCE Status Frames Transmitted	The number of LMI Status frames transmitted on this logical port. This statistic includes all Status frames with a report type of LIV (link integrity verification).

Table 9-9. Frame Relay Logical Port Summary Statistics (Continued)

Statistic	Description
DCE Full Status Frames Transmitted	The number of LMI Status frames transmitted on this logical port from the DCE device. This statistic includes all Status frames with a report type of Full. Full Status frames include the status (for example, active or inactive) of each PVC configured on this logical port.
DCE Async Status Frames Transmitted	The number of asynchronous LMI Status frames transmitted on this logical port. For logical ports configured for ANSI Annex D or CCITT Annex A, this count includes only Status frames with a report type of Async. For logical ports configured for LMI Revision 1, this count includes only Update Status messages.
DCE Error Frames Received	The number of LMI Status Enquiry frames received (either LIV or Full) that contain either an invalid receive sequence number (Nr) or an invalid send sequence number (Ns).
DCE Status Enquiry Frames Received	The total number of LMI Status Enquiry frames received on this logical port. This statistic includes both LIV and Full Status Enquiry messages.
DCE Status Enquiry Frames Error Count	The total number of LMI errors on this logical port. These errors include the following: • The number of times a Status Enquiry frame (LIV and Full) was not received during a T392 second interval. See Table 9-2 on page 9-3 for an explanation of T392. • The number of times the LMI protocol declares the link to be down. See the description of the DCE Fail Count field for more information. Any value other than zero in this field indicates a problem.
DCE Fail Count	The number of times the LMI protocol declares the link to be down. The protocol declares the link as down if N392 out of N393 events are in error. The DCE Status Enquiry Frames Error Count statistic outlines the reasons for counting a condition as an error. See Table 9-2 on page 9-3 for an explanation of N392 and N393.
LMI Status Information	
LMI Operator Status	The state of the connection between the two communication devices for which you are collecting statistics. If the logical port is functioning properly, this value should display as *Up*. You may encounter a situation where LMI Operator Status is *Down*, but the operating status of the logical port is *Up*. This indicates that a problem lies with link management, not with the physical link itself. If the value for this field is not set to *Up*, check to see if the DCE Poll Timer at the logical port is set to a value that is less than the keep alive value set on the FRAD (router). If the switch does not receive a poll before this timer expires, LMI will not come up.

Table 9-9. Frame Relay Logical Port Summary Statistics (Continued)

Statistic	Description
LMI Error Frames Received	The number of LMI error frames that were received. If you are collecting statistics for a UNI-NNI logical port, this value is the sum of all DCE and DTE error frames.
CLLM Statistic	
CLLM PDUs Count	The number of transmitted CLLM PDUs. See "Monitoring CLLM Congestion Notification" on page 9-22 for more information on CLLM.
Utilization Statistics	
Logical Port Rec Util (%)	The amount of traffic received on a logical port as a percentage of the committed information rate (CIR). It does not measure the amount of bandwidth of the logical port, so the value that the system displays in this field can exceed 100%.
Logical Port Trans Util (%)	The amount of traffic queued for transmission on a logical port as a percentage of the CIR. It does not measure the amount of bandwidth of the logical port, so the value that the system displays in this field can exceed 100%.

Monitoring Multilink Frame Relay

Multilink Frame Relay (MLFR) provides additional bandwidth by allowing you to aggregate up to 32 separate trunks to act as a single Frame Relay trunk. The aggregate trunk is called a *bundle*; the individual trunks that make up the bundle are called *members*. Each bundle is configured as a logical port, and each member is also configured as a logical port.

MLFR is supported on B-STDX 9000 switches only. For information on setting up MLFR trunks, see the *NavisCore Frame Relay Configuration Guide*.

Viewing MLFR Bundles

To view MLFR bundles:

1. Select the B-STDX 9000 switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel Dialog Box appears. The exact appearance of the Switch Back Panel Dialog Box depends on the configuration of the switch you are monitoring. See "Viewing Switch Details" on page 2-9 for more information on switch back panels.
3. Select the IOM connected to the MLFR trunk. The View Card Attributes dialog box appears.
4. Select View MLFR Bundles. The View MLFR Trunk Bundle LPorts dialog box appears.

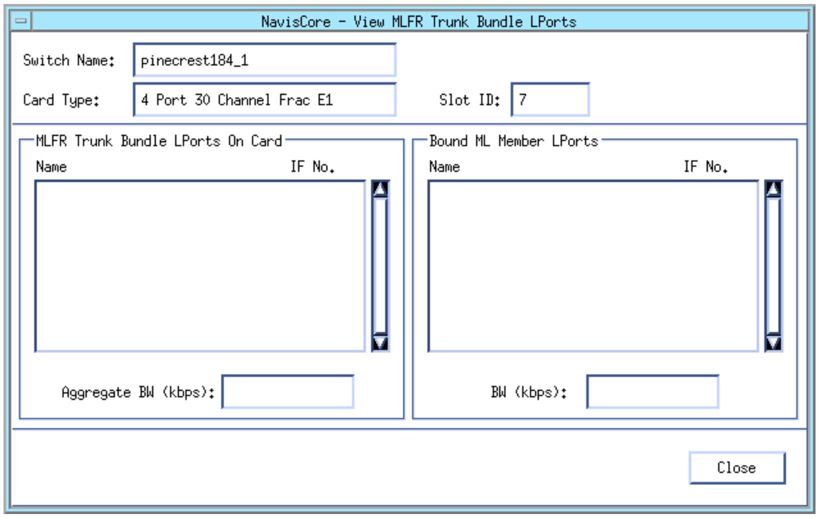


Figure 9-7. View MLFR Trunk Bundles LPorts Dialog Box

Table 9-10 lists and describes the fields on the dialog box.

Table 9-10. View MLFR Trunk Bundles LPort Dialog Box Fields

Field	Displays...
Switch Name	The name of the B-STDX switch you are monitoring.
Card Type	The type of IOM you selected.
Slot ID	The physical slot number where the I/O module that contains the selected port is installed.
MLFR Trunk Bundle LPorts on Card	
Name	The name assigned to the logical port associated with the trunk bundle.
IF No.	The trunk bundle logical port's interface number.
Aggregate BW (kbps)	The aggregate bandwidth of the trunk bundle in kilobits per second.
Bound ML Member LPorts	
Name	The name assigned to the logical port associated with each member.
IF No.	The member logical port's interface number.
BW (kbps)	The bandwidth of each member in kilobits per second.

Viewing MLFR Logical Port Attributes

You view MLFR logical port attributes in very much the same way that you view attributes for Frame Relay direct trunk logical ports. See "Viewing Frame Relay Logical Port Attributes" on page 9-1 for more information.

Keep in mind that a logical port is defined for each bundle, and a logical port is defined for each member.

When you view logical ports associated with bundles, you can view Administrative, Trap Control, Congestion Control, and Priority Frame attributes.

Administrative attributes are the only valid attributes for member logical ports. If the member logical port is bound to an MLFR trunk bundle logical port, the name of the bundle to which the member is bound appears. Otherwise, the field that displays the name of the bundle is blank.

Viewing MLFR Logical Port Summary Statistics

You can view summary statistics for logical ports associated with bundles and logical ports associated with members. For instructions on how to view logical port summary statistics, see "Viewing Frame Relay Logical Port Summary Statistics" on page 9-14.

When you view activity statistics on logical ports associated with bundles, the statistics reflect aggregate activity on all the member logical ports.

When you view activity statistics on logical ports associated with members, the statistics reflect activity on a specific logical port.

Monitoring CLLM Congestion Notification

Network congestion occurs when the available bandwidth to handle network traffic is insufficient. When a Frame Relay network becomes congested, switches discard frames until the congestion diminishes.

Frame Relay supports two types of congestion control: *implicit* and *explicit.*

Implicit congestion control involves using certain data link layer events to detect the frame loss.

Explicit congestion control involves the following types of notification:

Forward Explicit Congestion Notification (FECN) / Backward Explicit Congestion Notification (BECN) — Flow control is built into the Frame Relay header in the form of FECN and BECN bits.

Consolidated Link Layer Management (CLLM) — CLLM congestion notification occurs during increases in network traffic load. One DLCI address (1007) is reserved exclusively for transmitting congestion notification.

About CLLM

You can enable or disable CLLM on any Frame Relay UNI or NNI port. The CLLM mechanism applies to PVCs only. The switch reserves DLCI address 1007 exclusively for transmitting congestion notification messages to the user device. A CLLM message is sent periodically to the CPE or network access device until congestion is alleviated. A CLLM message notifies users of congestion activity outside the conventional framing structure. A CLLM message that is generated as a result of congestion contains a list of DLCIs that correspond to the congested Frame Relay bearer connections.

In addition to notifying users of congested VCs, a CLLM message can also notify users of inactive VCs. In this case, the CLLM message contains a list of all VCs that are not in an active state.

Each CLLM message supports a maximum of 127 DLCIs. The switch may transmit multiple messages during a CLLM update. You can configure the time duration between each consecutive CLLM update.

► If you are already using DLCI 1007, you must delete the PVC and assign a new DLCI number if you want to enable CLLM.

Computing the Time-Averaged Percentage of BECN Frames

To measure congestion at every logical port, switches compute the time-averaged percentage of BECN frames. After every CLLM interval, the switch computes the percentage of BECN frames out of the total number of frames received on all of the UNI logical port's VCs. After this computation, the switch then uses the following formula to compute the time-averaged percentage of BECN frames:

Time-Average % BECN Frames = [0.75 * X] + [0.25 * Y]
X = Previous Time-Average Percentage of BECN Frames
Y = Percentage of BECN Frames Out of Total Received

When the next CLLM interval expires, the current time-averaged percentage of BECN frames becomes the previous time-averaged percentage of BECN frames, and is used by the switch to compute the new time-averaged percentage of BECN frames.

CLLM Threshold States

The configurable parameters, CLLM Thrhld None and CLLM Thrhld Mild, determine the VC congestion threshold type and congestion state. These parameters represent a percentage of BECN frames received since the last CLLM message. The following guidelines determine the congestion state:

- If the time-averaged percentage of BECN frames received on any VC on the logical port does not exceed the configured CLLM Threshold None, the VC is not congested.
- If the time-averaged percentage of BECN frames received on any VC on the logical port exceeds the configured CLLM Threshld None but does not exceed the configured CLLM Threshld Mild, the VC is considered to be in a mildly congested state.
- If the time-averaged percentage of BECN frames received on any VC on the logical port exceeds the configured CLLM Threshld Mild, the VC is considered to be in an absolute congested state.
- If the operational status of the VC is down, the VC is considered out of service.

CLLM Messages

Based on the congestion threshold state, there are three types of CLLM messages:

Absolute CLLM — A list of all VCs that are in absolute congested state.

Mild CLLM — A list of all VCs that are in a mildly congested state.

Inactive CLLM — A list of all VCs whose operational status is down.

For example, a network has three VCs on a Frame Relay UNI port. One VC is in the absolute congested state, another VC is in the mild congested state, and the third VC is down. The switch sends three CLLM messages: an absolute CLLM message reports the VC that is in absolute congested state; a mild CLLM message reports the VC that is mild congested state; and an inactive CLLM messages reports the VC that is down.

Viewing CLLM Fields

The CLLM fields appear when you display Congestion Control attributes for a selected Frame Relay UNI logical port. See "Viewing Congestion Control Attributes" on page 6-10 for more information on displaying Congestion Control attributes.

For information on configuring CLLM, see the *NavisCore Frame Relay Configuration Guide*.

Table 9-11 lists and describes the CLLM fields.

Table 9-11. CLLM Fields

Field	Displays...
CLLM Admin State	One of the following: *Enable* - Enables CLLM notification on the logical port. *Disable* (default) - Disables CLLM notification on the logical port.
CLLM Interval (sec)	The number of seconds between two consecutive CLLM updates sent on the logical port. The CLLM update is sent as long as at least one VC on this logical port remains in a congested state or an out of service state. The default is 10 seconds.
CLLM Thrhld None (%)	The threshold percentage value (between 1-100) of BECN frames received on any VC on this port. The default is 10.
CLLM Thrhld Mild (%)	The threshold percentage value (between 1-100) of BECN frames received on any VC on this port. The value of CLLM Thrhld Mild must be equal to or greater than the value of CLLM Thrhld None. The default is 40.

Viewing CLLM PDU Statistics

A statistic on CLLM PDU activity appears when you display logical port summary statistics for the Frame Relay UNI logical port. See "Viewing Frame Relay Logical Port Summary Statistics" on page 9-14 for more information on displaying Frame Relay logical port summary statistics.

Viewing the Status of Multicast DLCIs

The Show All Multicast DLCIs function displays the list of Multicast DLCIs configured in the network. A Multicast DLCI is a circuit configured to send a multiple set of circuits on the same logical port. Using a single DLCI number, you can set up a member list of DLCIs. When the CPE sends traffic on the DLCI, the switch replicates the frames and transmits them over the member circuits.

To view all configured Multicast DLCIs, perform the following steps:

1. From the Monitor menu, select Ascend Objects ⇒ Show All Multicast DLCIs. The Show All Multicast DLCIs dialog box appears (see Figure 9-8).

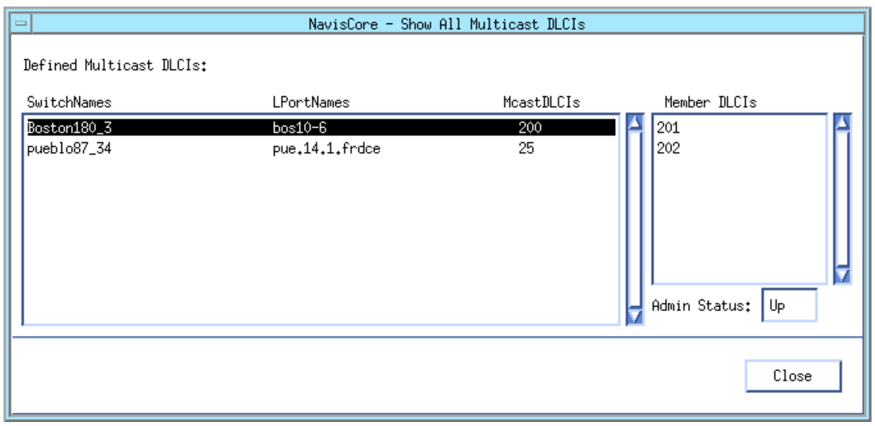


Figure 9-8. Show All Multicast DLCIs Dialog Box

When you finish reviewing the status information, choose Close to return to the network map.

Table 9-12 describes the Show All Multicast DLCIs dialog box fields.

Table 9-12. Show All Multicast DLCIs Fields

Field	Displays...
Switch Names	The name of the switch for which the multicast DLCI is configured.
LPort Names	The name of the logical port for which the DLCI is configured.
Mcast DLCIs	The number that uniquely identifies the multicast DLCI configured for this switch.
Member DLCIs	A DLCI for each member of the DLCI multicast group.
Admin Status	Whether the multicast DLCI is administratively *up* or *down.*

Viewing the Status of Management DLCIs

The Show All Management DLCIs function displays the status of all Management DLCIs configured on the network. A Management DLCI provides connectivity from the NMS to the Ascend network, as well as a method of monitoring and controlling the network without the use of Ethernet. This method connects a circuit through a router to the Ascend network. For more information about how to configure a Management DLCI, see the *NavisCore Frame Relay Configuration Guide*.

To view all configured Management DLCIs, complete the following steps:

1. From the Monitor menu, select Ascend Objects ⇒ Show All Management DLCIs. The Show All Management DLCIs dialog box appears (Figure 9-9).

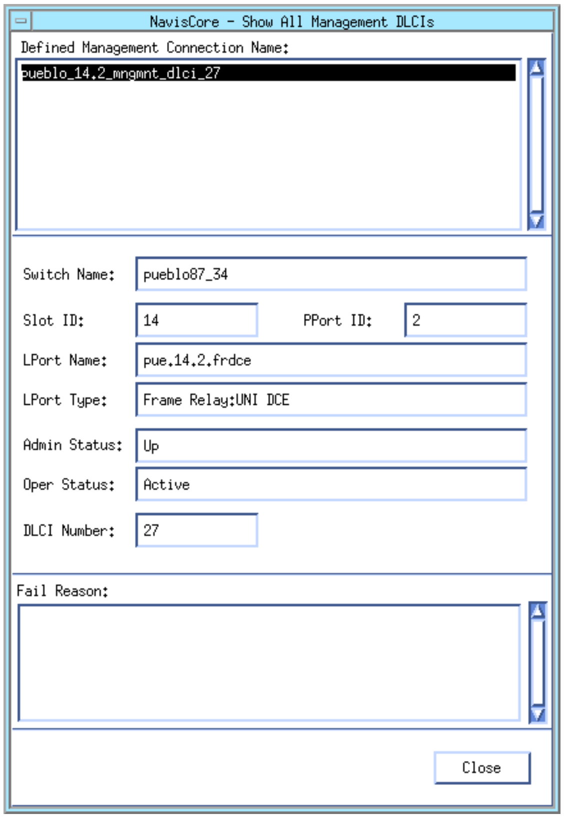


Figure 9-9. Show All Management DLCIs Dialog Box

2. When you finish reviewing the status information, choose Close to return to the network map.

Table 9-13 describes the Show All Management DLCIs dialog box fields.

Table 9-13. Show All Management DLCIs Fields

Field	Displays...
Defined Management Connection Name	The name configured for the management DLCI.
Switch Name	The name of the switch for which you configured the management DLCI.
Slot ID	Indicates the physical slot number where the I/O module that contains the selected port is installed.
PPort ID	The ID number of the physical port for which the selected logical port is configured.
LPort Name	The name of the logical port on the switch.
LPort Type	The type of port configured for this logical port.
Admin Status	One of the following: *Up* – The management DLCI configuration is administratively up. *Down* – The management DLCI configuration is administratively down.
Oper Status	The operational status of the management DLCI. Possible values include: *Active* – The connection is operational. *Inactive* – The connection is not operational. *Unknown* – The connection configuration is not contained within the calling node. *Invalid* – The calling node did not respond to the NMS request for the status of this connection.
DLCI Number	The number that uniquely identifies this management DLCI configuration.
Fail Reason	A reason code if the Operator Status is Inactive. See Table 14-3 on page 14-5 for more information.

Troubleshooting a Frame Relay Logical Port

The Frame Relay Logical Port Summary Statistics dialog box (Figure 9-6) provides you with a lot of useful information for troubleshooting Frame Relay logical port problems.

Follow these steps to check for a logical port problem:

1. Display the Logical Port Summary Statistics dialog box. See "Viewing Frame Relay Logical Port Summary Statistics" on page 9-14 if you are not sure about how to do this.
2. Check to see if the LMI Operator Status displays a value of *Up*. If it is set to *Down,* there is a problem with the logical port. See Table 9-9 for more information about this statistic.
3. Check to see if the logical port is transmitting and receiving LMI status frames. This information is displayed in the Cumulative Statistics fields. If no frames are being transmitted or received, there is a problem with the logical port.
4. Check for DCE or DTE errors, which indicate a problem with the logical port.

LMI Operator Status is an extremely important indicator. For a Frame Relay logical port to operate properly, LMI Operator Status must be *Up*. Because Frame Relay is a connection-oriented protocol, the DTE must know the status of the logical link to the DCE at all times.

When LMI Operator Status is *Down,* the operational status of any PVCs associated with the logical port will be Inactive. See the description of Oper Status in Table 14-4 on page 14-8 for more information on Frame Relay PVC status.

LMI Operator Status could be *Down* for any of the following reasons:

- CPE equipment such as a router may have been powered down. In this case, look for a trap that indicates a change in logical port status.
- A physical layer problem may exist. In this case, look for a trap that indicates a change in physical port status or physical port summary statistics errors. Examples of physical layer problems include bad cables, a bad DS1 channel or DS0 channel or a misconfigured physical port. See "Viewing Physical Port Summary Statistics" on page 3-2 for more information on physical port summary statistics.
- A Frame Relay configuration error may exist. Look for errors on the Frame Relay Logical Port Summary Statistics dialog box. Examples of configuration problems include a mismatched LMI, a misconfigured DCE poll timer, and a misconfigured logical port type.
- Hardware failures, as indicated by traps and background diagnostics. Check for problems with CSUs/DSUs, routers, carrier equipment, and Ascend equipment.

10

Monitoring SMDS

This chapter describes SMDS attributes and statistics. It also describes how to monitor the status of SMDS management addresses and routes, and how to isolate network problems by disabling the SMDS switching system in the network.

Viewing SMDS Logical Port Attributes

To view SMDS logical port attributes:

1. Select the appropriate switch object on the network map.

2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1 on page 6-2).

3. Select the appropriate logical port name from the list box on the left.

4. From the View Attributes option menu, select SMDS to view SMDS-specific attributes. The SMDS-specific attributes appear in the bottom part of the dialog box. Table 10-1 lists and describes these attributes.

See Chapter 6, "Monitoring Logical Ports" for information on attributes that are not specific to SMDS (administrative, congestion control, and trap control attributes).

Table 10-1. SMDS-Specific Attribute Fields

Field	Displays...
Support Heart Beat Poll	Whether heart beat polls are supported. Heart beat polls check for a keep-alive signal coming from the CPE. The field displays *Yes* (*default*) only if the CPE connected to this port supports heart beat poll responses; otherwise displays *No*.
Heart Beat Poll Interval (1 - 40 sec)	The lapse of time between heart beat polling requests sent to the CPE. This value has a range between 1 and 40 seconds; the default is 10 seconds.
Heart Beat Poll Threshold (1 - 255)	The configured threshold of heart beat polling requests that can go unanswered before a trap is recorded in the event log. A threshold crossing alert (trap) is sent to the NMS each time the threshold for the DXI/SNI (Data Exchange Interface Protocol/Subscriber-Network Interface Protocol) is exceeded within a 15-minute time period. The unanswered heart beat poll count is reset every 15 minutes. This value has a range between 1 and 255; the default value is 30.
Protocol Error Checking	The level of protocol error checking performed on PDUs received by this logical port. This field is *enabled for debugging purposes only.* *On* – Complete Level 2 protocol error checking occurs. This activates Level 2 protocol error counters and you can use SMDS logical port statistics to view these errors (if any). There is a slight performance cost if you enable protocol error checking. *Off (default)* – Minimal address checking occurs.
Billing	One of the following: *Enabled* – SMDS billing is enabled. *Disabled* – SMDS billing is disabled.
Multiplex to this SSI: Switch	An individual address, if you are monitoring a DXI/SNI logical port that is multiplexed to a specific SMDS-to-Access Server interface-Data Terminal Equipment (SSI-DTE) logical port.
Multiplex to this SSI: LPort	The SSI-DTE logical port, if you are monitoring a DXI/SNI logical port that is multiplexed to a specific SSI-DTE logical port.

Viewing SMDS Logical Port Summary Statistics

To view SMDS logical port summary statistics:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (see Figure 6-1 on page 6-2).
3. Select the appropriate logical port name from the list box on the left.
4. Select Options ⇒ Statistics.
5. Choose View. The SMDS Logical Port Statistics dialog box appears.

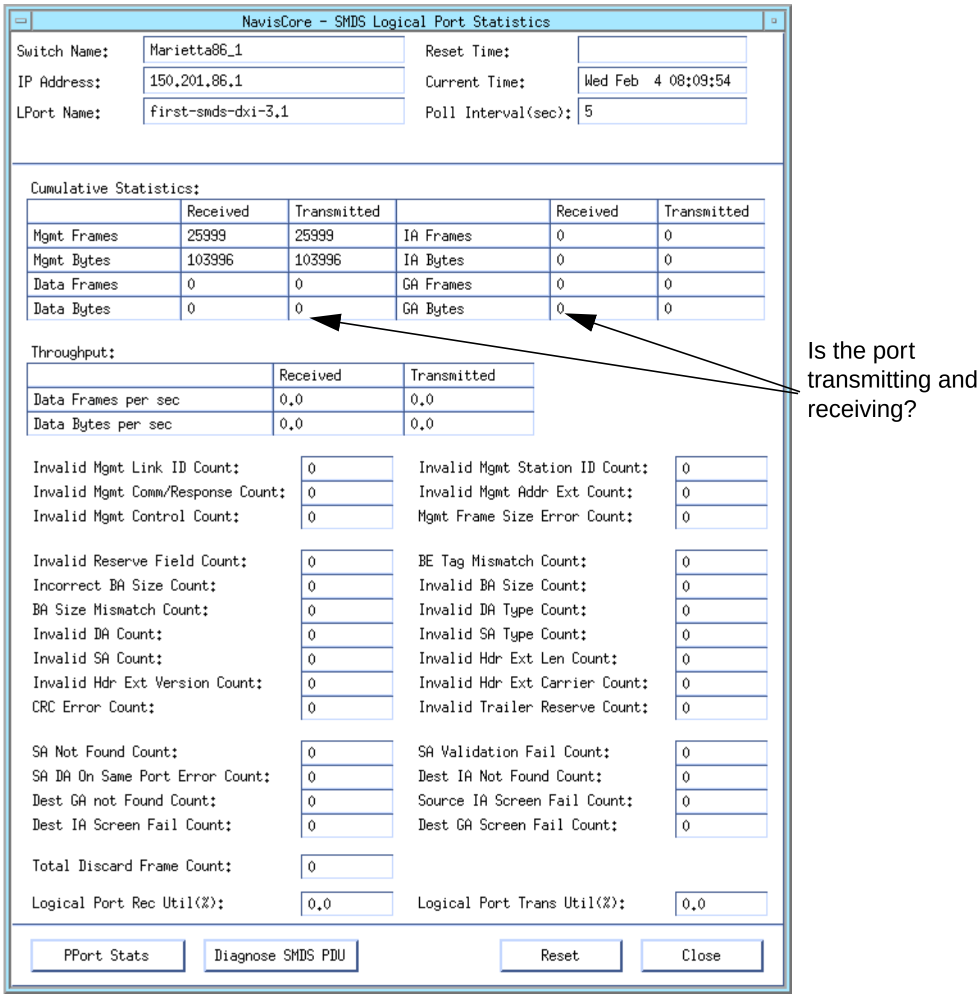


Figure 10-1. SMDS Logical Port Statistics

▶ NavisCore does not report values for the IA frame and GA frame counts for switches running switch software prior to release 4.2.

Table 10-2 describes all of the identifying, cumulative, and throughput information in the SMDS Logical Port Summary Statistics dialog box (see Figure 10-1).

Table 10-2. SMDS Identifying, Cumulative, and Throughput Descriptions

Statistic	Description
Identifying Fields	
Switch Name	The name of the switch where this logical port resides.
IP Address	The Ethernet IP address of the switch.
LPort Name	The name that identifies this logical port.
Reset Time	The time of the last reset of the statistics.
Current Time	The current system time.
Poll Interval (sec)	The time interval for the collection of statistical data. The default is 5. See "Setting the Polling Interval" on page 3-2 for details about how to set this value.
Cumulative Statistics	
Management Frames	The number of management frames received and transmitted since the last reset.
Management Bytes	The number of management bytes received and transmitted since the last reset.
Data Frames	The number of data frames received and transmitted since the last reset.
Data Bytes	The number of data bytes received and transmitted since the last reset.
IA Frames	The number of individually addressed frames received and transmitted since the last reset. Each frame is sent to a single address.
IA Bytes	The number of bytes in individually addressed frames received and transmitted since the last reset.
GA Frames	The number of group addressed frames received and transmitted since the last reset. Each frame is sent to multiple addresses (similar to multicasting).
GA Bytes	The number of bytes in group addressed frames received and transmitted since the last reset.
Throughput Statistics	
Data Frames per second	The number of data frames received and transmitted each second.
Data Bytes per second	The number of data bytes received and transmitted each second.

The SMDS Logical Port Statistics dialog box provides four different types of summary statistics about each logical port:

SMDS PDU Violation Statistics (S) — NavisCore increments a counter every time an SMDS protocol data unit (PDU) violation occurs on a logical port. The system maintains ten separate counters for each logical port to record the 10 SMDS PDU checks that the system *always* performs when switching SMDS packets.

Protocol Error Checking Statistics (P) — These statistics are recorded only when protocol error checking is on. (This value is set through NavisCore when you add the logical port.) If this parameter is set to *on*, complete protocol error checking occurs. If it is set to *off*, no protocol errors are recorded.

Miscellaneous Statistics (M) — Statistics that do not belong to the S or P categories.

Unsupported Statistics (U) — Statistics that are not used or not currently supported.

Table 10-3 describes each of the summary statistics shown in Figure 10-1.

> "The number of times" in the Displays field refers to the total number of frames counted since the system up time of the card.

Table 10-3. SMDS Logical Port Summary Statistics

Statistic	Type	Description
BA Size Mismatch Count	P	The number of times that the SMDS Interface Protocol (SIP) Level 3 PDU buffer allocation (BA) values in the header and trailer did not match. The BA size value resides in the header; the BA length value resides in the trailer. The BA size value must equal the length value of the frame, or a mismatch count is recorded.
BE Tag Mismatch Count	P	The number of times that the SIP Level 3 PDU beginning and end (BE) tag did not match. A BE tag resides in both the header and trailer portions of a frame. The value is incremented by one for each frame that is transmitted from 0 to 255. After the 255th frame, the counter is reset to 0. If the value of the BE tag in the header and trailer do not match, the BE Tag Mismatch Count increments.
CRC Error Count	U	Not used.
Dest GA Not Found Count	S	The number of times that the destination group address (GA) was not found because the switch configuration did not specify the destination GA.

Table 10-3. SMDS Logical Port Summary Statistics (Continued)

Statistic	Type	Description
Dest IA Not Found Count	S	The number of times that the destination individual address (IA) was not found because the switch configuration did not specify the destination IA.
Dest IA Screen Fail Count	S	The number of times that the Destination IA screen failed. Each time a user device transmits a packet to an Ascend switch, the packet is screened at the ingress port to verify that the source destination IA is authorized for a particular end-user port.
Dest GA Screen Fail Count	S	The number of times that the Destination Group Address (GA) screen failed. Each time a user device transmits a packet to an Ascend switch, the packet is screened at the ingress port to verify whether or not the destination is authorized to communicate with the source.
Incorrect BA Size Count	P	The number of times that the SIP Level 3 PDU BA size was invalid. For ease of process, the BA size must be divisible by 4. A BA size that is not divisible by 4 indicates that a packet is incorrectly padded, and therefore invalid.
Invalid BA Size Count	P	The number of times that the SIP Level 3 PDU BA size was invalid. As noted in the previous statistic, the BA size must be divisible by 4. In addition, when 12 is added to the BA size value, the result must be equal to the total number of bytes in the frame. If it is not equal, the BA size is invalid.
Invalid DA Count	U	Not used.
Invalid DA Type Count	P	The number of times that the DA type was invalid. Valid E.164 addresses start with either an *E* or a *C* prefix, as follows: • An *E* indicates a group address. • A *C* indicates an individual address. Any other prefix type is invalid.
Invalid Hdr Ext Carrier Count	U	Not used.
Invalid Hdr Ext Len Count	P	The number of times that the SIP Level 3 PDU Header Extension Length (HEL) was invalid. The HEL value resides in the header of the frame. The only valid value for the HEL is 03. If the HEL value is anything other than 03, the frame is dropped and the Invalid Hdr Ext Len Count value increments.
Invalid Hdr Ext Version Count	U	Not used.

Table 10-3. SMDS Logical Port Summary Statistics (Continued)

Statistic	Type	Description
Invalid Mgmt Addr Ext Count	P	The number of times that the Data Exchange Interface (DXI) Level 2 PDU Address Extension (AE) field was invalid. The AE bit is the least significant bit (LSB) of the DXI frame. The only valid value for the AE field is 1; if the value is 0, the frame is dropped. Possible causes of an invalid value are: 1. An incorrectly configured router. 2. Corruption by either the line or a user device (including an Ascend user device).
Invalid Mgmt Comm/Response Count	P	The number of times that the Data Exchange Interface (DXI) Level 2 PDU command/response field was invalid. This situation occurs if the Ascend switch cannot communicate with the user device or if the user device is out-of-service. If the heartbeat poll option is set to *Yes*, and the router doesn't respond after five consecutive fail counts, a trap is sent and the count value increments. For this statistic to function, either the Ascend switch or the user device must have its keep alive option set to *On*.
Invalid Mgmt Control Count	P	The number of times the DXI Level 2 PDU control field was invalid. The Level 2 PDU control field is a one-octet field that identifies the frame type – either UI (03) or Test (F3). When the switch receives a frame, the system checks the Level 2 PDU control field for a value of 03 (indicating a UI frame type). If the control field value is not 03, the Poll Final (P/F) bit is set and the system checks for a value of F3 (indicating a Test frame type). If a value of F3 is found, the frame is sent. If neither an 03 nor F3 value is found, the Invalid Mgmt Control Count increments.
Invalid Mgmt Link ID Count	S	The number of times that the DXI Level 2 PDU link ID was invalid. The fourth bit of the Level 2 PDU link ID determines whether the packet is a management or data frame. A value of 0 indicates a data frame, and a 1 indicates a management frame (heartbeat poll). Any other value is invalid.
Invalid Mgmt Station ID Count	P	The number of times that the DXI Level 2 PDU station ID was invalid. This bit determines whether the packet is either destined for or originated from a Data Service Unit (DSU). A value of 1 indicates that the packet is destined for a DSU. A value of 0 indicates that the packet originated from a DSU. Any other value is invalid and the frame is dropped.
Invalid Reserve Field Count	P	The number of times that the SIP Level 3 PDU reserved field in the header was invalid. The reserved field is a one-byte field in the header that is populated with 0's. Any other value is invalid and points to a corrupted frame, and the possibility of a bad line.
Invalid SA count	U	Not used.

Table 10-3. SMDS Logical Port Summary Statistics (Continued)

Statistic	Type	Description
Invalid SA Type Count	P	The number of times that the source address (SA) type was invalid. The only valid SA prefix is *C*. The counter flags any other prefix.
Invalid Trailer Reserve Count	P	The number of times that the SIP Level 3 PDU reserved field in the trailer was invalid. The reserved field is a one-byte field that is populated with 0's. Any value other than 0 is considered invalid and the frame is dropped.
Logical Port Trans Util	M	A measurement of traffic queued for transmission on a logical port as a percentage of the logical port speed. It does not measure the amount of logical port bandwidth. Therefore, this value can exceed 100%.
Logical Port Rec Util	M	A measurement of traffic queued for reception on a logical port as a percentage of the logical port speed.
Mgmt Frame Size Error Count	S	The number of times that a DXI Level 2 PDU frame size error occurred. A frame must be greater than 2 bytes for management frames and 40 bytes for data frames. The counter flags any frames that are less than the specified minimum as errors. **Note:** *If protocol error checking is set to Off, and this counter is incrementing, the frames that are in error are data frames.*
SA DA on Same Port Error Count	S	The number of times that the Source Address (SA) and the Destination Address (DA) were on the same port. This is an invalid condition. Check the configuration.
SA Not Found Count	S	The number of times that the SA was not found. The counter increments whenever a PDU is received that does not have an E.164 address (SA) configured within the SMDS Access Server.
SA Validation Fail Count	S	The number of times that the SA validation failed. This counter increments whenever an Ascend switch receives a PDU with an E.164 address that exists within the SMDS Access Server, but is not assigned to the DXI/SNI logical port that received the PDU.
Source IA Screen Fail Count	S	The number of times that the source IA screen failed. Each time a user device transmits a packet through an Ascend switch, the packet is screened at the ingress and egress ports to verify that the packet's source IA is authorized for a particular end-user port.
Total Discard Frame Count	M	The total number of frames discarded since the last reset.

Viewing SMDS PDU Statistics

To view SMDS PDU statistics, choose Diagnose SMDS PDU from the SMDS Logical Port Statistics dialog box shown in Figure 10-1 on page 10-3. The system displays the Diagnose SMDS PDU dialog box (see Figure 10-2).

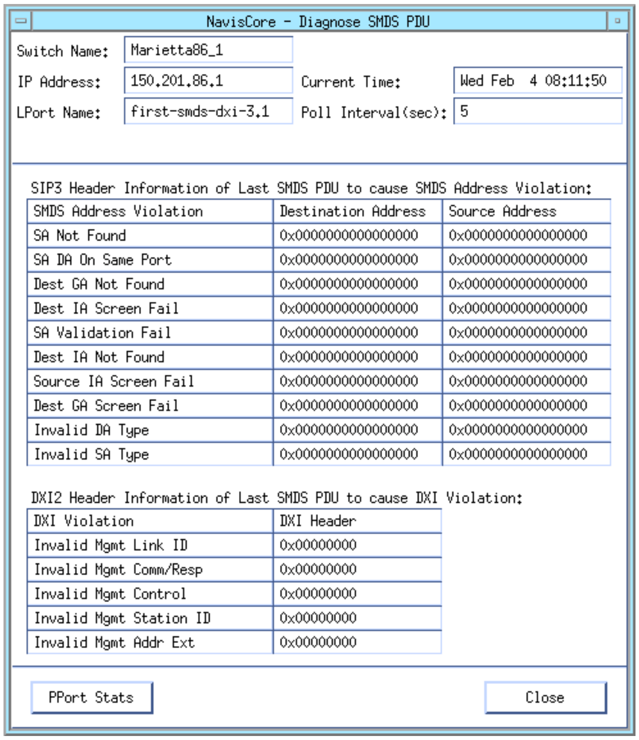


Figure 10-2. Diagnose SMDS PDU Dialog Box

Table 10-4 describes each of the statistics shown in Figure 10-2. See Table 10-3 on page 10-5 for additional information about these fields.

Table 10-4. SMDS PDU Diagnostic Statistics

Statistic	Description
SMDS Address Violations	
SA Not Found	The SA that cannot be found. This condition occurs whenever a Protocol Data Unit (PDU) is received with an E.164 address that is not configured within the SMDS Access Server.
SA DA On Same Port	The SA and the Destination Address (DA) that are on the same port. This is an invalid condition. Check the configuration.
Dest GA Not Found	The destination group address (GA) that could not be found because the switch configuration did not specify the destination GA.

Table 10-4. SMDS PDU Diagnostic Statistics (Continued)

Statistic	Description
Dest IA Screen Fail	The destination individual address (IA) that failed screening. Each time a user device transmits a packet through an Ascend switch, it is screened at the ingress port. This screening verifies that the packet's source destination IA is authorized for a particular end-user port. The destination IA field is screened upon ingress to check whether or not the destination is authorized to communicate with the source.
SA Validation Fail	The SA that could not be validated. SA validation fails whenever an Ascend switch receives a PDU with an E.164 address that exists within the SMDS Access Server, but is not assigned to the DXI/SNI logical port that receives the PDU.
Dest IA Not Found	The destination IA was not found because the switch configuration did not specify the Destination IA.
Source IA Screen Fail	The source IA that failed screening. Each time a user device transmits a packet through an Ascend switch, the packet is screened at the ingress and egress ports. Egress port screening verifies that the packet's Source IA is authorized for a particular end-user port.
Dest GA Screen Fail	The destination GA that failed screening. Each time a user device transmits a packet through an Ascend switch, it is screened at the ingress port. The destination GA is screened upon ingress to check whether or not the destination is authorized to communicate with the source.
Invalid DA Type	The value of the SMDS Interface Protocol (SIP) Level 3 PDU Destination Address. Valid E.164 addresses start with either an *E* or a *C* prefix, as follows: • An *E* indicates a group address. • A *C* indicates an individual address. Any other prefix type is invalid.
Invalid SA Type	The value of the SA type. The only valid SA prefix is *C*. The counter flags any other prefix.
DXI Violation	
Invalid Mgmt Link ID	The value for the DXI Level 2 PDU link ID. The fourth bit of the Level 2 PDU link ID determines whether the packet is a management or data frame. A value of 0 indicates a data frame, 1 indicates a management frame (heartbeat poll).
Invalid Mgmt Comm/Resp	The value for the DXI Level 2 PDU command/response field. The value in this field is invalid if the Ascend switch cannot communicate with the user device if the user device is out-of-service.

Table 10-4. SMDS PDU Diagnostic Statistics (Continued)

Statistic	Description
Invalid Mgmt Control	The value for the DXI Level 2 PDU control field. The Level 2 PDU control field is a one-octet field that identifies the frame type – either UI (03) or Test (F3). When the switch receives a frame, the system checks the Level 2 PDU control field for a value of 03 (UI frame). If a value of 03 is not found, the Poll Final (P/F) bit is set and the system checks for a value of F3 (Test frame). If a value of F3 is found, the frame is sent. If neither an 03 nor F3 value is found, the Invalid Mgmt Control Count increments.
Invalid Mgmt Station ID	The value for the DXI Level 2 PDU station ID. This bit determines whether the packet is either destined for or originated from a Data Service Unit (DSU). A value of 1 indicates that the packet is destined for a DSU; a value of 0 indicates that the packet originated from a DSU. Any other value is invalid and the frame is dropped.
Invalid Mgmt Addr Ext	The value of the DXI Level 2 PDU Address Extension (AE) field. The AE bit is the least significant bit (LSB) of the DXI frame and is set to 1. If the AE bit value is 0, the packet is dropped. Possible causes of this condition are: 1. Incorrectly configured router(s). 2. AE bit (being the LSB) corrupted by either the line or user device (including an Ascend user device).

Viewing SMDS Management Address Status

The Show All SMDS Management Address dialog box enables you to view the SMDS in-band management address connections defined for a switch network. An SMDS in-band management address allows the NMS to connect remotely to the Ascend network using SMDS services to transport the SNMP/UDP/IP protocol packets. For more information about how to configure an SMDS management address, see the *NavisCore SMDS Configuration Guide.*

To view all configured SMDS management addresses:

1. From the Monitor menu, select Ascend Objects ⇒ Show All Management Addresses. The Show All SMDS Management Address dialog box appears (see Figure 10-3).

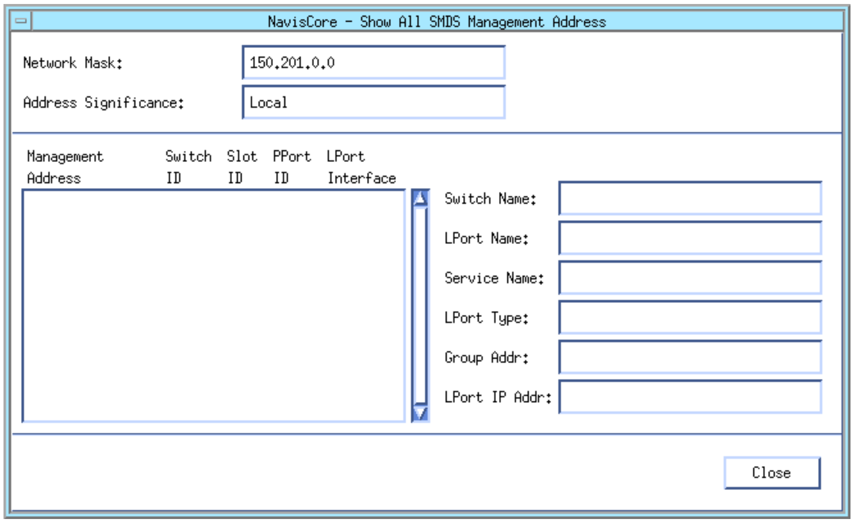


Figure 10-3. Show All SMDS Management Address Dialog Box

Table 10-5 describes the fields in the dialog box.

Table 10-5. Show All SMDS Management Addresses Fields

Field	Displays...
Network Mask	The Internet switch IP network number that was specified at the time of installation.
Address Significance	The default, Local (that is, local significance).
Management Address	The in-band management address for this connection. If the LPort Type is SSI, the system displays the management address. If the LPort Type is DXI/SNI, the system displays the individual address to which the logical port subscribes.
Switch ID	The switch ID associated with this management address.
Slot ID	The back panel physical slot number where the I/O module that contains the selected logical port is installed.
PPort ID	The physical port number on which this logical port resides.
LPort Interface	The logical port interface number.
Switch Name	The name of the switch associated with this connection.
LPort Name	The name of the logical port associated with this connection.
Service Name	SMDS service type.
LPort Type	The type of logical port configuration.
Group Addr	If applicable, the group address to which the logical port subscribes.
LPort IP Addr	The IP address of the selected logical port.

Viewing SMDS Route Status

For a summary of SMDS routes in the network, you can display the following:

- All of the destination switches
- Whether a route is defined
- The hop count for each route

To view all SMDS routes:

1. From the Monitor menu, select Ascend Objects ⇒ Show Smds Routes. The Show SMDS Routes dialog box appears, displaying a list of destination switch names along with a hop count if a route is defined (see Figure 10-4).

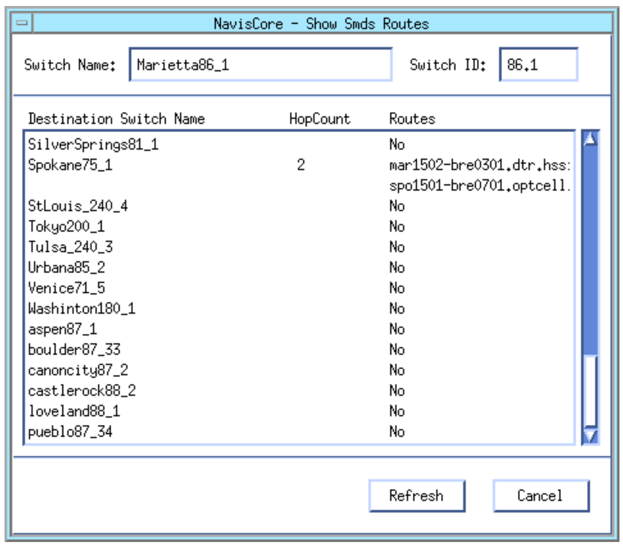


Figure 10-4. Show SMDS Routes Dialog Box

2. Choose Refresh to update the display.
3. Choose Cancel when you finish reviewing the information.

Table 10-6 describes the Show SMDS Routes dialog box fields.

Table 10-6. Show SMDS Routes Fields

Field	Displays...
Switch Name	The name of the currently selected switch.
Switch ID	The ID for the selected switch.
Destination Switch Name	A list of all configured destination switches.
HopCount	The hop count between the current switch and the corresponding destination switch.
Routes	The destination SMDS logical port name for the route. The field displays *No* if no route is defined.

Disabling the SMDS Switching System

When you need to isolate problems in the network, consider disabling the SMDS switching system. To disable the SMDS switching system for the entire Ascend network:

1. Edit the /opt/CascadeView/etc/CascadeView.cfg file using a text editor (e.g., VI or EMACS).
2. Change the CV_DISABLE_SMDS_SS value from 0 (enabled) to 1 (disabled).
3. Set the IA and GA mask size parameters to 0. See the *NavisCore SMDS Configuration Guide* for details.
4. For each B-STDX switch that runs SMDS in the network, synchronize the PRAM on the CP processor module. For instructions on how to do this, see the *NavisCore NMS Getting Started Guide*.
5. Cold boot the desired B-STDX switches.

11

Monitoring ISDN

This chapter provides information on monitoring and troubleshooting ISDN remote access activities and events in your Ascend network. This chapter describes the following:

- Monitoring ISDN call status, physical ports, logical ports, and Multilink PPP
- Reviewing diagnostic traps for ISDN remote access
- Running console-based call lookup of port statistics

Viewing ISDN Call Status

The switch software and NavisCore provide call monitoring support for ISDN PRI dial-in connections through the Show ISDN Status dialog box. This section describes:

- How to open the Show ISDN Status dialog box
- The information in the Show ISDN Status dialog box

Opening the Show ISDN Status Dialog Box

To open the Show ISDN Status dialog box:

1. On the network map, select the switch object that you want to monitor.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail.

The Switch Back Panel dialog box appears (see Figure 11-1).

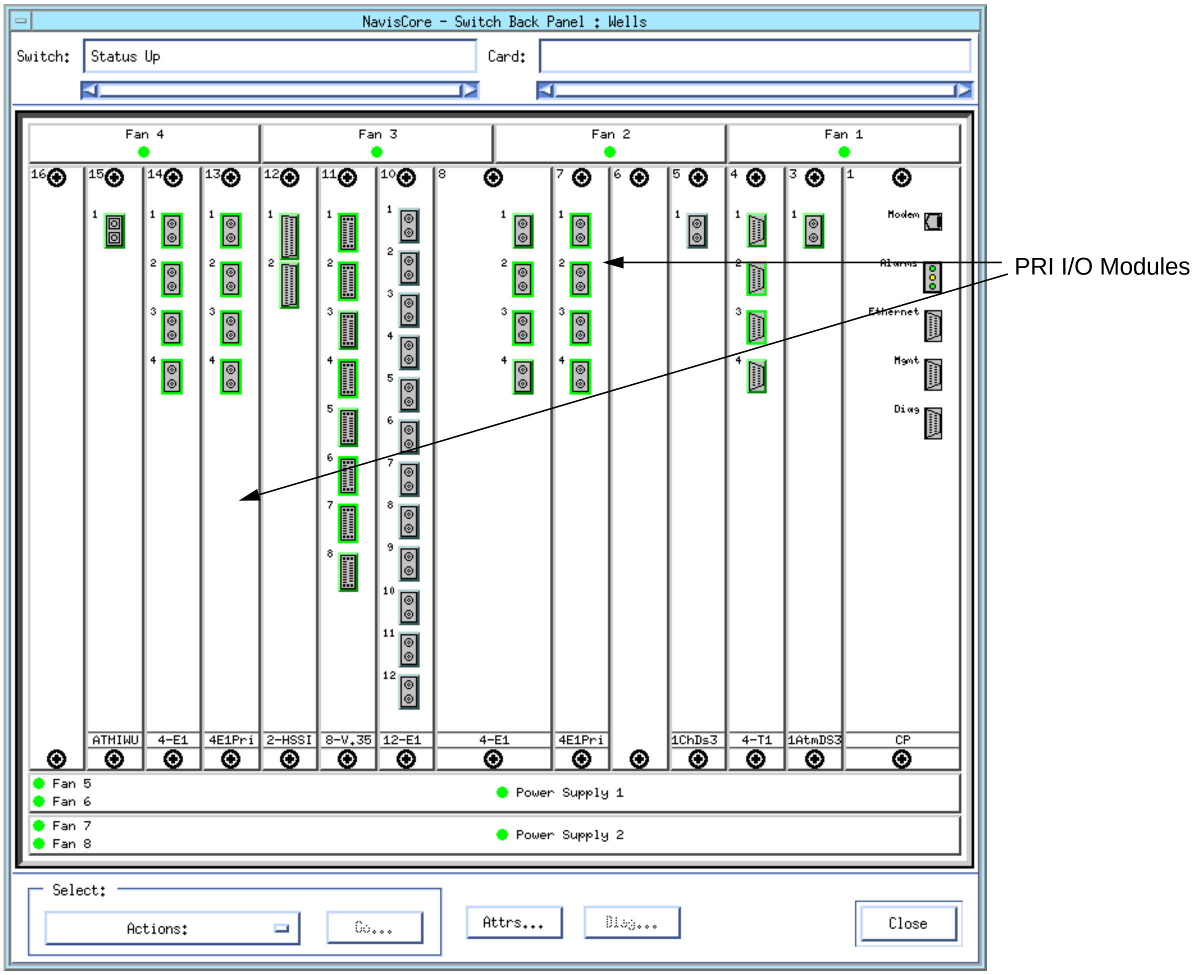


Figure 11-1. Switch Back Panel Dialog Box

3. Select the PRI I/O module that you want to monitor.

4. Select Actions ⇒ ISDN Status.

5. Choose Go. The Show ISDN Status dialog box appears (see Figure 11-2).

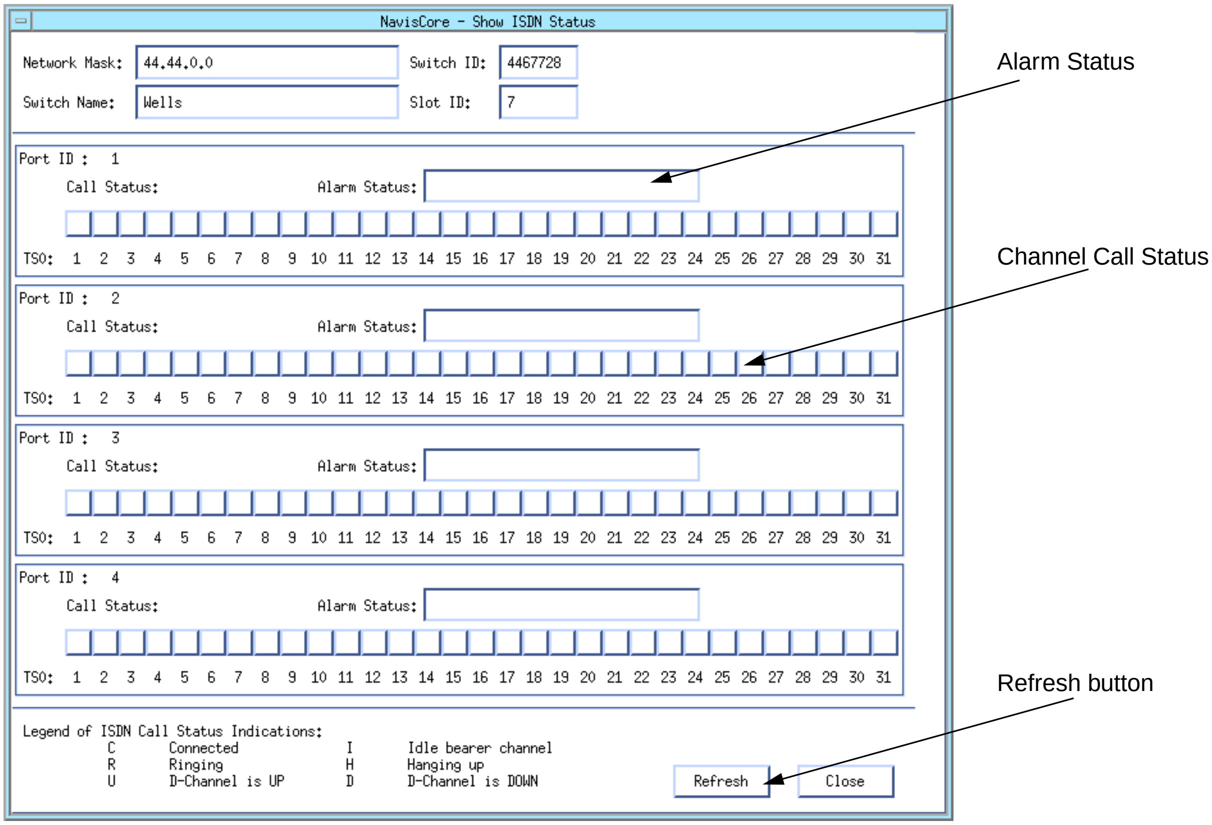


Figure 11-2. Show ISDN Status Dialog Box

Viewing ISDN Status Dialog Box Contents

The Show ISDN Status dialog box presents a graphical representation of B- and D-channels for each PRI port on the I/O module. The dialog box describes any alarms on the physical ports and includes the call status of each channel.

Viewing Alarm Status

The Show ISDN Status dialog box describes any alarms that are present on each PRI port (see Figure 11-2 on page 11-3). Table 11-1 describes those alarms.

Table 11-1. PRI Port Alarm Status Summary

Status	Description
Red	Loss of signal or out-of-frame error. This is due to either two or more framing-bit errors within a three millisecond period or two or more errors within five or less consecutive framing bits.
Yellow	A remote channel service unit (CSU) is transmitting a red alarm. The remote CSU is not receiving any transmission signals from the circuit therefor, the circuit is acting as a one-way link.
None	No alarm condition.

Viewing Channel Call Status

Each of the B- and D-channels reported in the Show ISDN Status dialog box can contain a single-character code representing the channel's call status (see Figure 11-2 on page 11-3). You can display the most current status information by choosing Refresh at the bottom of the dialog box. Table 11-2 describes each of the ISDN Call Status codes.

Table 11-2. ISDN Call Status Codes

Code	Description
C	The B-channel is connected (active).
D	The D-channel is down.
H	The B-channel is releasing the call (hanging up).
I	The B-channel is idle.
R	The B-channel is dialing (ringing).
U	The D-channel is up.

Viewing ISDN Physical Ports

You monitor physical port activity on ISDN PRI I/O modules in the same way that you monitor physical port activity for other services. See "Reviewing Physical Port Status" on page 2-44 for information on viewing physical port status and attributes. See "Viewing Physical Port Summary Statistics" on page 3-2 for information on viewing physical port statistics.

Viewing ISDN Logical Ports

There are two types of ISDN logical ports:

- D-channels for carrying management traffic
- B-channels for carrying data

There is one D-channel logical port for each ISDN physical port. There is one B-channel logical port for each B-channel that uses an ISDN physical port. For example, if 10 B-channels use the physical port, then you configure 10 B-channel logical ports.

The next two sections describe how to display attributes and statistics for these logical ports.

Viewing ISDN Logical Port Attributes

To view ISDN logical port attributes:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 11-1).
3. Select the physical port on the PRI I/O module that is associated with the logical port that you want to monitor. The View Physical Port Attributes dialog box appears for the selected physical port.
4. Choose Logical Port. The Show All Logical Ports in PPort dialog box appears.
5. Select the logical port you want to monitor.
6. Use the View Attributes option menu to display the following types of attributes:
   - Administrative
   - Authentication (B-channel ports that support RADIUS authentication only)
   - ISDN (B-channel ports only)
   - Trap control

See the *NavisCore ISDN Configuration Guide* for descriptions of these attributes.

Viewing ISDN Logical Port Statistics

To view logical port statistics:

1. On the network map, select the switch from which you want to obtain ISDN logical port statistics.
2. From the Monitor menu, select Ascend Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (see Figure 11-1).
3. Select the PRI I/O module physical port on which the logical port that you want to monitor resides. The View Physical Port Attributes dialog box appears for the selected physical port.
4. Choose Logical Port. The Show All Logical Ports in PPort dialog box appears.
5. Select the logical port you want to monitor.
6. Select Options ⇒ Statistics.
7. Choose View. The Logical Port Summary Statistics dialog box appears.

The statistics that appear are similar to Frame Relay logical port summary statistics. See “Viewing Frame Relay Logical Port Summary Statistics” on page 9-14 for more information.

In addition, B-channel logical ports display the statistics described in Table 11-3.

Table 11-3. ISDN B-Channel Logical Port Summary Statistics

Statistic	Description
ISDN B-Channel Source Address	The E.164 address of the source of this ISDN connection.
ISDN B-Channel Destination Address	The E.164 address of the destination of this ISDN connection.
ISDN B-Channel Client IP Address	The IP address of the client connected to this B-channel.
ISDN Call Duration	The number of seconds that the ISDN call has been established.
ISDN B-Channel Pool Utilization	The percentage of the B-channel pool that the selected B-channel is using.

Viewing Multilink PPP Information

Multilink Point-to-Point Protocol (PPP) is a method for splitting, recombining, and sequencing datagrams across multiple logical data links. The logical link is referred to as an *MP bundle*.

Several logical port and PVC components make up a multilink PPP data link. These components are:

- A B-channel logical port with PPP options configured.
- Two PPP-to-1490 logical ports.
- An ATM or Frame Relay internetworking logical port.
- PVCs that connect the PPP-to-1490 logical ports and the ATM/Frame Relay logical port.

You view information about these logical ports and PVCs the same way that you view information for all logical ports and PVCs. See the *NavisCore ISDN Configuration Guide* for more information.

Viewing Diagnostic Traps for ISDN Remote Access

On the switches that are configured to report to the NMS, diagnostic traps notify the operator of events taking place. You can view a list of currently logged trap alarm conditions by selecting the Ascend Events option from the Event Categories window. See Chapter 15, “Managing Traps,” for more information about accessing these traps.

This section describes three types of traps for ISDN remote access:

- Failed authentication attempt traps
- ISDN call rejected traps
- PPP negotiation failed traps

Failed Authentication Attempt Traps

The switch generates a trap for all failed authentication attempts. Table 11-4 contains a description of each of these traps.

Table 11-4. Failed Authentication Attempt Traps

Trap	Condition
No Response from Server	RADIUS server is unreachable.
Protocol Error	Invalid response packet received from RADIUS server.
Invalid Service-Type Attribute	The Service-Type in the RADIUS Users file is not set to “Framed.”
Invalid Framed-Protocol Attribute	The Framed-Protocol in the RADIUS Users file is not set to “PPP.”
Server Authentication Failed	Invalid username, password, slot ID, or IP address.

ISDN Call Rejected Diagnostic Traps

The switch generates a trap for each rejected call. All ISDN rejected call traps have the format:

```
An ISDN call has been rejected on logical port number due to
<trap name>.
```

Table 11-5 contains a description of each of the possible traps.

Table 11-5. Descriptions for Rejected ISDN Calls

Trap	Condition
Unassigned number	The destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned.
No route to specified transit network	The equipment sending this cause code has received a request to route the call through a particular transit network that it does not recognize. Either the transit network does not exist or the network does exist but does not serve the equipment that is sending this error.
Channel unacceptable	The channel most recently identified is not acceptable to the sending equipment for use in this call.
Normal call clearing	One of the users involved in the call has cleared it.
User busy	The called user is unable to accept another call. The user equipment is compatible with the call.
No user responding	The called user does not respond to a call establishment message with either an alerting or connect indication within the time period configured for timer T303 or T310 (defined in ITU Recommendation Q.931).
Call rejected	The equipment sending this code does not accept this call, although it could have accepted the call because the equipment sending this cause code is neither busy nor incompatible.
Number changed	The called number is no longer assigned. The new called number may be included in the diagnostic field. If a network does not support this capability, the “Unassigned number” trap is returned.
Destination out of order	The destination indicated by the user cannot be reached because its interface is not delivering a signaling message to the remote user. For example, this trap is generated when the remote user has a physical layer or data link layer failure or when user equipment is off-line.
Invalid number format	The called user cannot be reached because the called party number is not in a valid format or is not complete.
Facility rejected	The network cannot provide a facility requested by the user.

Table 11-5. Descriptions for Rejected ISDN Calls (Continued)

Trap	Condition
Response to STATUS ENQUIRY	A STATUS message was generated in response to a STATUS ENQUIRY message (trap text is included in the message).
Unspecified cause	A normal event has occurred and no other cause in the normal class applies.
No circuit available	An appropriate circuit is not presently available to handle the call.
Network out of order	The network is not functioning correctly, but the condition is likely to last a relatively long time (i.e., immediately reattempting the call is not likely to be successful).
Temporary failure	The network is not functioning correctly, but the condition is not likely to last a long time (i.e., immediately reattempting the call may be successful).
Network congestion	The switch is experiencing heavy traffic volume.
Access information discarded	The network cannot deliver requested access information such as user-to-user information, low-layer compatibility, high-layer compatibility, or sub-address as indicated in the diagnostic.
Requested circuit not available	The circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.
Requested facility not subscribed	The network cannot provide the requested supplementary service because the user has not completed the necessary administrative arrangements with its supporting networks.
Bearer capability not available	The user has requested a bearer capability that is implemented by the equipment that generated this cause but is not available at this time.
Service not available	A service not available event has occurred and no other cause in the *service not available* class applies.
Capability not implemented	The equipment sending this cause does not support the bearer capability requested.
Channel type not implemented	The equipment sending this cause does not support the channel type requested.
Requested facility not implemented	The equipment sending this cause does not support the requested supplementary service.
Invalid call reference value	The equipment sending this cause has received a message with a call reference that is not currently in use on the user-to-network interface.
Identified channel does not exist	The equipment sending this cause has received a request to use a channel not activated on the interface. For example, this cause is generated if channels 1 to 12 are configured but the user equipment on the network attempts to use channels 13 through 23.

Table 11-5. Descriptions for Rejected ISDN Calls (Continued)

Trap	Condition
Incompatible destination	The equipment sending this cause has received a request to establish a call that has low layer compatibility, high-layer compatibility, or other compatibility attributes (e.g., data rate) that cannot be accommodated.
Invalid message	An invalid message event has occurred and no other cause in the *invalid message* class applies.
Mandatory information element is missing	The equipment sending this cause has received a message that is missing an information element that must be present before that message can be processed.
Message type non-existent	The equipment sending this cause has received a message with a message type it does not recognize (i.e., the message type either is not defined or is defined but not implemented).
Message not compatible	The equipment sending this cause has either received a message incompatible with the call state, or has received a STATUS message indicating an incompatible call state.
Information element non-existent	The equipment sending this cause has received a message that includes information elements not recognized (i.e., the information element identifier is either not present or not defined, or is defined but not implemented).
Invalid information element contents	The equipment sending this cause has received an information element that it has implemented; however, one or more of the fields in the information element are coded in a way that has not been implemented by the equipment sending this cause.
Timer expired	The Q.931 timer has expired causing Q.931 error handling procedures to be initiated.
Protocol error	A protocol error event has occurred and no other cause in the *protocol error* class applies.
Interworking unspecified	Contact is being made with a network that does not provide causes for actions it takes; the precise cause for a message that is being sent cannot be ascertained.

PPP Negotiation Failed Diagnostic Traps

The switch generates one of the following traps if PPP negotiation fails:

```
PPP negotiation has failed on logical port <number> due to IP
Control Protocol failure.
```

```
PPP negotiation has failed on logical port <number> due to
Link Control Protocol failure.
```

```
PPP negotiation has failed on logical port <number> due to
PVC down.
```

Console-based Call Lookup of Port Statistics

Console-based call lookup provides a way to diagnose a problem with an ISDN remote access connection to the B-STDX 8000/9000 switch. Call lookup displays the port statistics on the console.

Viewing Port Statistics

To view port statistics:

1. Access the console port on the switch either directly or through a telnet session.
2. Issue the following command:

   ```
   show isdn call <telephone number of caller>
   ```

   Example:

   ```
   show isdn call 5089521234
   ```

   The console displays port statistics for the remote access session. Table 11-6 describes the port statistics displayed on the console.

Table 11-6. Remote Access Session Port Statistics

Statistic	Description
Calling #	The telephone number of the remote access user making the call.
Slot #	The slot number of the 4-port T1 or E1 ISDN I/O module receiving the call.
Pport #	The number of the physical port located on the ISDN I/O module.
Lport #	The number of the logical port (or ISDN channel) handling the call.
Ifnum	The interface number of the logical port where the call is attached.
Called #	The telephone number assigned to the Lport.
IP address	The IP address of the B-STDX 8000/9000 remote access switch.

12

Monitoring Trunks

This chapter describes how to monitor trunks for a specified switch. In an Ascend network, a trunk is a permanent link between logical port endpoints on two separate Ascend switches. A trunk represents a permanent link from one Ascend switch to another Ascend switch for the purpose of transporting user traffic, routing updates, network management pools, and other management traffic.

Ascend supports several types of trunks, including:

ATM Direct Line — A dedicated line between the switches. Data is transferred using ATM protocols.

ATM OPTimum Cell/Frame — A connection between the switches through a switched Public Data Network (PDN). Data is transferred using ATM protocols.

Frame Relay Direct Line — A dedicated line between the switches. Data is transferred using Frame Relay protocols.

Frame Relay OPTimum PVC — A connection between the switches through a switched Public Data Network (PDN). Data is transferred using Frame Relay protocols.

Multilink Frame Relay (MLFR) — A connection, similar in some ways to a Frame Relay Direct Line trunk, that combines up to 32 separate Frame Relay trunks into a single, aggregate Frame Relay trunk. The aggregate trunk is called a *bundle*; the individual trunks that make up the bundle are called *members*. Each bundle is configured as a logical port, and each member is also configured as a logical port.

SMDS OPTimum — A connection between the switches through an SMDS network.

Viewing the Trunk Status

To view trunks:

1. From the Monitor menu, select Ascend Objects ⇒ Show Trunks, and select one of the following options:

All on Map — Displays a list of all the trunks configured for the current map.

All on Switch — Displays a list of all the trunks configured for a selected switch.

After you select an option, the Show All Trunks dialog box appears (see Figure 12-1).

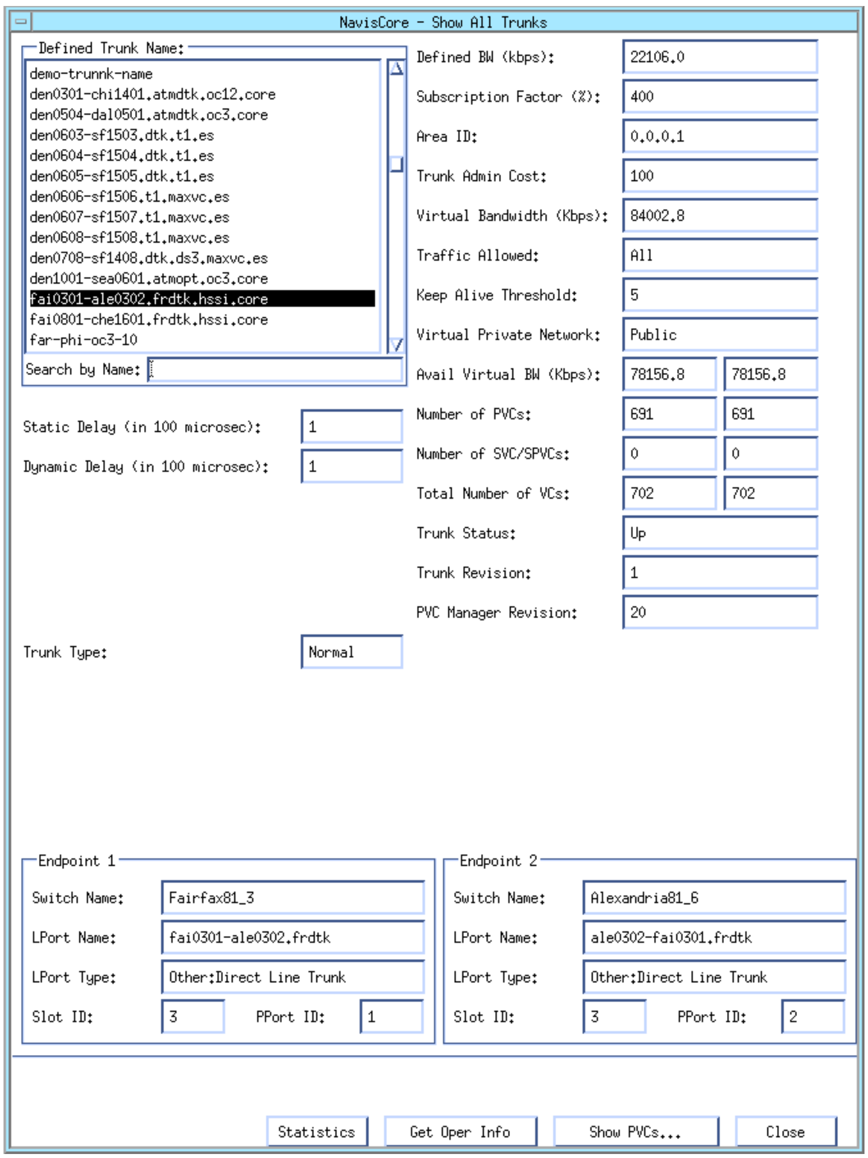


Figure 12-1. Show All Trunks Dialog Box

> If the trunk names do not appear immediately in the Defined Trunk Name list box, insert the cursor in the blank Search by Name field and press Return. This action will display a list of configured trunk names.

2. In the Defined Trunk Names list box, select the trunk from which you want to retrieve status information. You can use the Search by Name field to enter wild-card characters.

- Use an * to match any number of characters
- Use a ? to match a single character
- Type ***** to match the * character
- Type \? to match the ? character
- Type \\ to match the \ character

Table 12-1 describes the Show All Trunks dialog box buttons and Table 12-2 describes the Show All Trunks dialog box fields.

Table 12-1. Show All Trunks Dialog Box Buttons

Button	Function
View QoS Parameters	Displays the Show Logical Port Dos Parameters dialog box for the logical ports at both ends of the selected trunk. This button appears for ATM direct and OPTimum cell trunks only. See "Viewing QoS Parameters for ATM Trunks" on page 12-18.
Statistics	Displays the summary statistics for the selected trunk. See "Viewing Trunk Summary Statistics" on page 12-12.
Get Oper Info	Displays the status of the selected trunk.
Show PVCs	Displays a list of PVCs that are currently using the trunk. See "Viewing PVC Usage" on page 12-21.
Close	Exits the Show All Trunks dialog box.

Table 12-2. Show All Trunks Fields

Field	Services	Trunk Type(s)	Displays...
Defined Trunk Name	All	All	The names of the trunks configured for the current network map.
Defined BW (Kbps)	All	All Except MLFR	The bandwidth in Kbps for the selected trunk line.
Aggregate BW (Kbps)	Frame Relay	MLFR Only	The aggregate bandwidth in Kbps of all the MLFR member logical ports. For MLFR ports, this field appears in place of “Defined BW”.
Subscription Factor (%)	All Except ATM	All	The percentage used to calculate the available virtual bandwidth for the selected trunk. Because Ascend allocates the bandwidth of the committed information rate (CIR) when you configure the circuit, this K factor enables you to oversubscribe the trunk so that you can configure even more circuits. For example, you can set this factor to 200% to produce a virtual bandwidth that is two times greater than the defined bandwidth.
Area ID	All	All	The ID of the OSPF area to which the trunk belongs.
Trunk Admin Cost	All	All	A value that defines the cost of using this trunk for a virtual circuit when a virtual circuit is being dynamically created on the switch.
Virtual Bandwidth (Kbps)	All Except ATM	All	The result of the calculation: Defined Bandwidth * Trunk Over Subscription Factor% * .95 The value .95 is used because .05% of the bandwidth is reserved for management traffic.

Table 12-2. Show All Trunks Fields (Continued)

Field	Services	Trunk Type(s)	Displays...
Traffic Allowed	All	All	The type of traffic allowed on this trunk. Options include: *All* – Trunk can carry SVC, PVC, and network management traffic. *Mgmt Only* – Trunk can carry only network management traffic, such as SNMP communication between a switch and the NMS. *Mgmt & Address Restricted* – Trunk can carry PVCs and network management traffic. This trunk does not support SVC addressing information. If this is the only trunk between two nodes, and these nodes cannot pass addressing information over other network trunks, this mode effectively prevents SVCs from traversing this trunk. *Private* – Trunk is reserved for a VPN.
Keep Alive Threshold	All	All	The number of seconds the trunk protocol will continue to exchange Keep Alive (KA) control frames without getting a response from the remote node, before bringing the trunk down.
Virtual Private Network	All	All	The virtual private network (VPN) name, if the trunk is part of a VPN. Otherwise, this field displays *Public*.
Avail Virtual BW (Kbps) [a]	All Except ATM	All	The amount of bandwidth, in Kbps, available for circuit configuration and allotment on the selected trunk at each logical port endpoint. Each configured circuit that traverses the selected trunk decrements this value by its CIR. This allocation only occurs at circuit initialization. If a trunk fails in the network and you must reroute the circuits, this checking does not occur.
[a] A negative value in the Avail Virtual BW fields indicates that a trunk has gone down. When a trunk goes down, the system reroutes the circuits that were routed over the bad trunk and, if necessary, may use more than the available virtual bandwidth on trunks that are operational. This condition may cause certain trunks to have a negative available virtual bandwidth.			
Number of PVCs	All	All	The total number of PVCs (every type of PVC, including management PVCs) that traverse each trunk logical port endpoint.
Number of SVC/SPVCs	All	All	The total number of SVCs/SPVCs that traverse each trunk logical port endpoint.

Table 12-2. Show All Trunks Fields (Continued)

Field	Services	Trunk Type(s)	Displays...
Total Number of VCs	All	All	The total number of virtual circuits (PVCs, SVC/SPVCs, MPTs, management circuits) that are traversing the trunk at each logical port endpoint. You may notice a discrepancy between the total number of VCs and the number of PVCs. For example, as shown in Figure 12-1, suppose that the Number of PVCs field displays 691, the number of SVC/SPVCs field displays 0, and the Total Number of VCs field displays 702. MPTs could account for the 11-VC difference between the number of PVCs and the total number of VCs.
Trunk Status	All	All	The current status of the selected trunk. Options include: *Unknown* – The NMS cannot communicate with one or both switch endpoints that make up this trunk. *Down* – The switches cannot establish a communication link. *Attempt* – A switch is attempting to contact another switch but has not yet received a response. *Init* – A one-way communication exists between the two switches. *Two-way* – A bi-directional communication exists between the two switches. *Exchange Start* – The two switches are about to exchange the network topology. *Exchange* – The two switches are exchanging network topology. *Loading* – The two switches are requesting the most recent link state information. *Backed-up* – A primary trunk exists and is ready for backup. *Up* – The trunk is up and operational between the two switches. *Defined* – A backup trunk is ready for backup.
Trunk Revision	All	All	The revision of link trunk protocol software at each endpoint.
PVC Manager Revision	All	All	The PVC manager software revision.

Table 12-2. Show All Trunks Fields (Continued)

Field	Services	Trunk Type(s)	Displays...
Static Delay (in 100 microsec)	All	All	*For Direct/OPTimum trunks*, a value that represents the measured one-way delay in 100 microseconds units. This measurement is taken when the trunk is initialized, and it is only updated when the trunk changes state from down to up. The static delay value is used in conjunction with the end-to-end delay routing metric to enable you to route circuits over trunks with the lowest end-to-end delay. *For trunks that support PNNI*, a value in microseconds that represents the configured static delay of the trunk. The cell transmission delay (CTD) that PNNI advertises is the sum of this value and the appropriate cell delay variation (CDV) that is taken from the provisioned Call Admission Control (CAC) objectives.
Dynamic Delay (in 100 microsec)	All	All	The measured one-way delay in 100 microseconds units. When a trunk comes up, the switch calculates the dynamic delay every second until the trunk goes down. To calculate the delay, the local switch sends a KA frame to the remote switch. When the remote switch replies, the local switch divides the round-trip delay time by two. The resulting delay value – the one-way delay value – becomes a sample for calculating the dynamic delay value. The switch then takes the most recent sample, adds it to the last 15 samples, and calculates the average of all 16 samples. This average becomes the value that appears in the Dynamic Delay field. ***Note:*** *Under most conditions, the dynamic delay value will match the static delay value. However, if some characteristics of the underlying transmission media for the trunk change such that the dynamic delay changes, this value may differ from the static delay.*

Table 12-2. Show All Trunks Fields (Continued)

Field	Services	Trunk Type(s)	Displays...
Trunk Type	All	All	One of the following: *Normal* is a common trunk. *Primary* indicates that the trunk has a backup for fault tolerance. *Backup* indicates that it is the backup trunk (when failure occurs on the primary trunk). Primary and backup trunks can be used to implement APS Trunk Backup. See “Viewing Physical Port Redundancy” on page 2-66 for more information.
Primary Trunk to be Backup	All	Primary, Backup	The trunk that is used as a primary trunk. A backup trunk exists for fault tolerance purposes in the event of a trunk failure.
Call setup retry interval (sec)	All	Primary, Backup	The lapse of time between each retry during a given retry cycle. The default is 15 seconds. For example, if your system performs 5 retries for each retry cycle and the wait between each retry cycle is 10 minutes, you may want to perform each retry at each 2-minute interval. Therefore, the Call Setup Retry Interval would be set at 120 seconds.
No. of retries/setup cycle	All	Primary, Backup	The number of retries that the system performs during a retry cycle. The default is 20 retries.
Retry cycle interval (min).	All	Primary, Backup	The lapse of time between retry cycles (in minutes). The default is 10 minutes.
Initiate Backup Call Setup	All	Backup	The name of the switch that performs the backup call setup for the trunk.
Backup on Trunk Failure	All	Primary, Backup	A value of *Enabled* to indicate that the primary trunk will be backed up automatically upon failure. *Disabled* specifies that the trunk backup option will not be used.
Trunk failure thresh. (sec)	All	Primary, Backup	The configured trunk failure threshold. The default value for this field is 5 seconds. If the primary trunk remains down for a period of time greater than this threshold, and the value for the Backup on Trunk Failure field is set to *Enabled*, the switch enters into a call setup retry cycle to enable the backup trunk(s).

Table 12-2. Show All Trunks Fields (Continued)

Field	Services	Trunk Type(s)	Displays...
Trunk restoration thresh. (sec)	All	Primary, Backup	The configured trunk restoration threshold. The purpose of this parameter is to prevent unnecessary losses in service that can happen if restoration is attempted on a primary trunk that is cycling between the up and down states, and not yet ready to carry traffic. The switch considers a primary trunk available for restoration if it remains in the link-up state for a minimum amount of time as defined by this threshold. The default value for this field is 15 seconds.
Switch Name	All	All	The name of the Ascend switch at each trunk endpoint.
LPort Name	All	All	The name of the logical port at each trunk endpoint.
Lport Type	All	All	The configured logical port type.
Slot ID	All	All	The number of the slot where the I/O module containing the selected port resides.
PPort ID	All	All	The physical port ID number on which the logical port is configured.

Viewing Trunks on the Map

If you configure more than one trunk between two switches, these trunks appear as a solid line between the switch object on the network map.

To view all of the trunk connections between two switches:

1. On the network map, double-click on the solid line between the switch object. A trunk submap window appears, similar to the example shown in Figure 12-2.

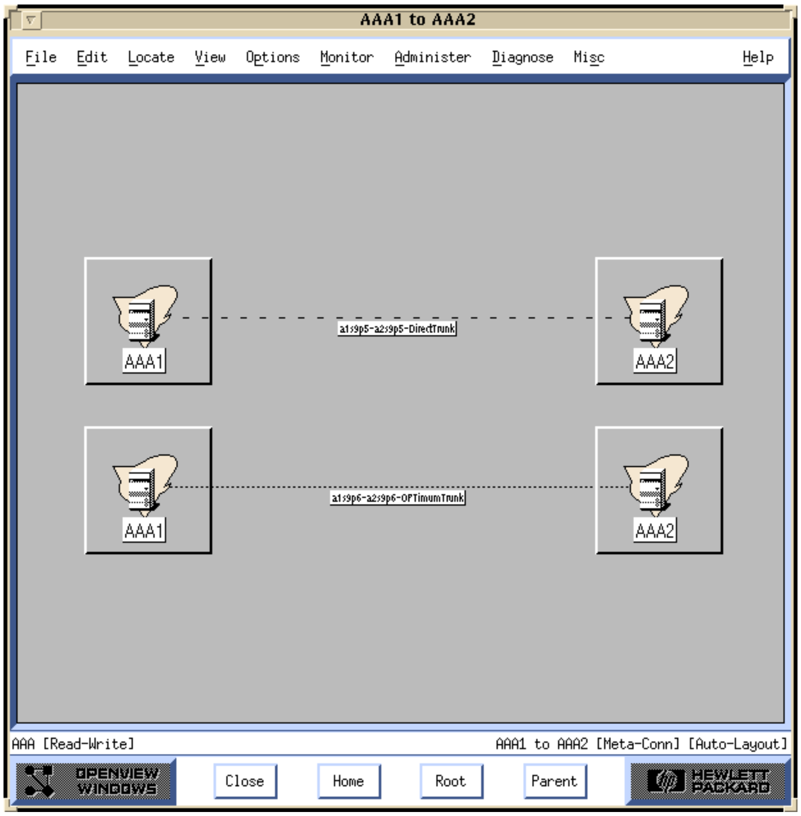


Figure 12-2. Displaying Multiple Trunks

2. Choose Close to exit this window and return to the network map.

Trunk Coloring

The trunk lines on the network map change color based on the polled status and the traps received by the Ascend Event Log. Table 12-3 describes the color scheme used to identify the status of a trunk connection on the network map.

Table 12-3. Trunk Color Status Indicators

Color	Status
Black	Either the line connection has not been defined as a trunk, or the environment variable $XUSERFILESEARCHPATH does not point to: `/opt/CascadeView/app-defaults.` [a]
Red	Trunk is down.
Blue	Trunk status is Unknown or Unmanaged.
Yellow	Trunk connection is coming up.
Green	Trunk connection is up.
Orange	Only one trunk connection out of many connections is up.
Cyan	More than one trunk connection is defined between the two endpoints. At least one trunk is up and one trunk is down.

[a] If the trunk-line graphic is black, set the following environment variable in .profile:

```
$ XUSERFILESEARCHPATH =/opt/CascadeView/app-defaults/%N
$ export XUSERFILESEARCHPATH
```

For more information about operational states and status, select Display Legend from the Help menu.

Viewing Trunk Summary Statistics

Trunk summary statistics enable you to view data that reflects the transmission and receipt of data from endpoint A to B and B to A. To view trunk statistics:

1. From the Monitor menu, select Ascend Objects ⇒ Show Trunks and select one of the following options:

   All on Map — Displays a list of all the trunks configured for the current map.

   All on Switch — Displays a list of all the trunks configured for a selected switch.

   The Show All Trunks dialog box appears (Figure 12-1 on page 12-2).

2. To view summary statistics for the selected trunk, choose Statistics. The Trunk Summary Statistics dialog box appears. Fields vary depending on the type of trunk. Figure 12-3 shows an example of ATM trunk statistics.

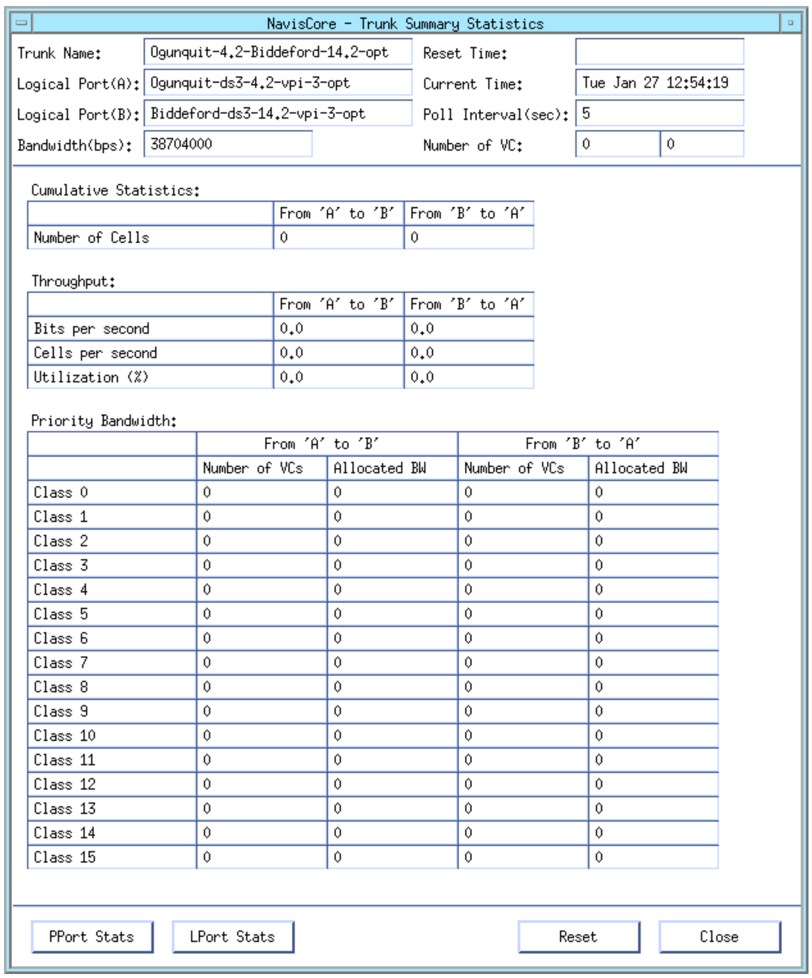


Figure 12-3. Trunk Summary Statistics Dialog Box (ATM Trunk)

Figure 12-4 shows an example of Frame Relay trunk statistics.

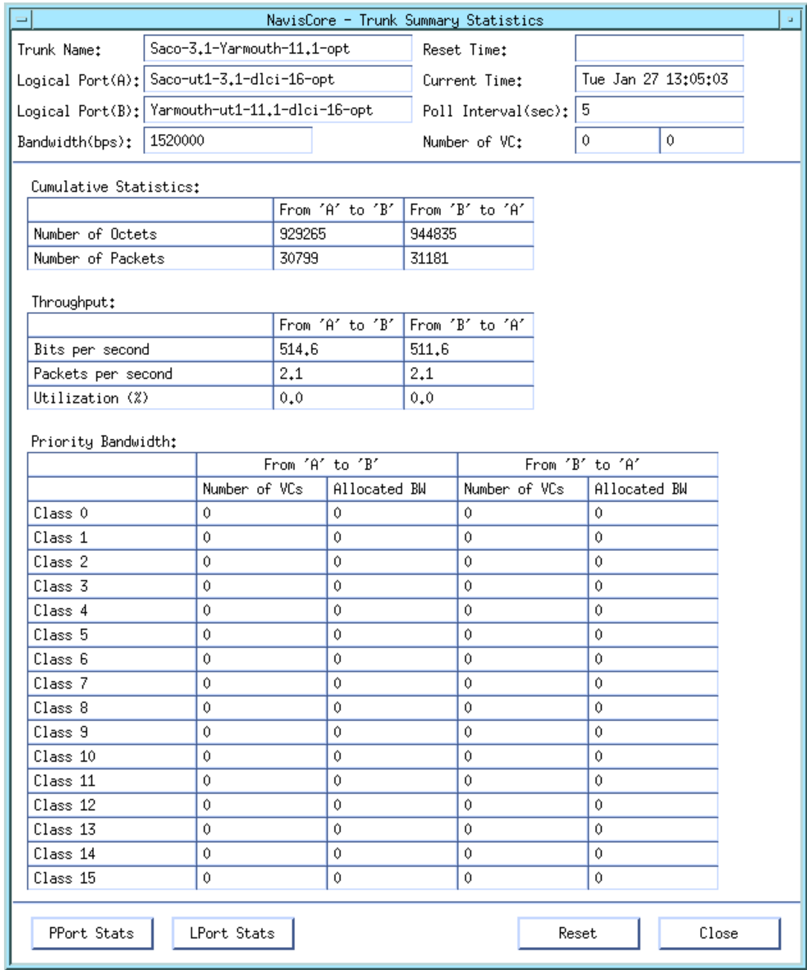


Figure 12-4. Trunk Summary Statistics Dialog Box (Frame Trunk)

Table 12-4 describes the Trunk Summary Statistics dialog box buttons.

Table 12-4. Trunk Summary Statistics Dialog Box Buttons

Button	Function
PPort Stats	Displays the physical port statistics for both ends of the trunk. See Chapter 3, "Generating Physical Port Statistics" for more information on physical port statistics.
LPort Stats	Displays the logical port statistics for both trunk endpoints. See either "Viewing ATM Logical Port Summary Statistics" on page 7-41 or "Viewing Frame Relay Logical Port Summary Statistics" on page 9-14 for more information.
MLFR PPort/LPort Stats	Displays physical port and logical port statistics for each MLFR member. See "Viewing MLFR Trunk Statistics" on page 12-15 for information.
Reset	Resets the displayed values to zero.

Table 12-5 describes the trunk summary statistics.

Table 12-5. Trunk Summary Statistics Fields

Statistic	Description
Trunk Name	The name that identifies the trunk.
Logical Port A	One endpoint of a trunk line connection.
Logical Port B	One endpoint of a trunk line connection.
Bandwidth (bps)	The physical port bandwidth configured for the selected logical ports at each endpoint. The bandwidth for each logical port endpoint must be the same.
Reset Time	The time of the last reset of the switch.
Current Time	The current system time.
Poll Interval (sec)	The time interval for the collection of statistical data. See "Setting the Polling Interval" on page 3-2 for details about how to set this value.
Number of VC	The number of VCs that the trunk supports.
Number of Octets (*Frame Trunks only*)	The total number of octets (bytes) received and transmitted since the last reset.
Number of Cells/Packets	The total number of cells/packets transmitted from one endpoint to the other.
Bits per second	The total number of bits per second (bps) transmitted from one endpoint to the other.
Cells/Packets per second	The total number of cells/packets per second (pps) transmitted from one endpoint to the other.
Utilization (%)	The percentage of trunk speed.
Priority Bandwidth (Class 0-15)	The bandwidth priority (0-15), where 0 is the highest priority and 15 is the lowest priority. In the event of network problems, the trunk will favor VCs assigned a lower bandwidth priority (e.g., 0) over VCs assigned a higher bandwidth priority (e.g., 15).
Number of VCs	The number of VCs in each priority bandwidth class.
Allocated BW	The amount of virtual bandwidth (in Kbps) allocated for each priority bandwidth class. Virtual bandwidth is bandwidth that is available for circuit configuration and allotment on the selected trunk.

Viewing MLFR Trunk Statistics

MLFR trunks differ from other trunks in that they are an aggregate of several trunks. You can view both aggregate statistics as well as statistics for the logical port members.

To view MLFR trunk statistics:

1. From the Monitor menu, select Ascend Objects ⇒ Show Trunks and select one of the following options:

   All on Map — Displays a list of all the trunks configured for the current map.

   All on Switch — Displays a list of all the trunks configured for a selected switch.

   The Show All Trunks dialog box appears (Figure 12-1 on page 12-2).

2. In the Defined Trunk Name list box, select the MLFR trunk from which you want to retrieve status information.

3. To view summary statistics, choose Statistics. The MLFR Trunk Summary Statistics dialog box appears.

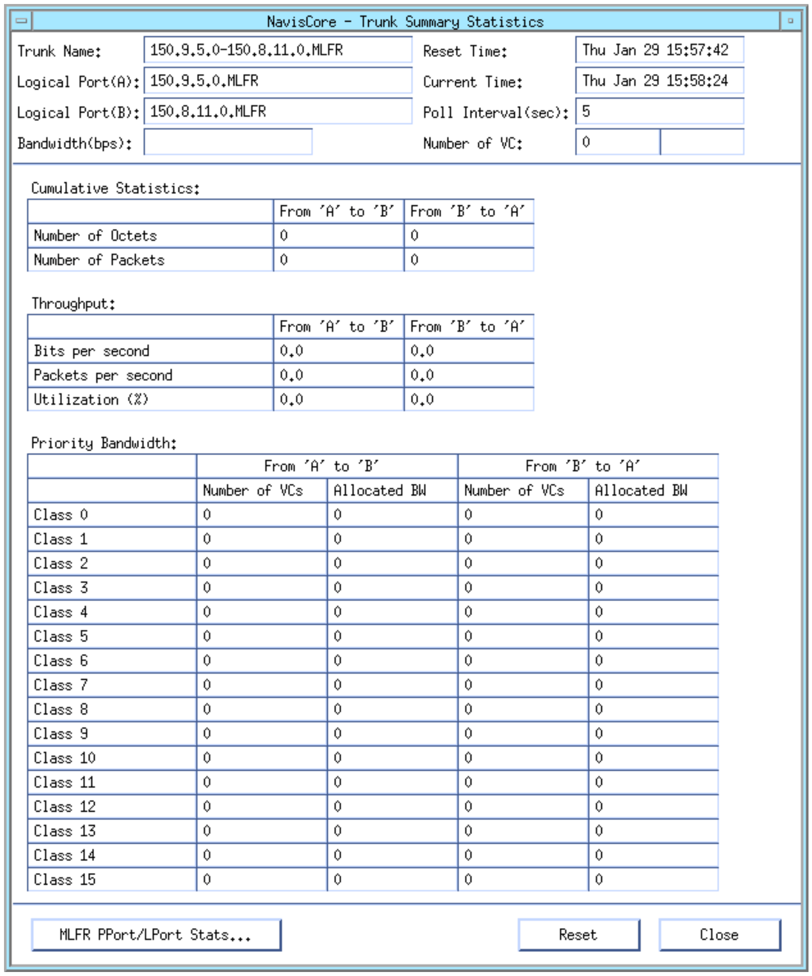


Figure 12-5. MLFR Trunk Summary Statistics Dialog Box

The MLFR trunk summary statistics are the same as those displayed for other Frame Relay-based trunks. However, keep in mind that the statistics reflect aggregate activity for all of the trunk's member logical ports. See Table 12-5 on page 12-14 for more information on trunk statistics.

4. To view statistics for the MLFR trunk members, choose MLFR PPort/LPort Stats. The Select Bound ML Member LPorts dialog box appears (see Figure 12-6).

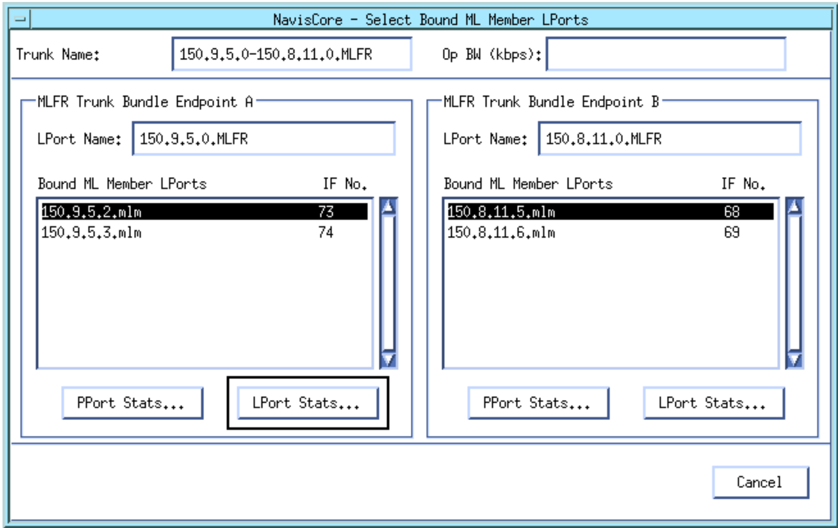


Figure 12-6. Select Bound ML Member LPorts Dialog Box

5. Select an MLFR member and do one of the following actions:

- Choose PPort Stats to view physical port statistics on the physical port associated with the member logical port. See Chapter 3, "Generating Physical Port Statistics" for more information on interpreting physical port statistics.
- Choose LPort Stats to view statistics on the member logical port. See "Viewing MLFR Logical Port Summary Statistics" on page 9-21 for more information on interpreting logical port statistics.

Viewing QoS Parameters for ATM Trunks

To view Quality of Service (QOS) parameters for ATM direct and OPTimum cell trunks:

1. From the Monitor menu, select Ascend Objects ⇒ Show Trunks and select one of the following options:

   All on Map — Displays a list of all the trunks configured for the current map.

   All on Switch — Displays a list of all the trunks configured for a selected switch.

   The Show All Trunks dialog box appears (Figure 12-1 on page 12-2).

2. Select the ATM direct or OPTimum trunk name from the Defined Trunk Name list box.

3. Choose View QoS Parameters. The Show Logical Port QoS Parameters dialog box appears (see Figure 12-7).

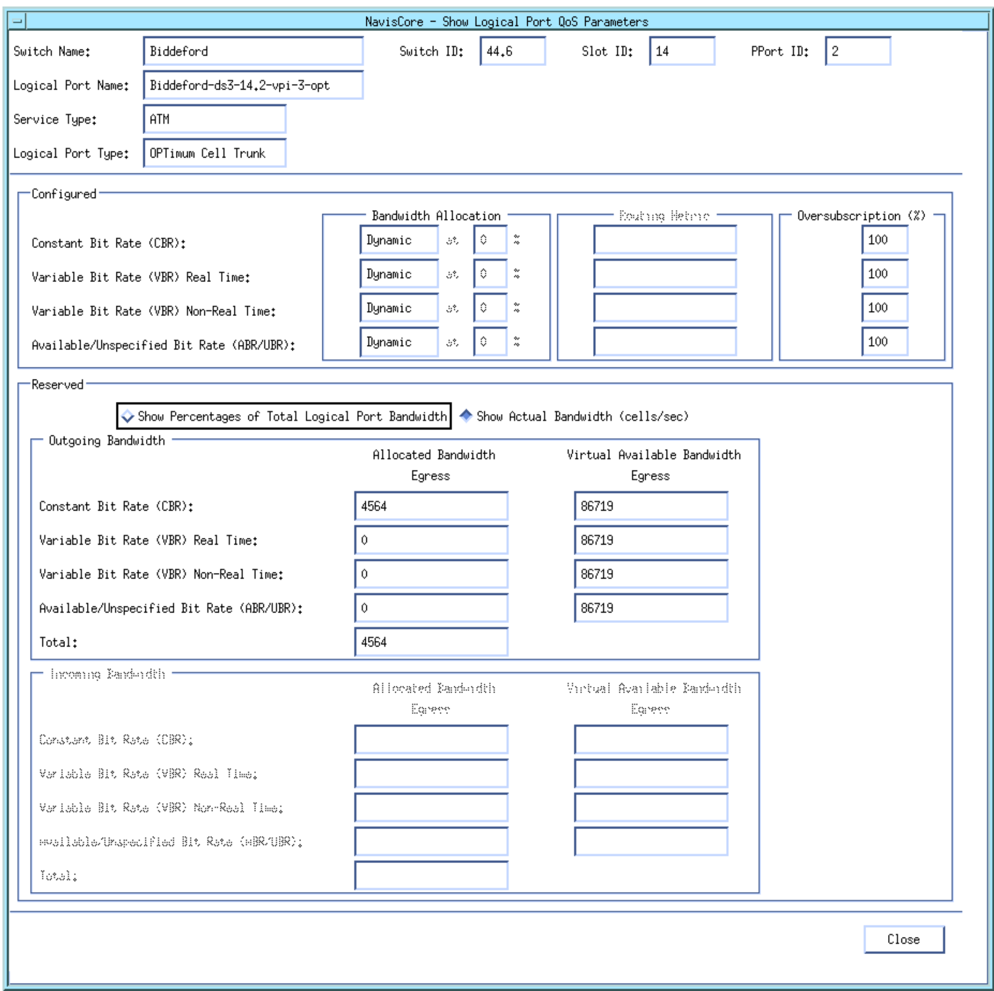


Figure 12-7. Show Logical Port QoS Parameters Dialog Box

Table 12-6 describes the fields on the Show Logical Port QoS Parameters dialog box.

Table 12-6. Show Logical Port QoS Parameters

Field	Displays...
Identification Fields	
Logical Port Name	The name that identifies the logical port.
Service Type	The service type.
Logical Port Type	The type of trunk, either ATM OPTimum Trunk or ATM Direct Trunk.
Configured (Class of Service)	
Constant Bit Rate (CBR)	Configured parameters for the CBR class of service. The CBR class handles digital information, such as video and digitized voice, that must be represented by a continuous stream of bits. CBR traffic requires guaranteed throughput rates and service levels.
Variable Bit Rate (VBR) Real Time	Configured parameters for the VBR-RT class of service. The VBR-RT class handles packaging special delay-sensitive applications, such as packet video, that require low cell delay variation between endpoints.
Variable Bit Rate (VBR) Non-Real Time	Configured parameters for the VBR-NRT class of service. The VBR-NRT class handles packaging for transfer of long, bursty data streams over a pre-established ATM connection. This service is also used for short, bursty data, such as LAN traffic. CPE protocols adjust for any delay or loss incurred through the use of VBR non-real time.
Available/Unspecified Bit Rate (ABR/UBR)	Configured parameters for the ABR/UBR class of service. The ABR/UBR class is primarily used for LAN traffic. The CPE should compensate for any delay or lost cell traffic.
Configured QoS Parameters	
Bandwidth Allocation	*Dynamic* or *Fixed* for each service class. *Dynamic* enables the bandwidth allocation to change dynamically according to bandwidth demands. Dynamic bandwidth allocation pools the remaining bandwidth for this logical port. This includes bandwidth that has not already been allocated to a specific queue or assigned to a connection. *Fixed* specifies the percentage of bandwidth that is reserved for the service class. If all four service classes are set to Fixed, then all four values should add up to 100% so that bandwidth is not wasted.

Table 12-6. Show Logical Port QoS Parameters (Continued)

Field	Displays...
Routing Metric	The routing metric for the trunk. Routing metrics allow the switch to select less congested paths and avoid congested paths when transferring data. One of the following routing metrics appears: *Cell/Frame Delay Variation* – Measures the average variation in delay between one cell and the next, measured in fractions of a second. When emulating a circuit, cell delay variation measurements allow the network to determine if cells are arriving too fast or too slow. *End-to-End Delay* – Measures the time it takes a cell to get from one end of a connection to the other. *Admin Cost* – Measures the administrative cost associated with the trunk. The administrative cost is specified by the administrator, allowing for manual routing.
Oversubscription	A minimum value of 100% to indicate the available virtual bandwidth that is available for a service class. A value of 100% ensures that the port will deliver all user data for that service class without unanticipated delays or excessive cell loss. A value of 200% effectively doubles the available virtual bandwidth that is available for that service class. However, if all network traffic attempts to use the network resources at precisely the same time (for example, during multiple file transfer sessions over the same trunk), some traffic may be delayed, or may even be dropped. ***Note:*** *The Oversubscription value for CBR is always set at 100% and cannot be modified.*
Outgoing/Incoming Bandwidth	
Allocated Bandwidth (Egress)	The allocated bandwidth as a percentage of total logical port bandwidth or as the actual bandwidth (in cells per second) depending on the option (“Show Percentages of Total Logical Port Bandwidth” or “Show Actual Bandwidth”) that you select at the bottom of the dialog box.
Virtual Available Bandwidth (Egress)	The virtual available bandwidth as a percentage of total logical port bandwidth or as the actual bandwidth (in cells per second) depending on the option (“Show Percentages of Total Logical Port Bandwidth” or “Show Actual Bandwidth”) that you select at the bottom of the dialog box.

Viewing PVC Usage

You can view all the PVCs that are currently using the trunk. To view these PVCs:

1. From the Monitor menu, select Ascend Objects ⇒ Show Trunks and select one of the following options:

   All on Map — Displays a list of all the trunks configured for the current map.

   All on Switch — Displays a list of all the trunks configured for a selected switch.

   The Show All Trunks dialog box appears (Figure 12-1 on page 12-2).

2. Select the trunk name from the Defined Trunk Name list box.

3. Choose Show PVCs. The Show All PVCs on Trunk dialog box appears (see Figure 12-8).

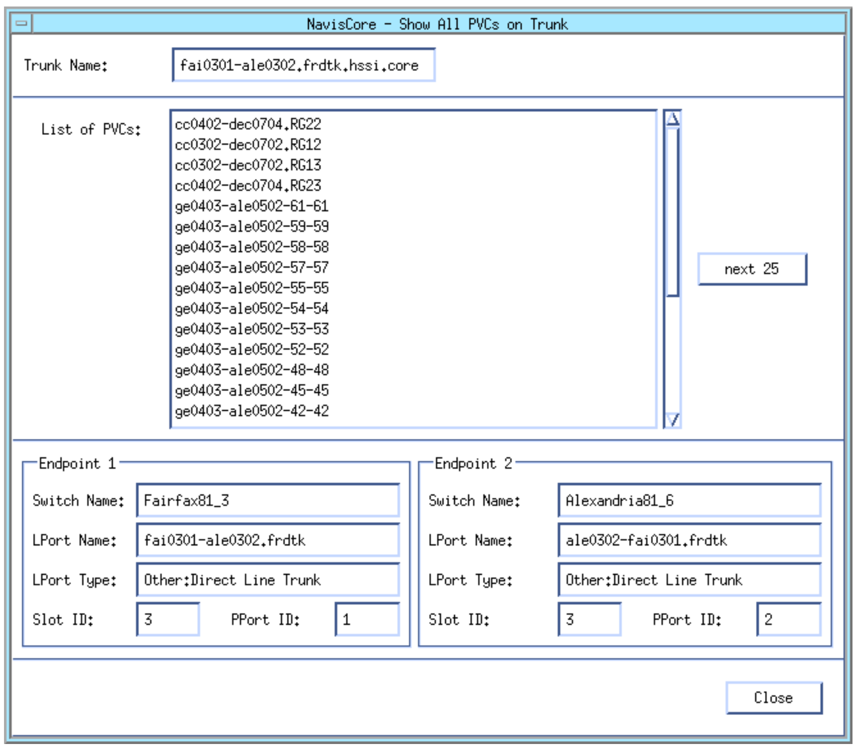


Figure 12-8. Show All PVCs on Trunk Dialog Box

The Show All PVCs on Trunk dialog box displays all the PVCs that are currently using the trunk. Table 12-7 describes the fields on the dialog box.

Table 12-7. Show All PVCs on Trunk Fields

Field	Displays...
Trunk Name	The configured trunk name.
List of PVCs	The list of PVCs that are using the trunk.
Endpoint 1/Endpoint 2	The following information about both trunk endpoints: *Switch Name* – The names of the switches at both ends of the trunk. *LPort Name* – The names of the logical ports at both ends of the trunk. *LPort Type* – The type of trunk that connects the logical ports. *Slot ID* – The number of the slot that contains the trunk’s physical port at the specified switch. *PPort ID* – The ID of the trunk’s physical port at the specified switch.

Viewing Customer/VPN Parameters

Virtual private networks (VPNs) enable you to create multiple private networks out of a single public network. After creating a VPN name and ID, you then create and associate one or more customer names and IDs with this VPN. Once you add the VPNs and customers to the database, you then assign the UNI/NNI logical ports to the particular VPN/customer association. In addition, you must also associate the required public network with a particular VPN.

You must associate any PVCs you create on the UNI/NNI logical ports with the desired VPN/customer pairing. SVCs on the other hands, automatically inherit the VPN/customer pairing of the host logical ports.

To enable a customer to monitor network resources without the ability to provision, edit either the .cshrc or the .profile file for an NMS user and add the following lines:

```
OVwRegDir=/opt/CascadeView/registration
export OVwRegDir
```

This line disables the Administer menu and all its provisioning functions; the NMS user only sees the Monitor menu functions.

Accessing VPN Functions

From the Administer menu, you can use the Ascend Objects: Select VPN/Customer function to monitor VPN and customer information.

From the Monitor menu, you can select Ascend Objects and use the following functions to monitor VPN and customer information:

- Show All Customers
- Show All Virtual Private Networks

Using the Select VPN/Customer Function

To monitor logical ports, PVCs, or trunks for a specific VPN or customer, use the Select Customer/VPN function. This function allows you to filter information on logical port, PVC, or trunk objects that does not pertain to the specified VPN or customer.

> You must log on to use the Select Customer/VPN function.

First select a VPN or customer name. Then when you monitor the logical port, PVC, or trunk objects, NavisCore only displays information for the selected VPN or customer name.

To use the Select VPN/Customer function:

1. From the Administer menu, select Ascend Object:Select Customer/VPN. The Select Customer/Virtual Private Network dialog box displays the names and IDs of customers and VPNs (see Figure 12-9).

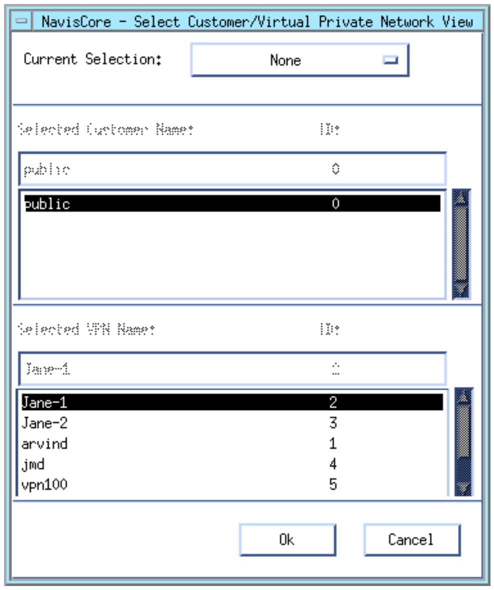


Figure 12-9. Select Customer/Virtual Private Network Dialog Box

2. Use the Current Selection menu to select either Customer or Virtual Private Network. Use None (default) to display all configured logical ports, PVCs, and trunks.
3. Review the selected customer name or selected VPN name list.
4. Choose OK to select a customer/VPN view.
5. Choose Cancel to exit the dialog box.

Viewing VPN Customers

To display all VPN customers:

1. From the Monitor menu, select Show All Customers/VPNs ⇒ Show All Customers. The Show All Customers dialog box appears (see Figure 12-10).

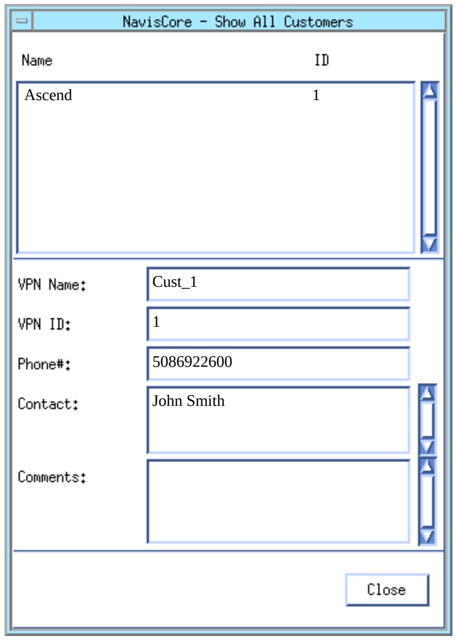


Figure 12-10. Show All Customers Dialog Box

Table 12-8 describes the Show All Customers fields.

2. When you finish viewing the information, choose Close to return to the network map.

Table 12-8. Show All Customers Fields

Field	Description
Name	The name of the customer using the VPN.
ID	The ID associated with each customer.
VPN Name	The name of the VPN assigned to this customer.
VPN ID	The ID of the VPN assigned to this customer.
Phone #	The phone number of the contact person at the customer site.
Contact	The name of the contact person at the customer site.
Comments	Any applicable comments.

Viewing VPNs

To view all VPNs defined on a map:

1. From the Monitor menu, select Ascend Objects ⇒ Show All Customers/VPNs ⇒ Show All Virtual Private Networks. The Show All Virtual Private Networks dialog box appears (see Figure 12-11).

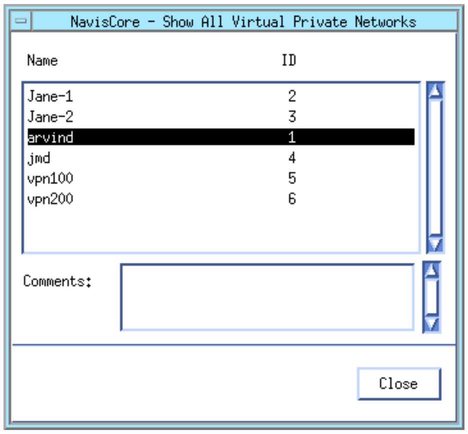


Figure 12-11. Show All Virtual Private Networks Dialog Box

2. Select the VPN name.

This dialog box displays the following fields:

Name — The name of the virtual private network (VPN).

ID — The ID associated with each VPN.

Comment — Any applicable comments.

3. When you finish viewing information, choose Close to return to the network map.

13

Monitoring ATM Circuits

This chapter describes how to monitor ATM circuits. Ascend switches support ATM communications over the following types of circuits:

- Point-to-Point Permanent Virtual Circuits (PVCs)
- Point-to-Multipoint PVCs
- Point-to-Point Soft PVCs (SPVCs)
- Point-to-Multipoint SPVCs
- Switched Virtual Circuits (SVCs)

Viewing Point-to-Point ATM PVCs

This section describes how to view the status and summary statistics of point-to-point ATM PVCs.

Viewing Point-to-Point ATM PVC Status

To view the current configuration, status, and routing information for all point-to-point PVCs in the network:

1. From the Monitor menu, select Ascend Objects ⇒ Show Circuits, and select one of the following options:

   All by Name — Enter a specific circuit name. To use wild-card characters to search by name, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

   All on Switch — Select a switch on the current map, then use this option to view a list of all the circuits configured for this switch.

All on Switch and by Name — Select a switch on the current map, then use this option to enter a specific circuit to search by name. To use wild-card characters, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

All on Map — Displays a list of all the circuits configured for the current map.

All by Defined Path — Displays a list of all circuits that have a defined path.

All Point-to-Multipoint — Displays a list of all point-to-multipoint circuits. See "Viewing Point-to-Multipoint PVCs" on page 13-23 for more information.

After you select an option, the Show All PVCs dialog box appears. Figure 13-1 shows a sample dialog box with a selected ATM PVC.

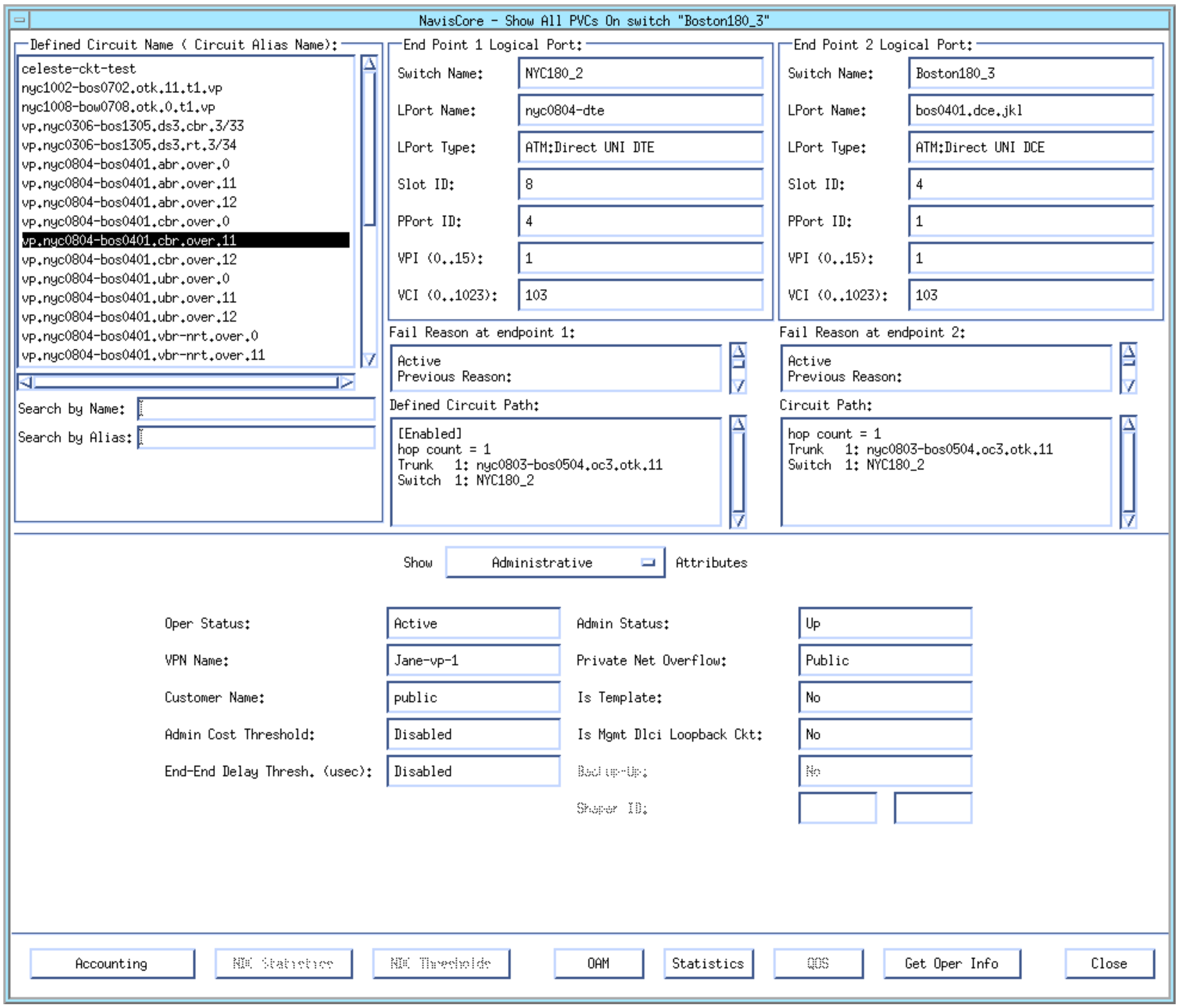


Figure 13-1. Show All PVCs Dialog Box (ATM PVC and Administrative Attributes)

> If the circuit names do not appear immediately in the Defined Circuit Name list box, insert the cursor in the blank Search by Name field and press Return. This action will display a list of configured circuits.

2. Select the name of the circuit for which you want to retrieve status information. Use the Search by Name or Search by Alias fields to enter wild-card characters:
   - Use an * to match any number of characters
   - Use a ? to match a single character
   - Type * to match the * character
   - Type \? to match the ? character
   - Type \\ to match the \ character

The specific fields that appear on the Show All PVCs dialog box depend on the type of service. For example, ATM PVC fields differ from Frame Relay PVC fields. See Chapter 14, “Monitoring Frame Relay Circuits” for information on Frame Relay PVCs.

The Show All PVCs dialog box displays general PVC information at the top of the dialog box and provides the Show Attributes option menu enabling you to view attributes. See the following sections to view specific PVC attribute information:

PVC Attribute	See...
Administrative	“Viewing ATM PVC Administrative Attributes” on page 13-9.
Common User Preference	“Viewing ATM PVC Common User-Preference Attributes” on page 13-10.
ATM User Preference	“Viewing ATM PVC ATM User-Preference Attributes” on page 13-12.
Traffic Type	“Viewing ATM PVC Traffic Type Attributes” on page 13-13.
NDC	“Viewing ATM PVC NDC Attributes” on page 13-15.
Frame Discard	“Viewing ATM PVC Frame Discard Attributes” on page 13-16.
Extended QoS Parameters	“Viewing ATM PVC Extended QoS Attributes” on page 13-17.

Table 13-1 describes the option menu and buttons on the dialog box and Table 13-2 describes general PVC information fields.

Table 13-1. Show All PVCs Buttons

Button	Function
Show Attributes (Option Menu)	Displays an option menu from which you can select ATM PVC attributes.
Accounting	Accesses the accounting functions for a PVC. For more information, see the *NavisXtend Accounting Server Administrator's Guide.*
NDC Statistics	Displays the Network Data Collection (NDC) statistics for the selected circuit (applies to ATM PVCs only). For more information, see "Viewing NTM and NDC Statistics" on page 13-30.
NDC Thresholds	Displays the configured NDC thresholds for the circuit. For more information, see "Viewing NTM and NDC Statistics" on page 13-30.
OAM	Runs the Operations, Administration, and Management diagnostics for the selected circuit. For more information, see "Testing ATM Circuits" on page 13-90.
Statistics	Displays the summary statistics for the selected circuit.
Get Oper Info	Updates the values in the fields.
Close	Exits the dialog box.

Table 13-2. General PVC Information Fields (ATM PVCs)

Field	Displays...
Defined Circuit Name	A list of the PVCs in the network.
Logical Port – Information on the two logical port endpoints.	
Switch Name	The name of the switch at each endpoint of the circuit.
LPort Name	The name of the logical port at each endpoint of the circuit.
LPort Type	The configured type of the selected logical port.
Slot ID	The number of the physical slot where the I/O module used by the circuit is installed.
PPort ID	The number of the physical port on which the circuit is configured.

Table 13-2. General PVC Information Fields (ATM PVCs) (Continued)

Field	Displays...
VPI (0..nnnn)	The virtual path identifier (VPI) for the selected circuit at this endpoint. A virtual path is a group of virtual channels carried between two points. VPIs provide a way to bundle traffic headed in the same direction. The number that the system displays for this field is equivalent to the VPI value in the ATM cell header and is used to route cell traffic. See the *NavisCore ATM Configuration Guide* for more information.
VCI (32..nnnn)	The virtual channel identifier (VCI) for the selected circuit at this endpoint. A virtual channel is a connection between two communicating ATM entities. It may consist of a group of several ATM links, CPE to central office switch, switch to switch, and switch to user equipment. All communications proceed along this same VC, which preserves call sequence and provides a certain quality of service. The number in this field equals the VCI value in the ATM cell header. See the *NavisCore ATM Configuration Guide* for more information.
Fail Reason at endpoint 1 (2)	The reason a selected circuit failed (if any) for a given endpoint. See Table 13-3 for information on operational status codes.
Defined Circuit Path	The configured circuit path.
Actual Circuit Path	The actual path that OSPF selected for this circuit.

► The Show All PVCs dialog box displays the circuit names and circuit attributes as configured in the NMS. The Status, Path, and Fail Reasons are extracted directly from the switch.

Table 13-12 describes the inactive PVC status codes.

Table 13-3. Inactive PVC Operational Status Codes

Fail Reason	Description	Solution
Circuit Admin Status is Down	Circuit activity is disabled; the admin status is set to Down.	Reconfigure the circuit's admin status to Up.
Internal Error: No VC Buffer at [*node*]	A shortage of virtual circuit buffers exists at the node.	**Serious Error! Report problem to the Ascend Technical Assistance Center.**
Not enough bandwidth on trunk at [*node*]	One of the trunks in the circuit path does not have enough bandwidth to accommodate the circuit.	Reconfigure the circuit to a lower bandwidth or increase the physical or virtual bandwidth of the trunk. You can also add more parallel trunks. Keep in mind that increasing the physical or virtual trunk bandwidth will temporarily disrupt traffic on the trunk.
Destination node is unreachable at [*node*]	The destination node is not accessible from the higher numbered node.	Troubleshoot a possible connectivity problem with the unreachable switch.
Ascend circuit segment call has timed out	Attempts to establish the circuit (PVC) through the network have failed and timed out.	This problem may occur on a defined path where the alternate path option is disabled.
Internal error: No circuit PDU buffer at [*node*]	A shortage of protocol buffers exists.	**Serious Error! Report problem to the Ascend Technical Assistance Center.**
OPTimum path flow is blocked at [*node*]	Data flow through the public data network is temporarily blocked due to the flow-control mechanism.	This condition should correct itself. If the problem persists, check for congestion in the OPTimum path.
Trunk is down at [*node*]	A trunk line in the circuit path is down.	The circuit automatically reroutes if alternate paths are defined.
UNI/NNI is down at [*node, lport*]	The UNI or NNI is down at the node/interface number (ifnum).	Make sure the switch is connected to the user device. Display traffic in and out of the port by generating summary statistics.
PVC segments are not ready to receive beyond [*lport, node*]	(NNI specific problem.) The PVC segment(s) beyond this logical port sent a flow block message stating that it cannot receive data.	A trunk line in the circuit path may be down. Check the status of all PVC segments in the network beyond the logical port noted in the Fail Reason.

Table 13-3. Inactive PVC Operational Status Codes (Continued)

Fail Reason	Description	Solution
Warning: Defined Path is not available. The alternate path is in use. PVC segments are inactive beyond [*lport, node*]	The caller node cannot be reached through the defined path. This problem may be caused by a connection failure.	Verify the integrity of the trunk that is being used on the defined circuit path. Once the defined path is re-established, the circuit is routed back to the defined path within 20 seconds of availability.
IOP/IOM is down	An IOM used by the circuit is down.	Check the status of the IOM. See Chapter 2, "Viewing Switch, Module, and Physical Port Details" for more information.
No PVC Manager PDU msg buffer	The PVC manager has no user message buffer for the PDU.	**Serious Error! Report problem to the Ascend Technical Assistance Center.**
Port is not configured	No logical port is configured for use by the PVC.	Configure a logical port for the PVC. See the *NavisCore ATM Configuration Guide* for details.
Mis-configuration	Configuration error.	Check the PVC attributes as described in this chapter.
SVC setup failed	Soft PVC setup failed.	Check the soft PVC attributes and statistics. See "Viewing Soft PVCs" on page 13-47.
Source is in a 'backup' condition	The PVC switched over to a backup.	Check PVC attributes and statistics. See "Viewing Point-to-Point ATM PVCs" on page 13-1.
Source is unknown.	The PVC source is unknown.	Check PVC attributes and statistics. See "Viewing Point-to-Point ATM PVCs" on page 13-1.
Destination is unknown	The PVC destination is unknown.	Check PVC attributes and statistics. See "Viewing Point-to-Point ATM PVCs" on page 13-1.
Node running incompatible version of switch software exists in circuit path	A switch that is running an incompatible version of software is in the circuit path.	Verify that all switches in the circuit path are running compatible versions of switch software.
SMDS management trunk	The PVC attempted to traverse an SMDS management trunk.	Reroute the PVC so that it does not traverse an SMDS management trunk.

Table 13-3. Inactive PVC Operational Status Codes (Continued)

Fail Reason	Description	Solution
Endpoint never called	The PVC connection was never established.	Check PVC attributes and statistics. See "Viewing Point-to-Point ATM PVCs" on page 13-1.
Both endpoints in 'backup'	Both PVC endpoints are in a backup condition (that is, they are switching to backup PVCs).	Check PVC attributes and statistics. See "Viewing Point-to-Point ATM PVCs" on page 13-1.
Attempting to route through management trunk	The PVC attempted to traverse a management trunk.	Reroute the PVC so that it does not traverse a management trunk.
Multipoint parent not found	No multipoint circuit parent (that is, the circuit root) was found.	Check multipoint PVC attributes to see if the parent (that is, the circuit root) was defined. See "Viewing Point-to-Multipoint PVCs" on page 13-23.
Route changed during setup	The PVC route failed because it changed during PVC setup.	Make sure that the PVC route is stable during PVC setup.
No VPI or VCI is available	No VPI or VCI is available for the ATM PVC.	Configure an available VPI or VCI for the PVC. See the *NavisCore ATM Configuration Guide* for more information.
SVC cleared by user	The soft PVC was cleared by the user.	Re-establish the soft PVC connection.
Circuit path registration failed	Problems were encountered during PVC path registration.	Check PVC attributes and statistics. See "Viewing Point-to-Point ATM PVCs" on page 13-1.
Selected channel cannot be allocated	The ATM channel selected by the PVC cannot be allocated.	Check ATM PVC attributes. See "Viewing Point-to-Point ATM PVCs" on page 13-1.
No available bandwidth in reverse direction	No bandwidth in the reverse direction is available.	Check the PVC configuration to see if sufficient bandwidth is available.
Disrupted due to priority routing	High priority VCI is in the PVC's path. The PVC is disrupted due to priority routing.	Network congestion or other problems initiated priority-routing algorithms that disrupted the PVC. This condition should clear as soon as the problem is corrected.
Couldn't allocate negative priority bandwidth	No negative priority bandwidth could be allocated.	Check the PVC configuration to see if there is sufficient bandwidth available.

Viewing ATM PVC Administrative Attributes

To view ATM PVC administrative attributes: from the Show All PVCs dialog box (Figure 13-1 on page 13-2), select the ATM PVC you want to view. The administrative attributes appear by default.

Table 13-4 describes ATM PVC administrative attributes.

Table 13-4. ATM PVC Administrative Attributes Fields

Field	Displays...
Oper Status	The operational status of the PVC. There are four possible values: *Active* – The PVC is operational between the two endpoints. *Inactive* – The PVC is not operational between the two endpoints. *Invalid* – The PVC configuration is not contained within the calling node. *Unknown* – The calling node did not respond to the NMS request for the status of this PVC.
VPN Name	The VPN name for the PVC (if applicable) or *Public* if the PVC is not reserved for a VPN.
Customer Name	The customer name for the selected PVC (if applicable). Otherwise, the field displays *Public*.
Admin Cost Threshold	The maximum administrative cost for the circuit. The circuit cannot be established unless at least one path with a cost less than or equal to the admin cost is available. This cost allows administrators to create paths manually. If the switch encounters problems establishing PVCs over manually defined paths, increase the cost.
End-End Delay Thresh (µsec)	One of the following: *Enabled* – The end-end delay feature is enabled. If this field is enabled, a value will appear in the Cell Transfer Delay field when you display ATM user-preference attributes. This field is described in Table 13-6 on page 13-12. *Disabled* – The end-end delay feature is disabled.
Admin Status	One of the following: *Up* – The admin status of the circuit is up. *Down* – The admin status of the circuit is down.
Private Net Overflow	One of the following: *Public* – The customer is allowed to use a public trunk in the event of overflow or trunk failure. *Restrict* – The customer is restricted to its own VPN trunks during overflow or trunk failure.

Table 13-4. ATM PVC Administrative Attributes Fields (Continued)

Field	Displays...
Is Template	One of the following: *Yes* – This circuit connection was defined as a template. *No* – This connection is not a template.
Is Mgmt Dlci Loopback Ckt	Always displays *No* for circuits that support ATM traffic only.
Backed-Up	One of the following: *Yes* – This circuit has a backup circuit. *No* – This circuit does not have a backup circuit.
Shaper ID (Circuits that use ATM UNI DTE/DCE logical ports associated with the ATM IWU IOM or ATM CS IOM)	The ID of the traffic shaper that the circuit uses to transmit data. A traffic shaper is associated with several parameters that control traffic, such as priority parameters, sustainable cell rate (SCR), peak cell rate (PCR), and maximum burst size (MBS).

Viewing ATM PVC Common User-Preference Attributes

To view ATM PVC common user-preference attributes:

1. From the Show All PVCs dialog box (Figure 13-1 on page 13-2), select the ATM PVC you want to view.
2. Choose Show Common User Preference Attributes. The attributes fields appear (see Figure 13-2).

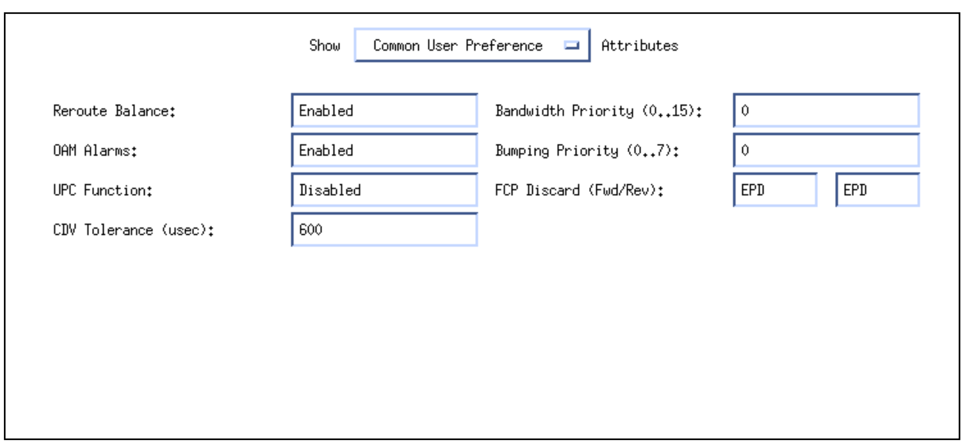


Figure 13-2. ATM PVC Common User-Preference Attributes Fields

Table 13-5 describes the common user-preference attributes fields.

Table 13-5. ATM PVC Common User-Preference Attributes Fields

Field	Displays...
Reroute Balance	One of the following: *Enabled* (the default) – Switch tuning parameters take effect for the circuit. *Disabled* – Switch tuning parameters are ignored for the circuit.
OAM Alarms	One of the following: *Enabled* – The circuit generates OAM F5 or F4 AIS alarms to indicate that the circuit is down. *Disabled* – The circuit does not generate OAM F5 or F4 AIS alarms.
UPC Function	One of the following: *Enabled* – The circuit tags or drops cells that do not conform to the traffic parameters as they come into the port. *Ascend recommends that you enable the UPC function on all circuits.* *Disabled* – The circuit allows all traffic, including non-conforming traffic, into the port.
CDV Tolerance (µsec)	The cell delay variation (CDV) tolerance. CDV measures the average variation in delay between one cell and the next. Valid values are between 1 - 65535 µs. The default is 600 µs.
Bandwidth Priority	The bandwidth priority for the circuit, which is a value from 0 through 15 where 0 indicates the highest priority. In the event of provisioning, trunk failure recovery, or load balance rerouting, VCs use the combination of bandwidth priority and bumping priority to preserve proper routing priority. See “Viewing SVC Routing Priorities” on page 7-31 for a description of bandwidth priority.
Bumping Priority	The bumping priority for the circuit, which is a number from 0 through 7 where 0 indicates the highest priority. In the event of provisioning, trunk failure recovery, or load balance rerouting, VCs use the combination of bandwidth priority and bumping priority to preserve proper routing priority. See “Viewing SVC Routing Priorities” on page 7-31 for a description of bumping priority.
FCP Discard (Fwd/Rev) (CBX 500 FCP Only)	One of the following values for both the forward and reverse direction: *CLP1* – For UBR, ABR, and VBR-NRT PVCs, the ATM Flow Control Processor (FCP) discards each cell with CLP set to 1 that causes the PVC queue to exceed the discard thresholds. This flow control technique is also known as “Selective Discard.” *EPD* – For UBR, ABR, and VBR-NRT PVCs, the FCP performs early packet discard (EPD). If a cell causes the queue for a PVC to exceed the discard thresholds, the PVC enters the EPD state. This means that the cells in the current packet are admitted to the queue. However, when the end of the current packet is detected, all of the cells in the next packet are discarded.

Viewing ATM PVC ATM User-Preference Attributes

To view ATM PVC ATM user-preference attributes:

1. From the Show All PVCs dialog box (Figure 13-1 on page 13-2), select the ATM PVC you want to view.
2. Choose Show ATM User Preference Attributes. The attributes fields appear (see Figure 13-3).

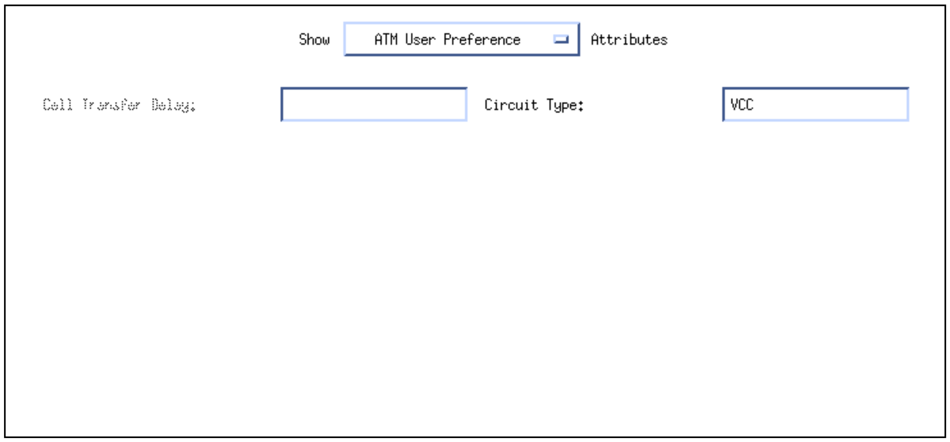


Figure 13-3. ATM PVC User-Preference Attributes Fields

Table 13-6 describes the ATM user-preference attributes fields.

Table 13-6. ATM PVC ATM User-Preference Attributes Fields

Field	Displays...
Cell Transfer Delay	The accumulated cell transfer delay (CTD) for the circuit, in microseconds. The CTD is the time it takes for a cell to go from one end of the circuit to the other. This field is blank if this feature is disabled.
Circuit Type	The circuit type, either a virtual path connection (VPC) or virtual channel connection (VCC).

Viewing ATM PVC Traffic Type Attributes

To view ATM PVC traffic type attributes:

1. From the Show All PVCs dialog box (Figure 13-1 on page 13-2), select the ATM PVC you want to view.
2. Choose Show Traffic Type Attributes. The attributes fields appear (see Figure 13-4).

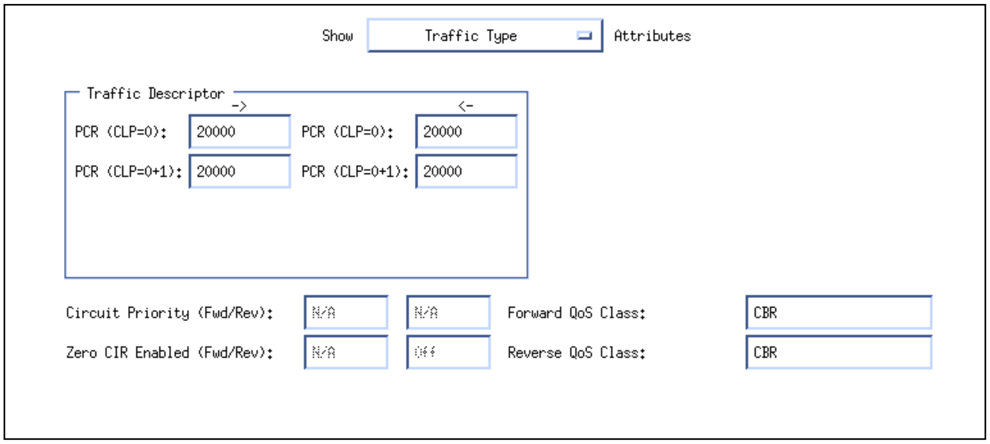


Figure 13-4. ATM PVC Traffic Type Attributes Fields

Table 13-7 describes the traffic type attributes fields.

Table 13-7. ATM PVC Traffic Type Attributes Fields

Field	Displays...
Traffic Descriptor	One or more of the following traffic descriptors for the forward and reverse directions: *PCR CLP=0 (cells/sec)* – The PCR in cells per second for high-priority traffic (i.e., the CLP=0 cell stream). PCR is the maximum allowed cell transmission rate. It defines the shortest time period between cells, and provides the highest guarantee that network performance objectives (based on cell loss ratio) will be met. *PCR CLP=0+1 (cells/sec)* – The PCR in cells per second for the combined high- and low-priority traffic (i.e., the CLP=0+1 aggregate cell stream). *SCR CLP=0 (cells/sec)* – The SCR in cells per second for the combined high-priority traffic (i.e., the CLP=0 cell stream). SCR is the maximum average cell transmission rate that is allowed over a given period of time on a given circuit. *SCR CLP=0+1 (cells/sec)* – The SCR in cells per second for the combined high- and low-priority traffic (i.e., the CLP=0+1 aggregate cell stream). *MBS CLP=0 (cells/sec)* – The MBS (in cells per second) for the combined high-priority traffic (i.e., the CLP=0 cell stream). MBS is the maximum number of cells that can be received at the PCR. *MBS CLP=0+1 (cells/sec)* – The MBS (in cells per second) for the combined high- and low-priority traffic (i.e., the CLP=0+1 cell stream). *MCR CLP=0 (cells/sec)* – The Minimum Cell Rate (MCR) (in cells per second) for the combined high-priority traffic (i.e., the CLP=0 cell stream). MCR is the rate at which the source switch is always allowed to send data.
Circuit Priority (Fwd/Rev)	The forward and reverse circuit priority, where 1 is highest priority, 2 is medium priority, 3 is low priority, and 4 is lowest priority. This field applies to PVCs of QoS class VBR-RT and VBR-NRT on CBX 500 and GX 550 switches only.
Zero CIR Enabled	This field applies to Frame Relay PVCs and ATM-to-Frame PVCs only. See "Viewing Frame Relay PVC Traffic Type Attributes" on page 14-13.
Forward QoS Class	The Quality of Service class for forward traffic.
Reverse QoS Class	The Quality of Service class for reverse traffic. This value does not have to be the same as the Forward QoS Class.

Viewing ATM PVC NDC Attributes

To view ATM PVC NDC attributes:

1. From the Show All PVCs dialog box (see Figure 13-1 on page 13-2), select the ATM PVC you want to view.
2. Choose Show NDC Attributes. The attributes fields appear (see Figure 13-5).

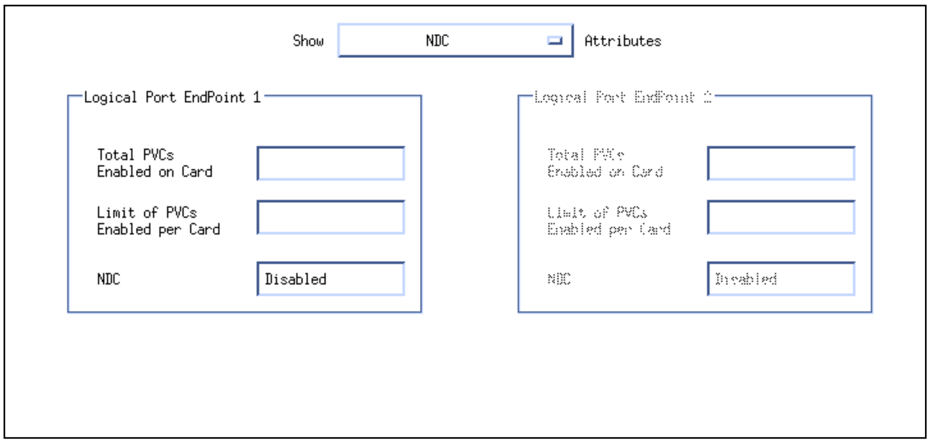


Figure 13-5. ATM PVC NDC Attributes Fields

Table 13-8 describes the NDC attributes fields.

Table 13-8. ATM PVC NDC Attributes Fields

Field	Displays...
Total PVCs Enabled on Card	The current number of NDC-enabled endpoints for the card at each endpoint.
Limit of PVCs Enabled per Card	The limit (360) of NDC-enabled endpoints you can configure on a module at each endpoint.
NDC	One of the following: *Enabled* – NDC statistics are collected for this circuit endpoint. *Disabled* – NDC statistics are not collected for this circuit endpoint.

Viewing ATM PVC Frame Discard Attributes

To view ATM PVC frame discard attributes:

1. From the Show All PVCs dialog box (see Figure 13-1 on page 13-2), select the ATM PVC you want to view.
2. Choose Show Frame Discard Attributes. The attributes fields appear (see Figure 13-6).

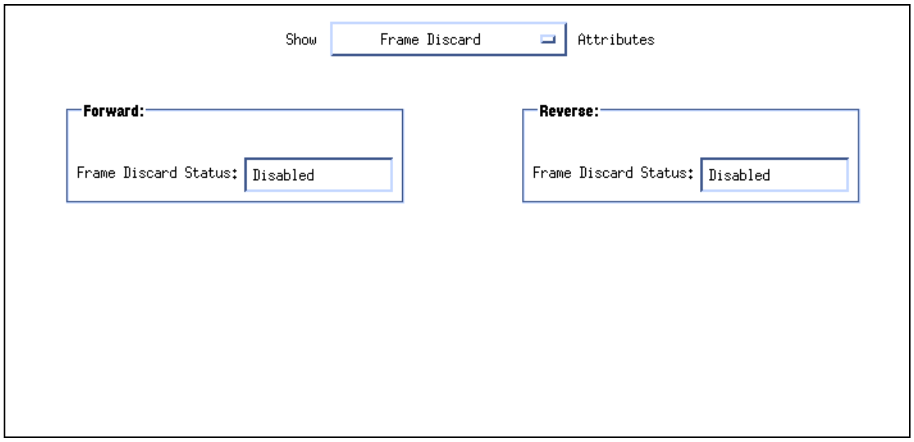


Figure 13-6. ATM PVC Frame Discard Attributes Fields

Table 13-9 describes the frame discard attributes fields.

Table 13-9. ATM PVC Frame Discard Attributes Fields

Field	Displays...
Forward	One of the following: *Enabled* – Frame discard is enabled in the forward direction. Frame discard is enabled to turn on the physical port output buffer EPD/PPD function for this PVC. When enabled, ATM Adaptation Layer 5 (AAL5) traffic that traverses the PVC is subject to EPD/PPD when physical port congestion is encountered. *Disabled* – Frame discard is disabled in the forward direction.
Reverse	One of the following: *Enabled* – Frame discard is enabled in the reverse direction. See the description of the Forward field for more information on frame discard. *Disabled* – Frame discard is disabled in the reverse direction.

Viewing ATM PVC Extended QoS Attributes

To view ATM PVC extended QoS attributes:

1. From the Show All PVCs dialog box (see Figure 13-1 on page 13-2), select the ATM PVC you want to view.
2. Choose Show Extended QoS Parameters Attributes. The attributes fields appear (see Figure 13-7).

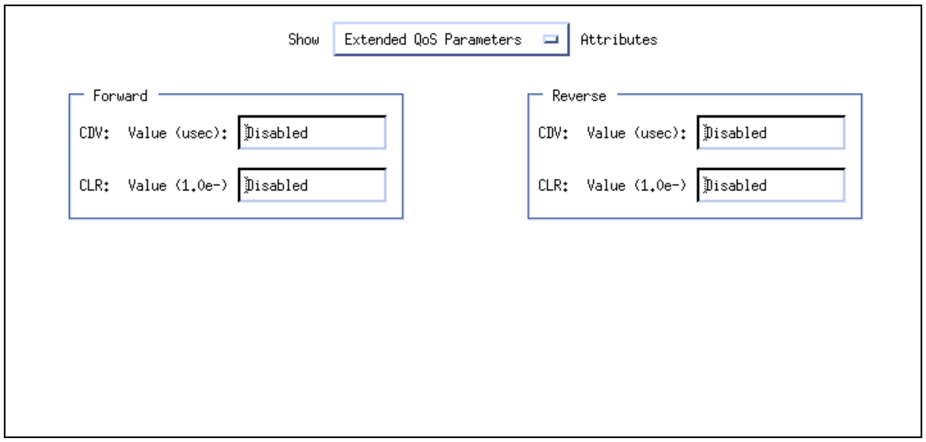


Figure 13-7. ATM PVC Extended QoS Attributes Fields

Table 13-10 describes the extended QoS parameters attributes fields.

Table 13-10. ATM PVC Extended QoS Attributes Fields

Field	Displays...
CDV: Value (µsec)	The accumulated forward and reverse CDV for the circuit, in microseconds. If the attribute is not configured, displays *Disabled*.
CLR: Value (1.0e-)	The forward and reverse cell loss ratio (CLR) requirement. This value is expressed as a negative exponent of 10. A value of 255 indicates that any CLR is acceptable. If the attribute is not configured, displays *Disabled*.

Viewing Point-to-Point ATM PVC Summary Statistics

Point-to-Point ATM PVC summary statistics display the number of cells a circuit has sent and received, the round-trip delay, and other Quality of Service statistics for the circuit.

> Resource Management (RM) cells are counted as passed CLP 0 or passed CLP 1 cells. The Logical Port Statistics dialog box provides separate RM cell statistics on a per logical port basis (see "Viewing Logical Port Summary Statistics" on page 6-19).

To view point-to-point ATM PVC statistics:

1. From the Monitor menu, select Ascend Objects ⇒ Show Circuits.
2. Select one of the following options:

   All by Name — Enter a specific circuit name. To use wild-card characters to search by name, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

   All on Switch — Select a switch on the current map, then use this option to view a list of all the circuits configured for this switch.

   All on Switch and by Name — Select a switch on the current map, then use this option to enter a specific circuit to search by name. To use wild-card characters, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

   All on Map — Displays a list of all the circuits configured for the current map.

   All by Defined Path — Displays a list of all circuits that have a defined path.

   All Point-to-Multipoint — Displays a list of all point-to-multipoint circuits. See "Viewing Point-to-Multipoint PVCs" on page 13-23 for more information.

   After you select an option, the Show All PVCs dialog box appears (Figure 13-1 on page 13-2).

3. Select the ATM PVC you want to view.
4. Choose Statistics to view the Circuit Summary Statistics dialog box. The fields vary depending on the type of traffic the circuit supports. Figure 13-8 shows the Circuit Summary Statistics dialog box for ATM circuits, and Figure 13-9 shows the Circuit Summary Statistics dialog box for Frame-to-ATM circuits.

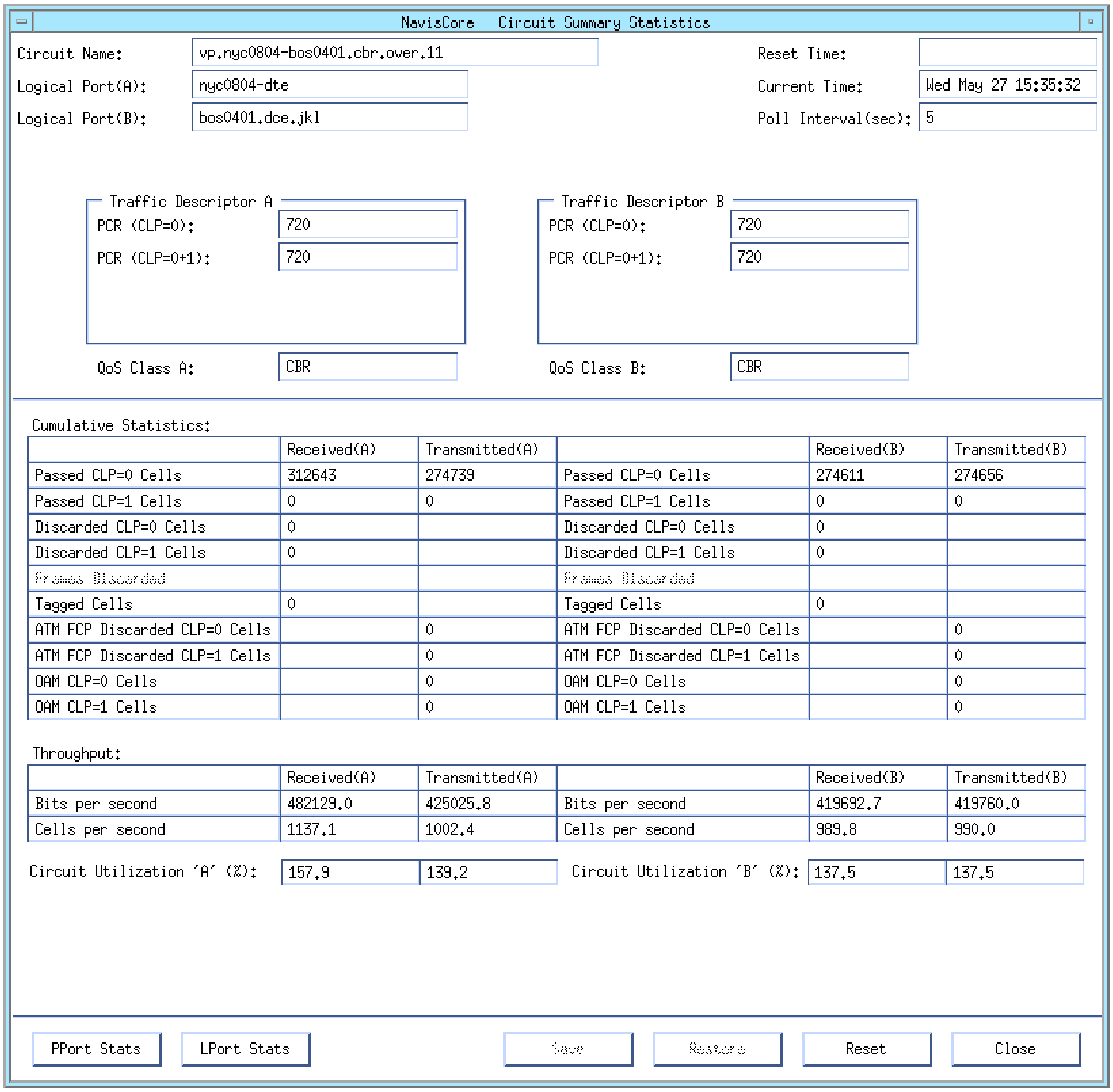


Figure 13-8. Circuit Summary Statistics Dialog Box (ATM Circuits)

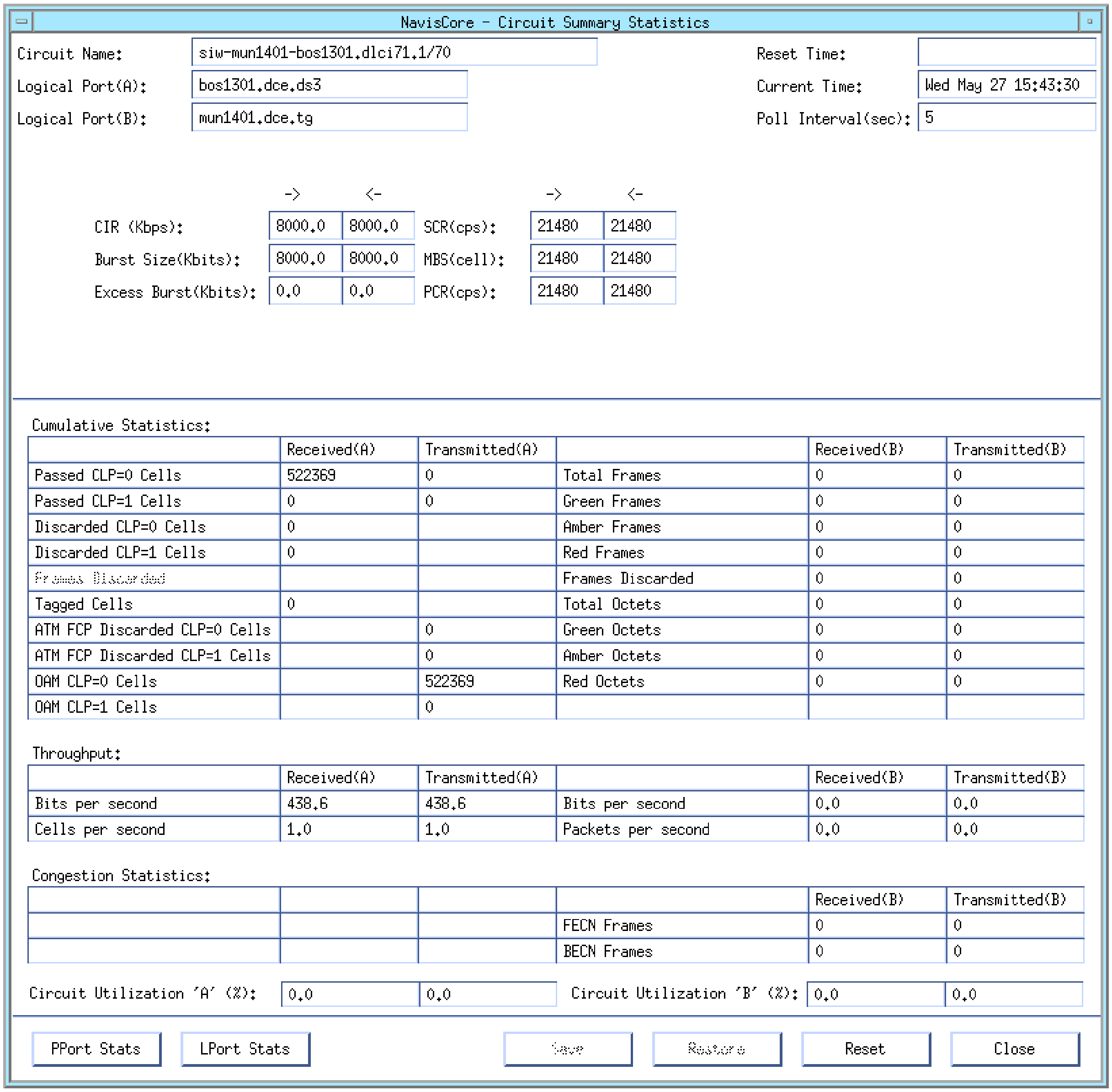


Figure 13-9. Circuit Summary Statistics Dialog Box (Frame-to-ATM Circuits)

This dialog box displays statistics for transmitted and received data for each circuit logical port endpoint (A and B). These statistics reflect how a circuit's data is used over the network.

Table 13-11 describes the statistics and other fields that appear for ATM circuits. For Frame-to-ATM circuits, note that ATM statistics appear for the ATM circuit endpoint, and Frame Relay statistics appear for the Frame Relay circuit endpoint. For information on Frame Relay statistics, see "Viewing Frame Relay PVC Summary Statistics" on page 14-20.

Table 13-11. Circuit Summary Statistics Fields (ATM)

Statistic	Description
Circuit Name	The name of the circuit.
Logical Port (A)	The logical port at one circuit endpoint.
Logical Port (B)	The logical port at one circuit endpoint.
Reset Time	The time of the last reset of the selected switch (if you are viewing all PVCs on switch).
Current Time	The current system time (if you are viewing all PVCs on switch).
Poll Interval (sec)	The time interval for the collection of statistical data.
Traffic Descriptor A	The traffic descriptor configured for one circuit endpoint.
Traffic Descriptor B	The traffic descriptor configured for one circuit endpoint.
QoS Class A	The QoS class configured for one circuit endpoint.
QoS Class B	The QoS class configured for one circuit endpoint.
Cumulative Statistics	
Passed CLP=0 Cells	The total number of cells that were received and transmitted.
Passed CLP=1 Cells	The total number of CLP=1 cells received at the port. This does not include CLP=0 cells that were received and then tagged at CLP=1 cells because of a traffic descriptor violation (they were counted as tagged cells).
Discarded CLP=0 Cells	The total number of received CLP=0 cells that are dropped because the cell violates the defined traffic descriptor. *Note: Consistently high values in the Discarded CLP=0 Cells, Discarded CLP=1 Cells, and Tagged Cells fields indicate that either the source may need to slow transmission or that you should reconfigure the traffic descriptors to reflect the source speed.*
Discarded CLP=1 Cells	The total number of CLP=1 cells that are discarded because the cells violate the defined traffic descriptor. *Note: Consistently high values in the Discarded CLP=0 Cells, Discarded CLP=1 Cells, and Tagged Cells fields indicate that either the source may need to slow transmission or that you should reconfigure the traffic descriptors to reflect the source speed.*

Table 13-11. Circuit Summary Statistics Fields (ATM) (Continued)

Statistic	Description
Tagged Cells	The total number of CLP=0 cells that were tagged as CLP=1 cells. Cells are tagged if they do not conform to the defined traffic descriptor for the circuit. *Note: Consistently high values in the Discarded CLP=0 Cells, Discarded CLP=1 Cells, and Tagged Cells fields indicate that either the source may need to slow transmission or that you should reconfigure the traffic descriptors to reflect the source speed.*
ATM FCP Discarded CLP=0 Cells	The total number of received CLP=0 cells that are received and discarded by the ATM Flow Control Processor (FCP).
ATM FCP Discarded CLP=1 Cells	The total number of CLP=1 cells that are received and discarded by the ATM FCP.
OAM CLP=0 Cells	The total number of F4 and F5 OAM CLP=0 cells that were transmitted by the circuit.
OAM CLP=1 Cells	The total number of F4 and F5 OAM CLP=1 cells that were transmitted by the circuit.
Throughput Statistics	
Bits per second	The total number of bits received and transmitted by the circuit each second.
Cells per second	The total number of cells received and transmitted by the circuit each second.
Utilization Statistics	
Circuit Utilization A (%)	The amount of traffic queued for transmission on a circuit measured as a percentage of link speed. Therefore, the circuit utilization value can exceed 100%.
Circuit Utilization B (%)	The amount of traffic queued for transmission on a circuit measured as a percentage of link speed. Therefore, the circuit utilization value can exceed 100%.

Viewing Point-to-Multipoint PVCs

To view point-to-multipoint PVC status and statistics:

1. From the Monitor menu, select Ascend Objects ⇒ Show Circuits ⇒ All Point-to-Multipoint. The Show All Point-to-Multiple-Point Circuit Roots dialog box appears (see Figure 13-10).

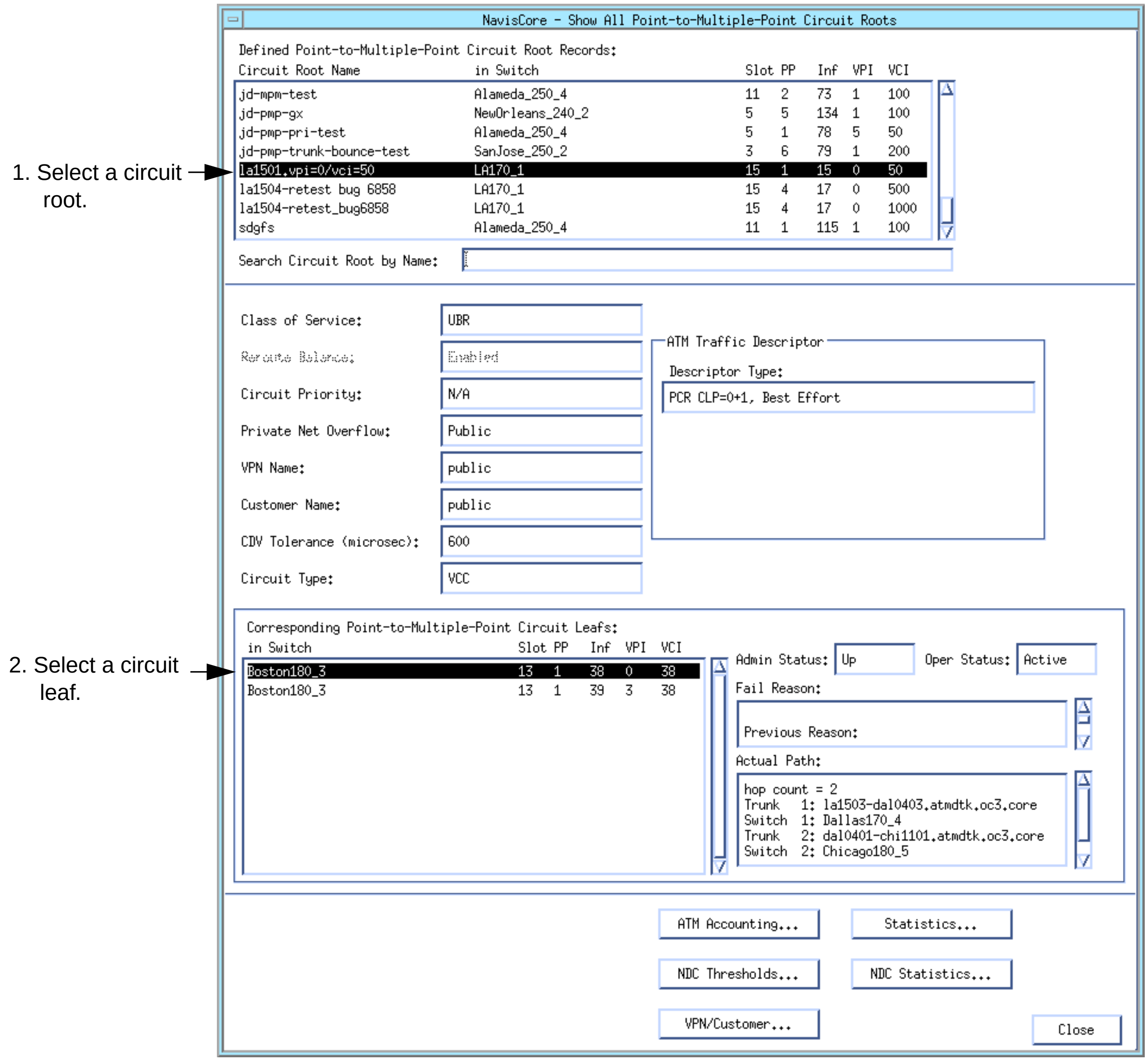


Figure 13-10. Show All Point-to-Multiple-Point Circuit Roots Dialog Box

> ▶ If the circuit names do not appear immediately in the Circuit Root Name list box, insert the cursor in the blank Search Circuit Root by Name field and press Return. This action will display a list of configured circuits.

2. Select the Point-to-Multipoint circuit root. To search for a circuit root name, use the Search by Name field to enter wild-card characters as follows:
   - Use an * to match any number of characters
   - Use a ? to match a single character
   - Type * to match the * character
   - Type \? to match the ? character
   - Type \\ to match the \ character

   After you select the circuit root name, a list of circuit leaves associated with the root appears in the lower left corner of the dialog box.

3. Select a circuit leaf. Status information on the leaf, as well as fail reason and path information, appear to the right of the list.

   Table 13-12 describes the buttons on the dialog box and Table 13-13 describes the fields on the dialog box.

Table 13-12. Show All Point-to-Multiple-Point Circuit Root Buttons

Button	Function
Accounting	Accesses the accounting functions for a PVC. For more information, see the *NavisXtend Accounting Server Administrator's Guide.*
Statistics	Displays the summary statistics for the selected circuit.
NDC Statistics	Displays the NDC statistics for the selected circuit. For more information on NDC statistics, see "Viewing NTM and NDC Statistics" on page 13-30.
NDC Thresholds	Displays the configured NDC thresholds for the circuit. For more information on NDC thresholds, see "Viewing NTM and NDC Statistics" on page 13-30.
VPN/Customer	Displays a dialog box that allows you to provision a VPN for the point-to-multipoint circuit. You must be logged on to NavisCore in order to access this dialog box. See the *NavisCore ATM Configuration Guide* for more information on provisioning VPNs.
Close	Exits the dialog box.

Table 13-13. ATM Point-to-Multipoint Circuit Fields

Field	Displays...
Circuit Root Information	
Circuit Root Name	The name of the circuit root.
in Switch	The name of the switch where the circuit root resides.
Slot	The number of the slot where the IOM that the circuit root uses is installed.
PP	The number of the physical port on the IOM that the circuit root uses.
Inf	The internal interface number assigned to the circuit root.
VPI/VCI	The VPI and VCI assigned to the circuit root.
Class of Service	The QoS assigned to the circuit root (e.g., CBR).
Reroute Balance	One of the following: *Enabled* (the default) – Switch tuning parameters take effect. *Disabled* – Switch tuning parameters are ignored for the circuit.
Circuit Priority	The forward and reverse circuit priority, where *1* is highest priority, *2* is medium priority, *3* is low priority, and *4* is lowest priority. This field applies to point-to-multipoint circuits with a QoS class of VBR-RT or VBR-NRT only.
Private Net Overflow	Displays “Public” if the customer is allowed to use a public trunk in the event of overflow or trunk failure. Displays “Restrict” if the customer is restricted to its own VPN trunks during overflow or trunk failure.
VPN Name	The VPN name for the circuit (if applicable) or *Public* if the circuit is not reserved for a VPN.
Customer Name	The customer name for the selected circuit (if applicable). Otherwise, the field displays *Public*.
CDV Tolerance (microsec)	The CDV tolerance. CDV variation measures the average variation in delay between one cell and the next. Valid values are between 1 - 65535 µs. The default is 600 µs.
Circuit Type	The circuit type, either a VPC or VCC.
ATM Traffic Descriptor	The ATM traffic descriptor and associated parameters assigned to the circuit root. See Table 13-7 on page 13-14 for more information on traffic descriptors.

Table 13-13. ATM Point-to-Multipoint Circuit Fields (Continued)

Field	Displays...
FCP Discard (CBX 500 FCP Only)	One of the following values: *CLP1* – For UBR, ABR, and VBR-NRT circuits, the ATM FCP discards each cell with CLP set to 1 that causes the circuit queue to exceed the discard thresholds. This flow control technique is also known as “Selective Discard.” *EPD* – For UBR, ABR, and VBR-NRT circuits, the FCP performs EPD. If a cell causes the queue for a circuit to exceed the discard thresholds, the circuit enters the EPD state. This means that the cells in the current packet are admitted to the queue. However, when the end of the current packet is detected, all of the cells in the next packet are discarded.
Circuit Leaf Information	
in Switch	The switch that is connected to the circuit root by the leaf.
Slot	The number of the slot where the IOM that the leaf uses is installed.
PP	The number of the physical port on the IOM that the leaf uses.
Inf	The internal interface number assigned to the leaf.
VPI/VCI	The VPI and VCI assigned to the leaf.
Admin Status	One of the following: *Up* – The administrative setting of the circuit is up. *Down* – The administrative setting of the circuit is down.
Oper Status	The operational status of the connection between the leaf and the root. There are four possible values: *Active* – The connection is operational between the two endpoints. *Inactive* – The connection is not operational between the two endpoints. *Invalid* – The connection configuration is not contained within the calling node. *Unknown* – The calling node did not respond to the NMS request for the status of this connection.
Fail Reason	The reason a selected circuit failed (if any). See Table 13-3 on page 13-6 for more information.
Actual Path	The path traversed by the root-to-leaf connection.

4. Choose Statistics to display summary statistics for the root-to-leaf connection. The Point-to-Multipoint Circuit Statistics dialog box appears (see Figure 13-11).

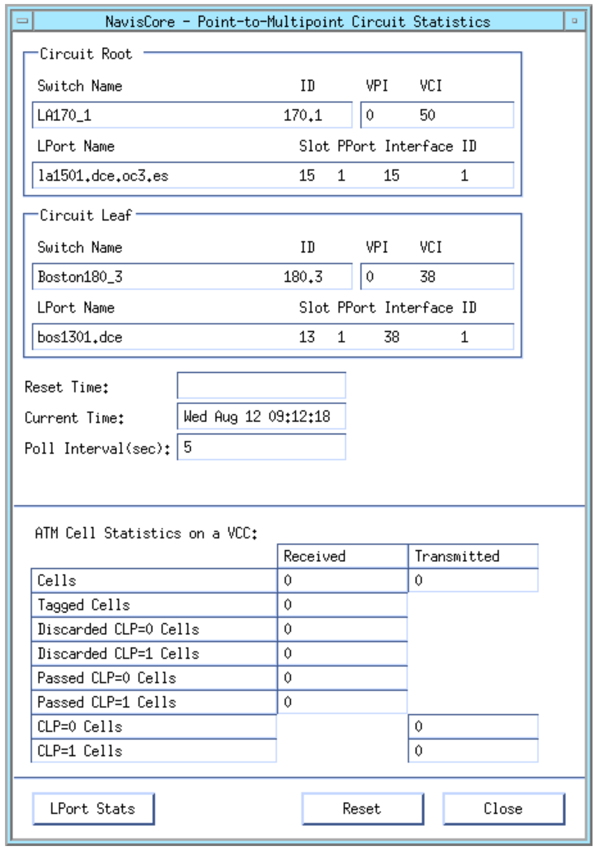


Figure 13-11. Point-to-Multipoint Circuit Statistics Dialog Box

This dialog box displays ATM cell statistics for a Point-to-Multipoint Circuit (transmitted and received data for each circuit endpoint). Table 13-14 describes the statistics fields.

Table 13-14. Point-to-Multipoint Circuit Statistics

Statistic	Description
Circuit Root	
Switch Name and ID	The name and number of the switch associated with the circuit root.
VPI	The VPI associated with the circuit root.
VCI	The VCI associated with the circuit root.
LPort Name	The name of the logical port associated with the circuit root.
Slot	The slot number of the IOM used by the logical port.
PPort	The number of the physical port to which the logical port is mapped.

Table 13-14. Point-to-Multipoint Circuit Statistics (Continued)

Statistic	Description
Interface	The logical port's internal interface number.
ID	The logical port's ID.
Circuit Leaf	
Switch Name and ID	The name and number of the switch associated with the circuit leaf.
VPI	The VPI associated with the circuit leaf.
VCI	The VCI associated with the circuit leaf.
LPort Name	The name of the logical port associated with the circuit leaf.
Slot	The slot number of the IOM used by the logical port.
PPort	The number of the physical port to which the logical port is mapped.
Interface	The logical port's internal interface number.
ID	The logical port's ID.
Time Information	
Reset Time	The time of the last reset of the selected switch.
Current Time	The current system time.
Poll Interval (sec)	The time interval for the collection of statistical data.
ATM Cell Statistics	
Cells	The total number of cells that were received and transmitted.
Tagged Cells	The total number of CLP=0 cells that were tagged as CLP=1 cells. Cells are tagged if they do not conform to the defined traffic descriptor for the circuit. *Note: Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells Fields indicate that either the source may need to slow transmission or that you need to reconfigure the traffic descriptors to reflect the source speed.*
Discarded CLP=0 Cells	The total number of received CLP=0 cells that are dropped because the cell violates the defined traffic descriptor. *Note: Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells Fields indicate that either the source may need to slow transmission or that you need to reconfigure the traffic descriptors to reflect the source speed.*

Table 13-14. Point-to-Multipoint Circuit Statistics (Continued)

Statistic	Description
Discarded CLP=1 Cells	The total number of CLP=1 cells that are discarded because the cells violate the defined traffic descriptor. *Note: Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells Fields indicate that either the source may need to slow transmission or that you need to reconfigure the traffic descriptors to reflect the source speed.*
Passed CLP=0 Cells	The total number of received CLP=0 cells that were passed for transmission.
Passed CLP=1 Cells	The total number of CLP=1 cells received at the port. This does not include CLP=0 cells that were received and then tagged at CLP=1 cells because of a traffic descriptor violation (they were counted as tagged cells).
CLP=0 Cells	The number of CLP=0 cells that were transmitted.
CLP=1 Cells	The number of cells that were tagged as CLP=1 and transmitted.

If one leaf of a point-to-multipoint connection indicates problems, check the other leaves of the connection. If the problems only exist on one leaf, check the configuration for that leaf.

Viewing NTM and NDC Statistics

This section describes how to configure and use Network Traffic Management (NTM) and Network Data Collection (NDC) on the Ascend switch. NTM and NDC provide you with statistics on point-to-point PVC and point-to-multipoint PVC traffic. Ascend has based the functional requirements for NTM and NDC on the Bellcore GR-1248 specification [GR1248].

NTM and NDC are disabled by default. To enable NTM and NDC, you first configure the NTM congestion thresholds for the “feeder” logical port. The feeder port can be any UNI, Direct trunk, or NNI logical port. Then, you set the NDC thresholds on a per-PVC basis. You can then monitor the NTM and NDC data that the logical port and PVC collect.

You can enable the NTM and NDC functions when you first configure your switch, or you can take the logical port/PVCs offline to enable these functions once you establish a basic switch-to-NMS configuration.

About Network Traffic Management

The purpose of NTM is to improve PVC traffic performance during overloads and failures in the network. NTM provides the following functions:

Measures of Congestion (MOC) — Defined at the ATM level based on percentage of cell loss.

NTM surveillance measurements — Used to detect overloads based on MOCs.

NTM control functions — Used to regulate/reroute the traffic flow during overloads.

Measures of Congestion

NTM applies a MOC to all congestable ATM modules. A congestable ATM module is any entity within an ATM Network Element (ATM NE) that can experience traffic congestion. The Ascend switch MOC is based on the count of CLP=0+1 cells discarded due to congestion in the output process. This count is sampled at each feeder logical port every 20 ms.

To prevent traffic bursts from corrupting the measurement, a MOC is subject to a smoothing algorithm that averages the congestion measurement over a period of time. The smoothed MOC is subject to four congestion thresholds (CT_0-CT_3), which you define for the logical port. The thresholds default to zero, which prevents the accumulation of congestion statistics. CT_3 is designated as the severe congestion threshold, and CT_0 is designated as the severe congestion abatement threshold. The CT_1 – CT_3 thresholds define four corresponding machine congestion levels, MC_0 – MC_3.

NTM Surveillance Measurements

The NTM surveillance measurements are based on 5-minute intervals. The timestamp of the counts corresponds to the end of the 5-minute interval.

For each logical port, the following counts are maintained for the 5-minute period:

- Total number of discarded CLP=0+1 cells.
- For each MC_0 - MC_3 level, the number of 20-ms periods spent in that level (from 0 to 15,000).
- For each MC_0 - MC_3 level, the number of times (based on 20-ms sampling) this level was entered (from 0 to 7,500). This includes transitions from both the higher and lower levels.

For each logical port, NavisCore provides a variety of NTM statistics, including the current plus three 5-minute history counts, as well as the timestamps for the history counts and the time elapsed (measured in seconds) in the current 5-minute period. The timestamps use the Universal Coordinated Time (UCT) available on the switch and have a 1-second resolution.

NTM State Change Notifications

When the smoothed MOC exceeds CT_3 and stays above CT_0 for the specified time interval (T), an SNMP trap is issued to the NMS. Once this first trap is sent, when the smoothed MOC falls below CT_0, another SNMP trap is sent. The interval T defaults to 30 seconds. Traps are issued within 5 seconds of the respective event detection.

NTM Control Functions

Only automatic NTM control functions are used to alleviate congestion. The NMS is not used to specify alternate routes. Currently, the hardware output process implements selective cell discards without software intervention.

About Network Data Collection

You configure the NDC measurements to detect any violation of PVC service subscription parameters and establish trends in network traffic patterns and loads. Scheduled measurements are taken on a regular basis as soon as the ATM NE is put into service. The measurements monitor the usage and health of the network.

Ascend switches support NDC scheduled measurements for up to 360 simultaneously monitored circuits per IOM.

For each feeder port and PVC, NavisCore provides a variety of NDC statistics including:

- The current plus two 15-minute history counts.
- The timestamps for the history counts (taken at the end of respective 15-minute periods). The timestamps use the Universal Coordinated Time (UCT) available on the switch and have a 1-second resolution.
- The time elapsed in the current 15-minute period.

There are three types of NDC scheduled measurements:

Traffic load measurements — Count the number of incoming/outgoing cells on a per-interface and per-VC basis.

UPC/NPC disagreement measurements — Collect the number of cells discarded due to UPC/NPC violations on a per-VC basis.

Traffic load and congestion measurements — Count the cells processed and discarded by a congestable ATM NE module, respectively. These counts do not include cells discarded due to UPC/NPC disagreements.

Traffic Load Measurements

The traffic load measurements count all NDC-valid cells. These are all user+OAM cells submitted to UPC/NPC before policing actions occur. Traffic load measurements maintain a count of the number of incoming/outgoing CLP=0+1 user+OAM cells in a 15-minute period for all UNI and NNI logical ports.

For the PVC endpoint you select, these measurements also maintain a count of the following user/OAM cells at the ingress/egress node in a 15-minute period:

- Number of incoming CLP=0+1 cells
- Number of outgoing CLP=0+1 cells

UPC/NPC Disagreement Measurements

The UPC/NPC disagreement measurements count the number of cells the network discards due to peak cell rate violation at the UNI (UPC) and at ingress VC at B-ICI (NPC). Two counts of incoming cells that are discarded due to traffic descriptor violations are collected on a per-VC basis:

- Number of incoming discarded CLP=0+1 cells.
- Number of incoming discarded high-priority (CLP=0) cells, including cells tagged as CLP=1 and then dropped; performed only if the ATM NE supports loss priority.

  In these two cases, NDC measurements count both the user and OAM cells. These measurements are applied to selected PVC endpoints.

  If the ATM NE implements cell tagging, NDC measurements count the number of CLP=0 cells that are tagged as CLP=1 cells.

Traffic Load and Congestion Measurements

The NDC MOC is based on the number of CLP=0+1 cells discarded per-port. The sampling period is 20 ms, same as for NTM. The NDC uses the same congestion thresholds CT_1 - CT_3, and consequently the same machine congestion levels MC_0 - MC_3 as defined for NTM. This enables a simple accumulation of the 5-minute NTM values to provide the 15-minute value.

The following counts of user+OAM cells per port are maintained in the 15-minute period:

- Number of discarded CLP=0+1 cells.
- For each MC_0 - MC_3 level, number of 20 ms periods spent in that level (from 0 to 45,000).
- For each MC_0 - MC_3 level, number of times (based on 20 ms sampling) this level is entered (from 0 to 22,500), including transitions from both the higher and lower levels.

Configuring NTM Attributes for a Logical Port

To define the NTM attributes for a feeder logical port:

1. From the network map, select the appropriate switch object.
2. From the Misc menu, select NavisCore ⇒ Logon.
3. Enter the Operator password.
4. From the Administer menu, select Ascend Parameters ⇒ Set Parameters to access the Switch Back Panel dialog box.
5. Double-click on the physical port that supports ATM traffic to view the Set ATM Physical Port Attributes dialog box.
6. Choose Logical Port to access the Set All Logical Ports in PPort dialog box.
7. Select the feeder logical port and choose Modify. The Modify Logical Port Type dialog box appears.
8. Choose OK. The Modify Logical Port dialog box reappears.
9. Choose Options ⇒ NTM Parameters.
10. Choose Set. The NTM Congestion Thresholds dialog box appears (see Figure 13-12).

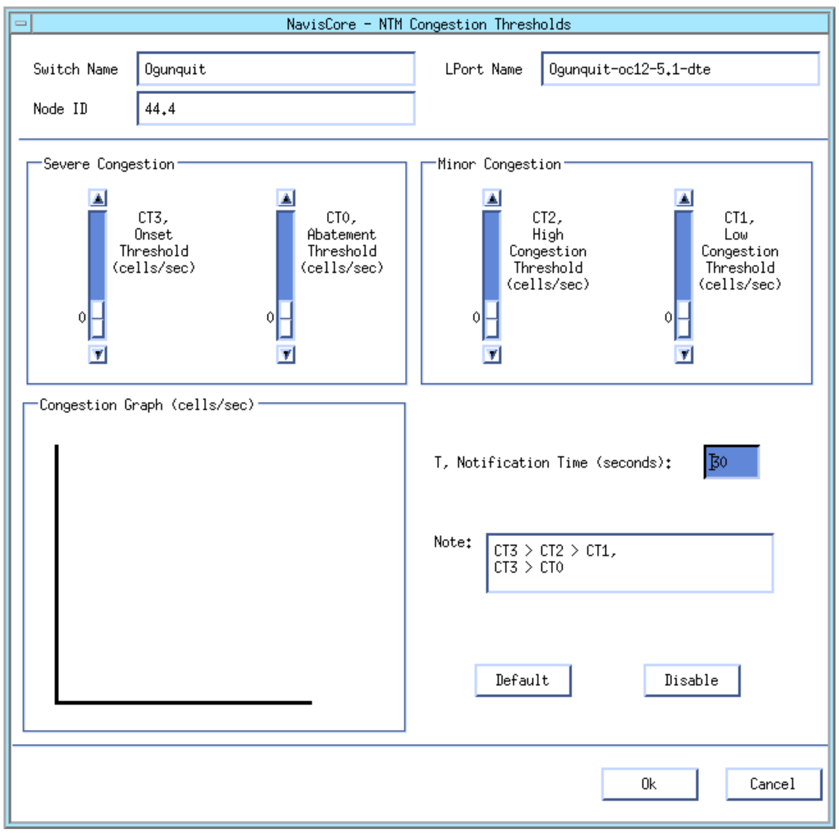


Figure 13-12. NTM Congestion Thresholds Dialog Box

11. To use the default NTM settings, choose Default. The defaults vary with respect to the IOM. Use the scroll bars or arrows to decrease the current settings to make this logical port more sensitive to congestion or increase these values to make it less sensitive.

    If the congestion level on this logical port exceeds the CT3 setting, and stays above the CT0 setting for at least 30 seconds, the port generates a trap. When the congestion level returns to the CT0 level for the specified time period, a second trap is generated.

12. When you finish setting congestion thresholds, choose OK.

Viewing NTM Parameters

To view NTM parameters:

1. From the Show All Logical Ports dialog box (Figure 6-1 on page 6-2), select Options ⇒ NTM Parameters.
2. Choose View. A dialog box similar to the NTM Congestion Thresholds dialog box appears (Figure 13-12 on page 13-34). The dialog box displays all of the NTM parameters.

   If the congestion level on this logical port exceeds the CT3 setting and stays above the CT0 setting for at least 30 seconds, the port generates a trap. When the congestion level returns to the CT0 level for the specified time period, a second trap is generated.

3. When you finish viewing NTM parameters, choose Close.

Viewing NTM Logical Port Statistics

To view NTM logical port statistics:

1. From the Show All Logical Ports dialog box (Figure 6-1 on page 6-2), select Options ⇒ NTM Statistics.
2. Choose View. The NTM Logical Port Data dialog box appears (see Figure 13-13).

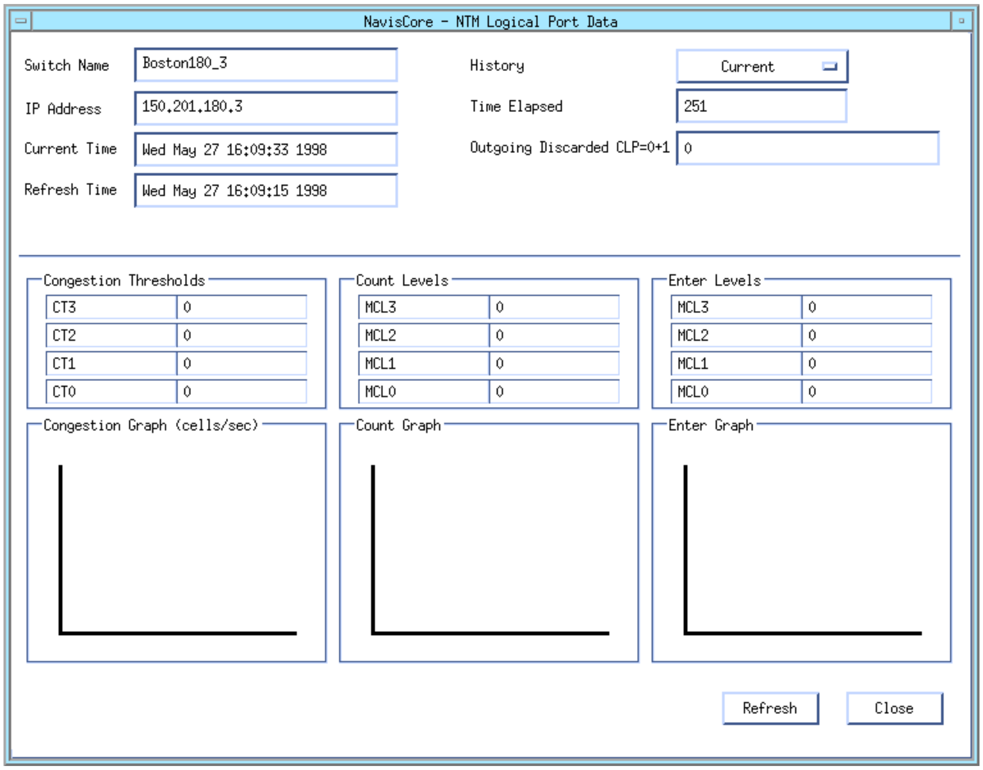


Figure 13-13. NTM Logical Port Data Dialog Box

The NTM Logical Port Data dialog box tracks the NTM statistics, including the number of outgoing discarded CLP=0+1 cells, and displays the following:

History — The current NTM data or data from three previous 5-minute intervals.

Time Elapsed/Timestamp — The seconds elapsed in the current time period. For a previous 5-minute interval, this field displays the UTC date and time.

This dialog box displays congestion thresholds and statistics in both text and color graphs, as follows:

Table 13-15. Congestion Thresholds and Statistics Color Key

Statistic	Color
CT3/MC3	Red
CT2/MC2	Orange
CT1/MC1	Yellow
CT0/MC0	Green

3. Choose Refresh to update these statistics.
4. Choose Close to return to the Show All Logical Ports dialog box.

Viewing NDC Logical Port Statistics

To view NDC logical port statistics:

1. From the Show All Logical Ports dialog box (Figure 6-1 on page 6-2), select Options ⇒ NDC Statistics.
2. Choose View. The NDC Logical Port Data dialog box appears (see Figure 13-14).

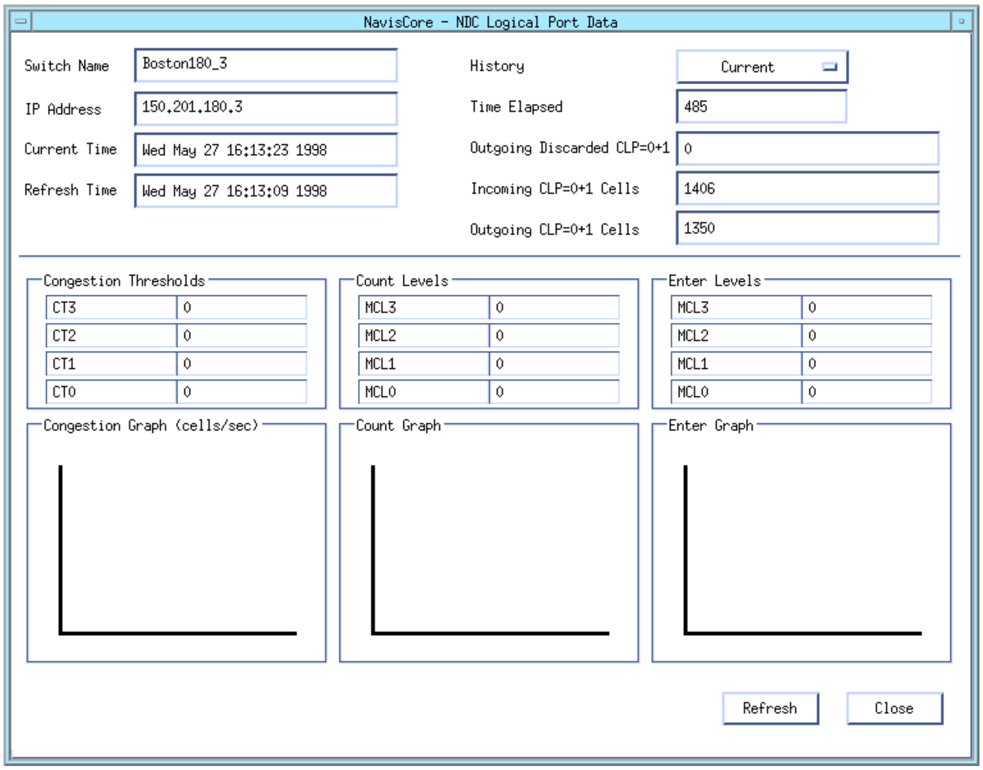


Figure 13-14. NDC Logical Port Data Dialog Box

The NDC Logical Port Data dialog box tracks the NDC statistics, including the number of:

- Outgoing discarded CLP=0+1 cells
- Incoming CLP=0+1 cells
- Outgoing CLP=0+1 cells

Use the History option menu to view current NDC data or data from previous 15-minute intervals. The Time Elapsed field displays the minutes elapsed in the current time period.

This dialog box displays congestion thresholds and statistics in both text and color graphs. The graphs use the same color coding scheme as described in Table 13-15 on page 13-36.

3. Choose the Refresh to update these statistics.
4. Choose Close to return to the Show All Logical Ports dialog box.

Configuring NDC Attributes for a Point-to-Point ATM PVC

You can configure NDC thresholds and attributes for both logical port endpoints on a point-to-point ATM PVC. To configure the NDC thresholds and attributes:

1. From the Administer menu, select Ascend Parameters ⇒ Set All Circuits ⇒ Point-to-Point. The Set All PVCs dialog box appears.
2. Select the ATM PVC on which you want to configure NDC thresholds.
3. Choose Modify. The Modify End Logical Ports dialog box appears.
4. Choose OK. The Modify PVC dialog box appears.
5. Choose Set NDC Attributes. The NDC attributes fields appear (see Figure 13-15).

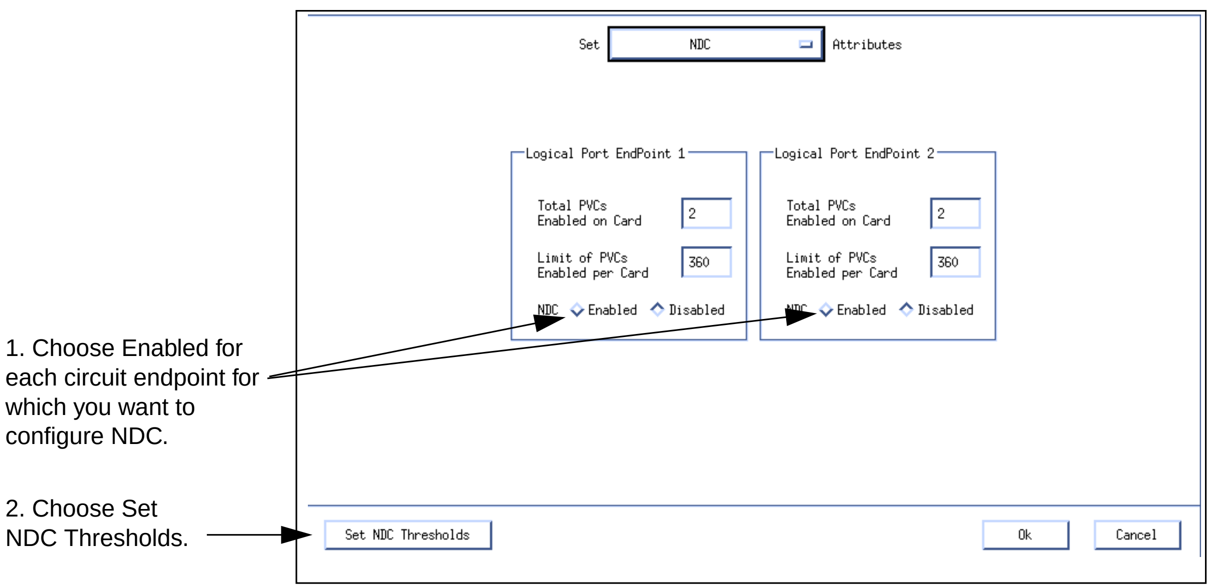


Figure 13-15. Setting NDC Attributes

For each logical port endpoint, the following NDC attributes appear:

Total PVCs Enabled on Card — The current number of NDC-enabled endpoints for the IOM associated with the selected logical port.

Limit of PVCs Enabled per Card — The limit (360) of NDC-enabled endpoints you can configure for the IOM associated with the selected logical port.

NDC — Choose Enabled to collect NDC statistics for this circuit endpoint. The default is Disabled.

6. Modify the parameters for each endpoint as necessary.
7. Choose Set NDC Thresholds. The NDC Thresholds dialog box appears (see Figure 13-16).

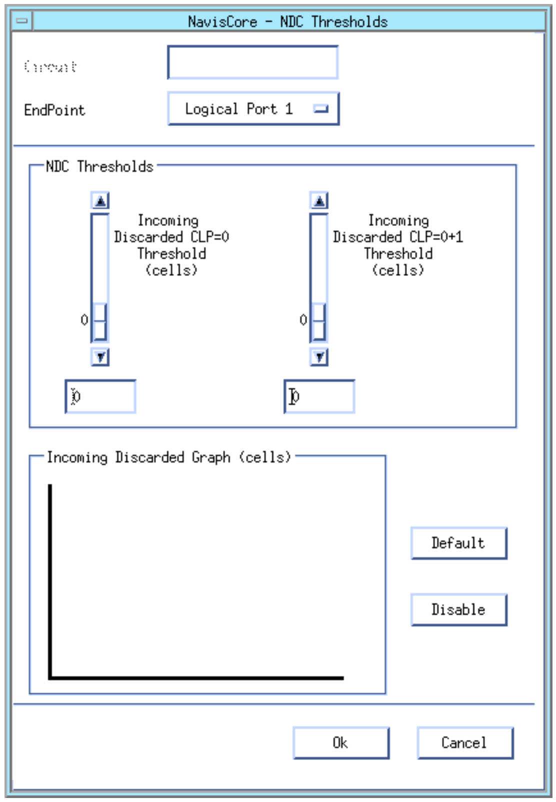


Figure 13-16. NDC Thresholds Dialog Box (Point-to-Point)

8. Skip this step if you did not enable both logical port endpoints for NDC (Figure 13-15 on page 13-38). Select a logical port endpoint (Logical Port 1 or Logical Port 2) in the EndPoint option menu.
9. Configure NDC thresholds. The thresholds apply to the number of incoming CLP=0 and CLP=0+1 cells that have been discarded. If the number of discarded cells for this endpoint exceeds the value you configure, a trap is generated.

   Choose Default to use the default threshold. Or, to override the default:

   - Use the scroll bar and arrows.
   - Type a cell value below each scroll bar and press Return.
10. Choose OK to set these thresholds. The Modify PVCs dialog box appears.
11. If you enabled both logical port endpoints for NDC, repeat the previous four steps to configure the other logical port endpoint.
12. Choose OK to return to the Set All PVCs dialog box.

Configuring NDC Attributes for a Point-to-Multipoint ATM PVC

You can only configure NDC attributes for a point-to-multipoint circuit when you initially define a circuit root. Once you create the root, you *cannot* enable or modify the NDC attributes.

The following steps describe how to configure the originating point (circuit root) for an ATM point-to-multipoint circuit, and how to configure NDC attributes for the circuit. For more information about defining an ATM circuit root, see the *NavisCore ATM Configuration Guide*.

1. Select the switch from the network map.

2. From the Administer menu, select Ascend Parameters ⇒ Set All Circuits ⇒ Point-to-Multipoint Circuits. The Set All Point-to-Multiple-Point Circuit Roots dialog box appears.

> ► If the circuit root names do not appear immediately in the Circuit Root Name list box, insert the cursor in the blank Search Circuit Root by Name field and press Return. This action will display a list of configured circuits.

The *Defined Point-to-Multiple-Point Circuit Root Records* list box at the top of the screen lists any existing point-to-multipoint circuit roots. The *Corresponding Point-to-Multiple-Point Circuit Leafs* list box lists any existing circuit leafs (endpoints) for the selected circuit root.

3. Choose Add. The Add Point-to-Multiple-Point Circuit Root (Select LPort) dialog box appears (see Figure 13-17).

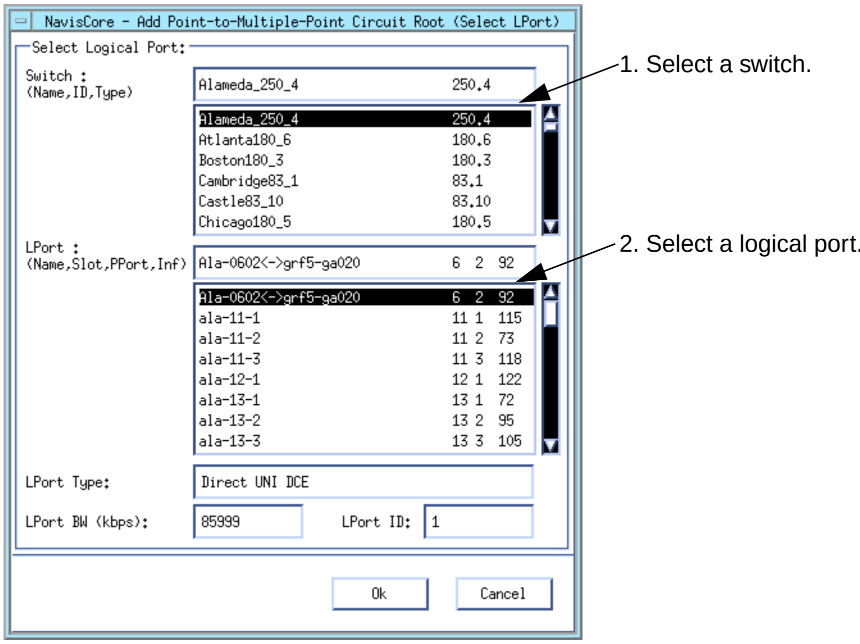


Figure 13-17. Add Point-to-Multiple-Point Circuit Root (Select LPort) Dialog Box

4. In the Switch list box, select the switch on which the originating point of the circuit will reside. The list contains the switch name and switch ID for all switches the NMS can currently access.
5. In the LPort list box, select the logical port on which the originating point of the circuit will reside. The dialog box displays the logical port name, slot ID, physical port number, and MIB interface number (Inf) for all logical ports on the selected switch.
6. Choose OK to display the Add Point-to-Multiple-Point Circuit Root dialog box (see Figure 13-18).

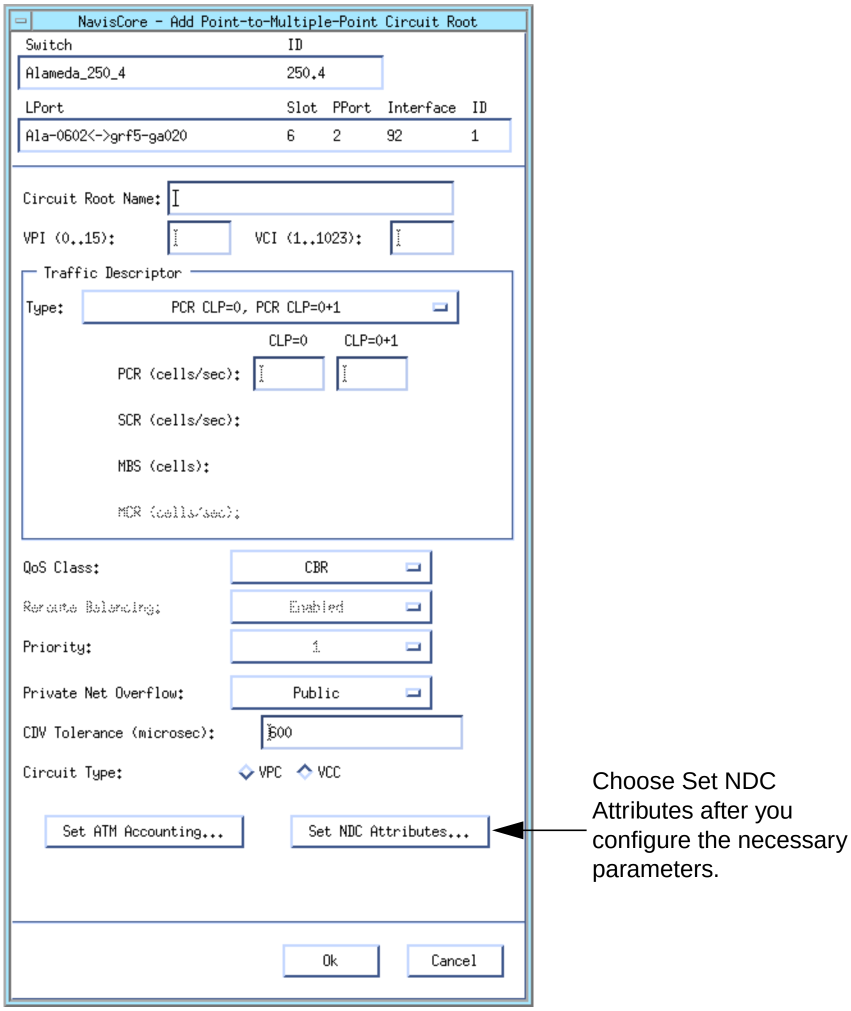


Figure 13-18. Add Point-to-Multiple-Point Circuit Root Dialog Box

7. In the Circuit Root Name field, enter an alphanumeric name for the circuit root.
8. In the VPI and VCI fields, enter the virtual path ID and virtual channel ID for this circuit root.
9. Configure the remaining parameters. For more information, see the *NavisCore ATM Configuration Guide*.
10. Choose Set NDC Attributes. The Set PMP NDC Attributes dialog box appears (see Figure 13-19).

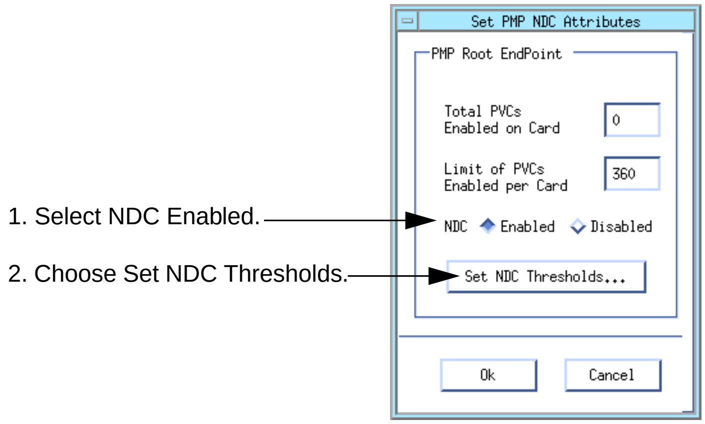


Figure 13-19. Set PMP NDC Attributes Dialog Box

The following NDC parameters appear:

Total PVCs Enabled on Card — The current number of NDC-enabled endpoints for the IOM associated with the selected logical port.

Limit of PVCs Enabled per Card — The limit (360) of NDC-enabled endpoints you can configure for the IOM associated with the selected logical port.

NDC — Choose Enabled to collect NDC statistics for the circuit. The default is Disabled.

11. Modify the parameters as necessary.

12. Choose Set NDC Thresholds. The NDC Thresholds dialog box appears (see Figure 13-20).

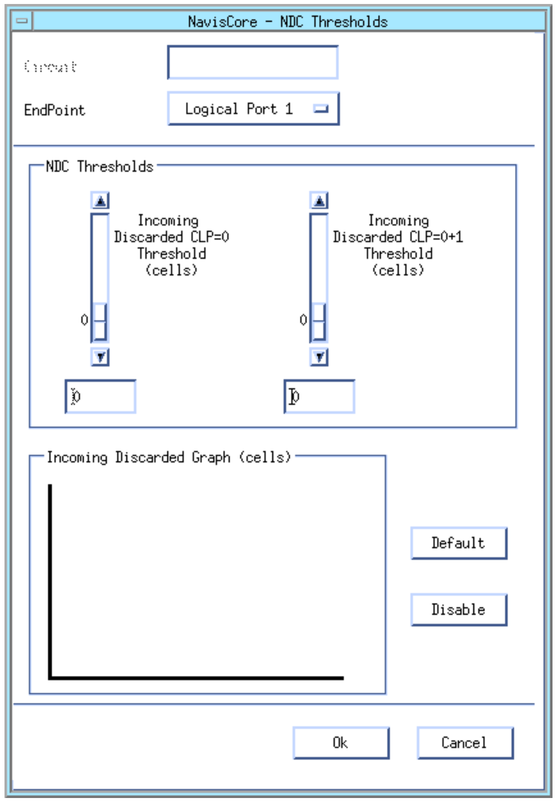


Figure 13-20. NDC Thresholds Dialog Box (Point-to-Multipoint)

13. Configure the NDC threshold. Choose Default to use the default threshold. Or, to override the default:

- Use the scroll bar and arrows.
- Type a cell value below each scroll bar and press Return.

These thresholds apply to the number of incoming CLP=0 and CLP=0+1 cells that have been discarded. If the number of discarded cells for this endpoint exceeds the value you configure, a trap is generated.

14. Choose OK to set these thresholds and return to the Set PMP NDC Attributes dialog box.

15. Choose OK to return to the Add Point-to-Multiple Point Circuit Root dialog box (Figure 13-18).

16. Choose OK to return to the Set All PMP Circuit Roots dialog box.

17. See the *NavisCore ATM Configuration Guide* to assign this point-to-multipoint circuit to a VPN and/or to continue configuring point-to-multipoint circuit leaves.

Viewing NDC PVC Thresholds

The NDC Thresholds function enables you to view NDC thresholds for either endpoint of a selected PVC. To view NDC thresholds:

1. From the Show All PVCs dialog box (Figure 13-1 on page 13-2), select the ATM PVC you want to view.
2. Choose NDC Thresholds. The NDC Thresholds dialog box appears (see Figure 13-21).

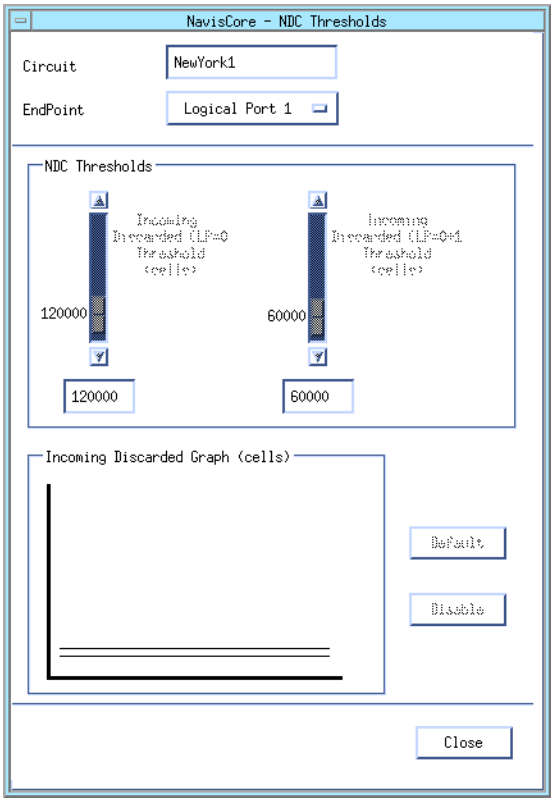


Figure 13-21. NDC Thresholds Dialog Box (View)

This dialog box displays the configured settings as well as a graph of discarded cells.

3. Choose Close to exit.

Viewing NDC PVC Data

The NDC Statistics function enables you to view NDC PVC statistics for either endpoint of the PVC you select. To view NDC PVC data:

1. From the Show All PVCs dialog box (see Figure 13-1 on page 13-2), select the ATM PVC you want to view.
2. Choose NDC Statistics. The NDC PVC Data dialog box appears (see Figure 13-22).

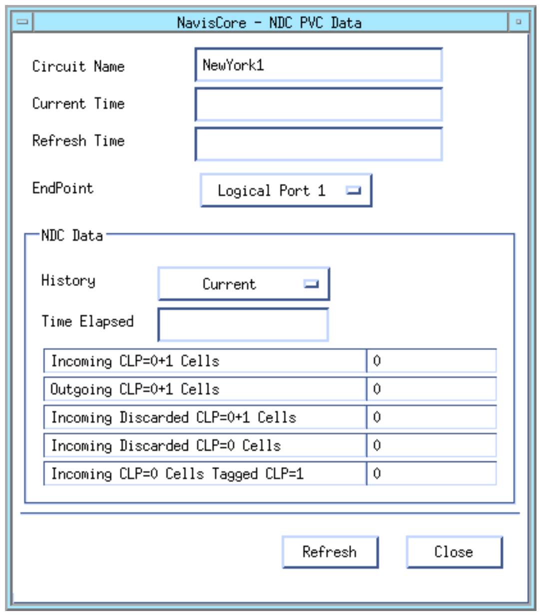


Figure 13-22. NDC PVC Data Dialog Box

For each logical port endpoint, this dialog box tracks the NDC PVC statistics, including the number of:

- Incoming CLP=0+1 cells
- Outgoing CLP=0+1 cells
- Incoming discarded CLP=0+1 cells
- Incoming discarded CLP=0 cells
- Incoming CLP=0 cells tagged CLP=1

Use the History option menu to view current NDC data or data from the two previous 15-minute intervals. The Time Elapsed field displays either the seconds elapsed in the current time period, or the UTC Timestamp for the specified 15-minute interval.

3. Choose Refresh to update these statistics.
4. Choose Close to return to the Show All PVCs dialog box.
5. Choose Close to return to the network map.

Viewing Soft PVCs

Soft PVCs have the characteristics of both ATM PVCs and ATM SVCs. Like an ATM PVC, a soft PVC is permanent once it is established. However, like an ATM SVC, the connection is established through signaling rather than administratively through network management. Soft PVCs can be used in either point-to-point or point-to-multipoint topologies.

There are two types of soft PVCs:

Soft Permanent Virtual Channel Connections (SPVCCs) — This type of soft PVC uses an ATM virtual channel connection (VCC).

Soft Permanent Virtual Path Connections (SPVPCs) — This type of soft PVC uses an ATM virtual path connection (VPC).

See the *Networking Services Technology Overview* for more information on VCCs and VPCs.

Viewing Point-to-Point SPVCs

To view point-to-point SPVC status and statistics:

1. From the Monitor menu, select Ascend Objects ⇒ Show All Soft PVCs ⇒ Point-to-Point. The Show All Point-to-Point SPVCs dialog box appears (see Figure 13-23).

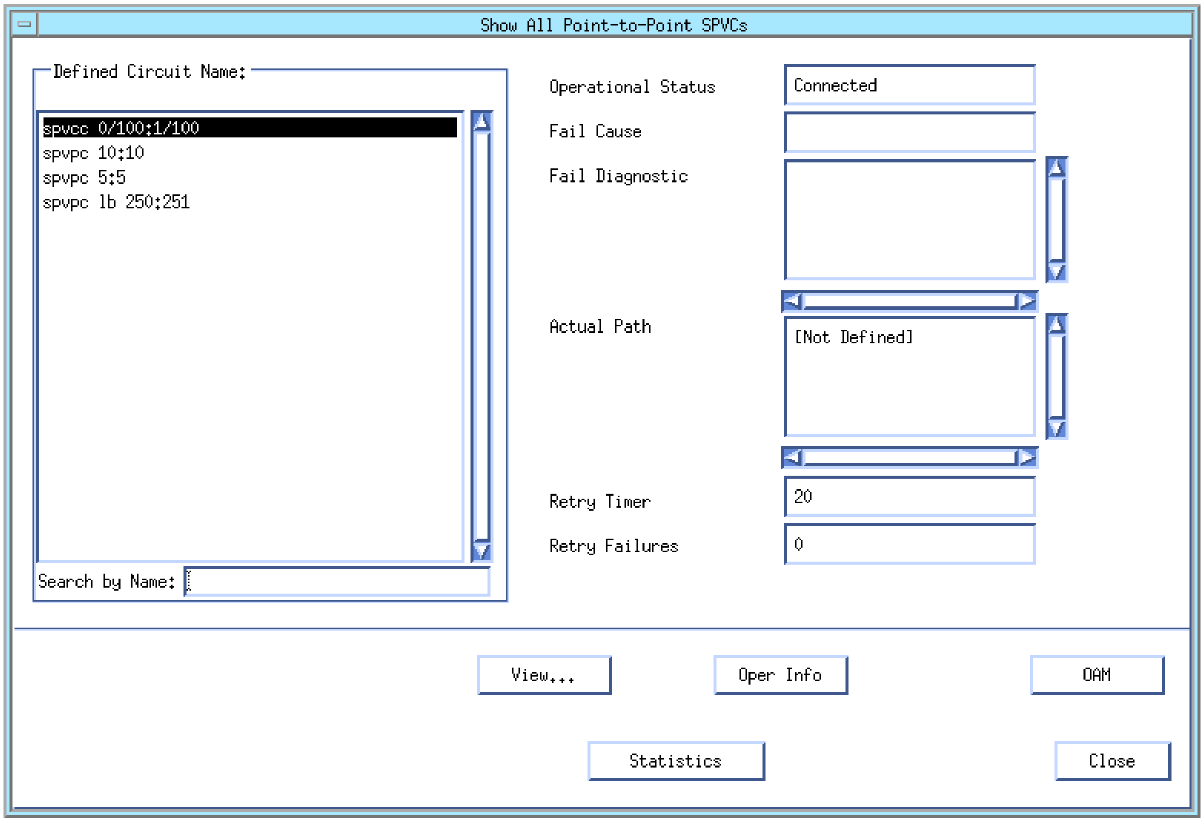


Figure 13-23. Show All Point-to-Point SPVCs Dialog Box

▶ If the circuit names do not appear immediately in the Defined Circuit Name list box, insert the cursor in the blank Search by Name field and press Return. This action will display a list of configured circuits.

2. Select the name of the circuit for which you want to retrieve status information. You can use the Search by Name field to enter wild-card characters.

- Use an * to match any number of characters
- Use a ? to match a single character
- Type * to match the * character
- Type \? to match the ? character
- Type \\ to match the \ character

Table 13-16 describes the buttons that appear on the Show All Point-to-Point SPVCs dialog box.

Table 13-16. Show All Point-to-Point SPVCs Buttons

Button	Function
View	Displays attributes for the selected circuit. See "Viewing Point-to-Point SPVC Attributes" for more information.
Oper Info	Updates field information.
OAM	Runs the Operations, Administration, and Management diagnostics for the selected circuit. See "Testing ATM Circuits" on page 13-90 for more information.
Statistics	Displays the summary statistics for the selected circuit, which are similar to SVC statistics. See Table 13-32 on page 13-85 for details.
Close	Closes the dialog box.

Table 13-17 describes the fields that appear on the Show All Point-to-Point SPVCs dialog box.

Table 13-17. Show All Point-to-Point SPVCs Fields

Field	Displays...
Defined Circuit Name	The name of the SPVC circuit.
Operational Status	One of the SPVC states: *Connected* – The SPVC has been successfully established. *Failed* – An attempt to establish the SPVC has failed. The SPVC is still active, and the switch will make another attempt to establish it. *Setup In Progress* – An attempt to establish the SPVC is in progress. *Other* – The SPVC is not active.
Fail Cause	The reason a selected circuit failed (if any). These causes are similar to the SVC failure causes. See Table E-1 on page E-2 for more information.
Fail Diagnostic	The value of the first eight bytes of diagnostic information from the cause field of the cause information element in the last release signaling message received for the SPVC.
Actual Path	The actual path that OSPF selected for this circuit to use to get to its destination.
Retry Timer	The current value of the retry timer, in seconds. When the retry timer reaches zero, the switch attempts to establish the SPVC.
Retry Failures	The number of failed attempts the switch has made to establish an SPVC since the last reset.

Viewing Point-to-Point SPVC Attributes

To view point-to-point SPVC attributes:

1. From the Show All Point-to-Point SPVCs dialog box (Figure 13-23 on page 13-48), select the point-to-point SPVC you want to view.
2. Choose View. The View Soft PVC dialog box appears (see Figure 13-24).

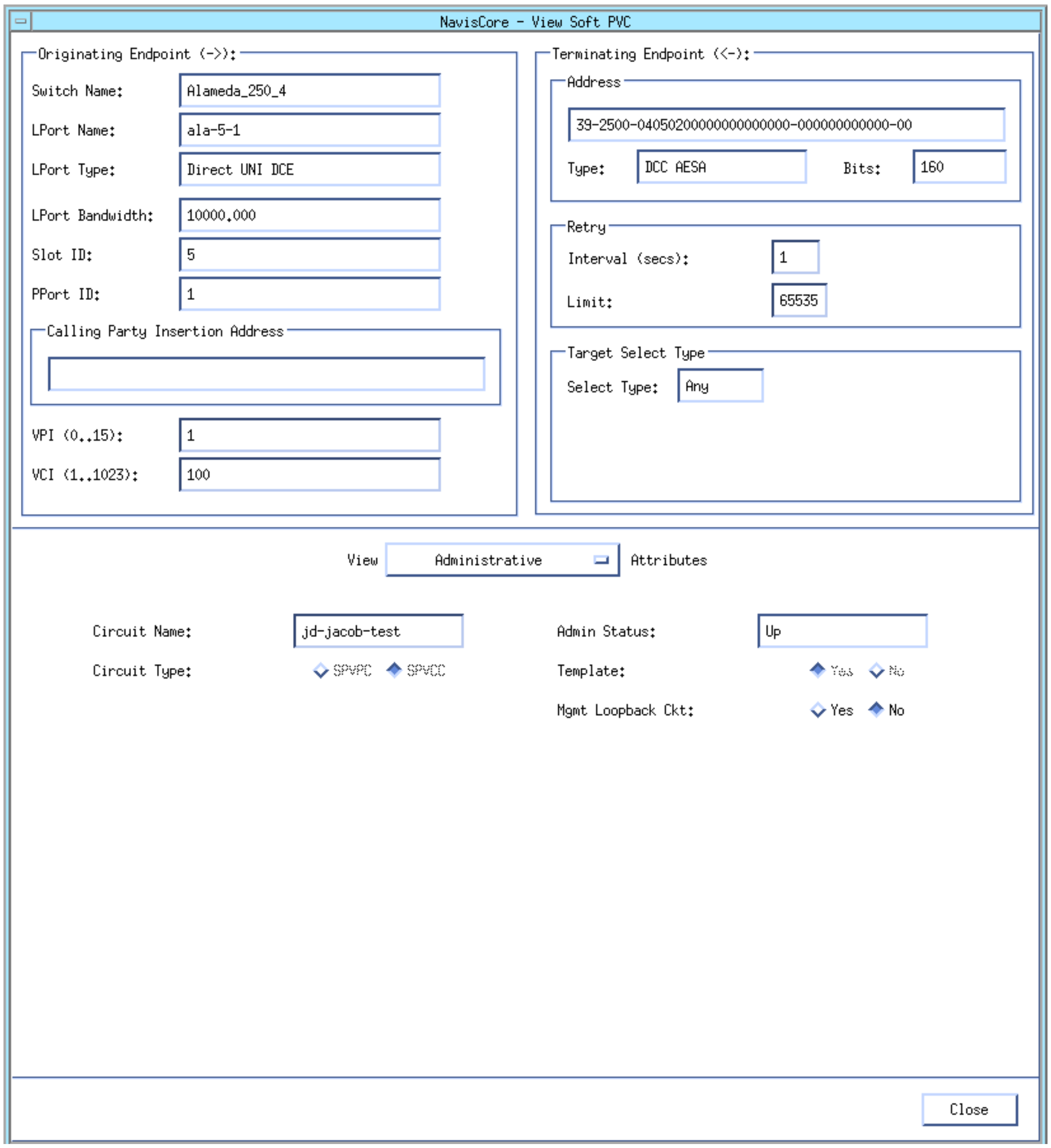


Figure 13-24. View Soft PVC Dialog Box

Table 13-18 describes the point-to-point SPVC attributes fields.

Table 13-18. Point-to-Point SPVCs Attributes Fields

Field	Displays...
Originating Endpoint	
Switch Name	The name of the switch where the SPVC originates.
LPort Name	The name of the logical port where the SPVC originates.
LPort Type	The type of logical port (e.g., Direct UNI DCE) where the SPVC originates.
LPort Bandwidth	The amount of bandwidth (in kilobits per second) configured for the originating logical port.
Slot ID	The number of the slot where the IOM associated with the originating logical port is installed.
PPort ID	The number of the physical port associated with the originating logical port.
Calling Party Insertion Address	The address that the originating logical port inserts into received packets if it receives a call with no address. To do this, the logical port must have its Insertion Mode SVC parameter set to either *Insert* or *Replace*. See the *NavisCore ATM Configuration Guide* for more information on SPVC addressing.
VPI	The VPI for the SPVC.
VCI (*SPVCCs only*)	The VCI for the SPVC.
Terminating Endpoint	
Address	The address of the terminating endpoint. See the *NavisCore ATM Configuration Guide* for more information on SPVC addressing.
Type	The type of address.
Bits	The number of bits allocated for the address.
Interval	The number of seconds the originating endpoint waits before trying to reestablish a connection. The originating endpoint makes several attempts to connect to the terminating endpoint.
Limit	The number of times the originating endpoint tries to connect to the terminating endpoint.

Table 13-18. Point-to-Point SPVCs Attributes Fields (Continued)

Field	Displays...
Select Type	One of the following: *Any* – The terminating endpoint uses any available VPI/VCI value. *Specified* – The terminating endpoint uses the VPI/VCI address you specify.
Administrative Attributes – Appear by default.	
Circuit Name	The name of the circuit
Circuit Type	The type of circuit (*SPVPC* or *SPVCC*).
Admin Status	The admin status of the circuit (*Up* or *Down*).
Is Template	One of the following: *Yes* – This circuit connection was defined as a template. *No* – This connection is not a template.
Mgmt Loopback Ckt	Not used.
Traffic Type Attributes – Select View Traffic Type Attributes to display the traffic type attributes fields.	
Traffic Descriptors	The traffic descriptors configured for the circuit.
Forward Traffic Descriptor	The traffic descriptor configured for the forward direction.
Reverse Traffic Descriptor	The traffic descriptor configured for the reverse direction.

Viewing Point-to-Multipoint SPVCs

To view point-to-multipoint SPVC status and statistics:

1. From the Monitor menu, select Ascend Objects ⇒ Show All Soft PVCs ⇒ Point-to-Multipoint. The Show All Point-to-Multipoint SPVCs dialog box appears (see Figure 13-25).

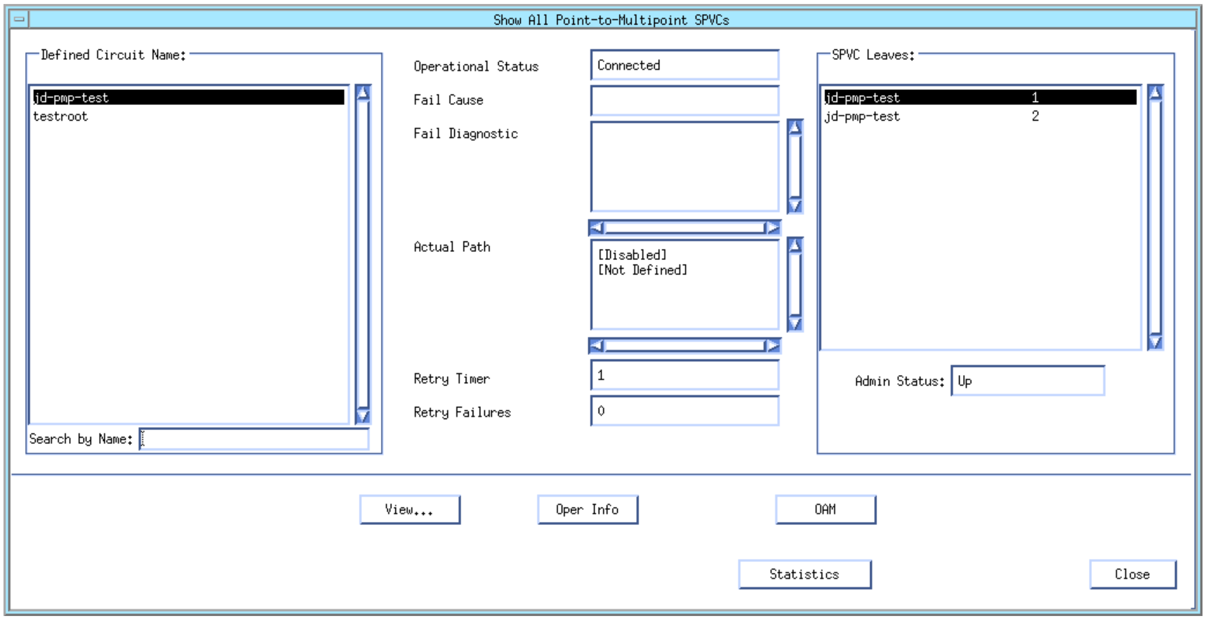


Figure 13-25. Show All Point-to-Multipoint SPVCs Dialog Box

> If the circuit names do not appear immediately in the Defined Circuit Name list box, insert the cursor in the blank Search by Name field and press Return. This action will display a list of configured circuits.

2. Select the name of the circuit for which you want to retrieve status information. You can use the Search by Name field to enter wild-card characters.

- Use an * to match any number of characters
- Use a ? to match a single character
- Type * to match the * character
- Type \? to match the ? character
- Type \\ to match the \ character

Table 13-19 describes the buttons that appear on the dialog box.

Table 13-19. Show All Point-to-Multipoint SPVCs Buttons

Button	Function
View	Displays attributes for the selected circuit. These attributes are the same as the attributes for point-to-point SPVCs. See Table 13-18 on page 13-51 for more information.
Oper Info	Updates field information.
Statistics	Displays the summary statistics for the selected circuit. The statistics displayed are similar to SVC circuit statistics. See Table 13-32 on page 13-85 for details.
Close	Closes the dialog box.

The fields that appear on the Show All Point-to-Multipoint SPVCs dialog box are the same as the fields on the Show All Point-to-Point SPVCs dialog box, except for the following fields:

SPVC Leaves — Each SPVC leaf associated with the circuit.

Admin Status — A value of *Up* or *Down* to indicate the admin status of the circuit.

See Table 13-17 on page 13-49 for descriptions of the other fields on the dialog box.

Viewing SPVCs as SVCs

Some SVC functions enable you to also view SPVC information. For example, the dialog box for viewing all failed SVC calls allows you to select SPVC logical ports and view historical information and detailed information on the failures of SPVCs associated with those ports. See “Viewing ATM SVC Failed Calls” on page 13-77 for more information.

Viewing ATM SVCs

This section describes how to monitor ATM SVCs in an Ascend network. You can check the status of configured SVC parameters and view statistics on SVC activity. For more information on ATM SVCs, see the *NavisCore ATM Configuration Guide*.

Viewing All Node Prefixes

Node prefixes apply to all logical ports on the switch and are used for routing aggregation. To view all node prefix formats on a switch:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Node Prefixes. The Show All Node Prefixes dialog box appears (see Figure 13-26).

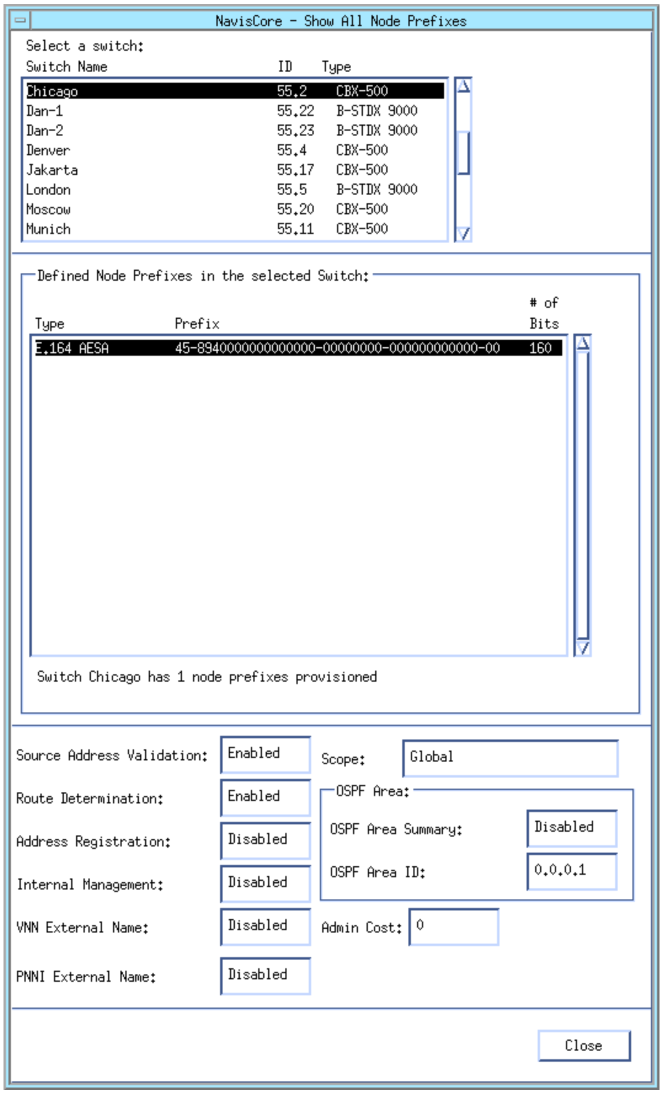


Figure 13-26. Show All Node Prefixes Dialog Box (ATM SVCs)

2. Select the switch whose node prefixes you want to view. The dialog box displays the defined node prefixes for this switch.
3. When you finish viewing the information, choose Close to return to the network map.

Table 13-20 describes the Show All Node Prefixes fields.

Table 13-20. Show All Node Prefixes Fields (ATM SVCs)

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch number used as the host assignment in the switch's internal IP address.
Type	The switch type (e.g., GX 550).
Defined Node Prefixes	
Type	Displays one of the following address formats: *E.164 (Native)* – Standard 1-15 digit ISDN number, which includes telephone numbers. *DCC AESA* – Data Country Code ATM End System Address, which identifies the country in which the address is registered. *ICD AESA* – International Country Designator ATM End System Address, which identifies the international organization to which the address applies. *E.164 AESA* – E.164 ATM End System Address, which encapsulates a standard 1-15 digit ISDN number, including telephone numbers. *Custom AESA* – ATM End System Address with customized octet structure and customized Authority and Format Identifier (AFI). *DCC Anycast AESA* – Data Country Code Anycast ATM End System Address. An ATM Anycast address identifies a functional group. *ICD Anycast AESA* – International Country Designator Anycast ATM End System Address. *E.164 Anycast AESA* – E.164 Anycast ATM End System Address.
Prefix	The configured node prefix.
# of Bits	The number of address bits that are checked during call screening and call routing.

Table 13-20. Show All Node Prefixes Fields (ATM SVCs) (Continued)

Field	Displays...
Source Address Validation	One of the following: *Enabled* – The prefix is used to validate the calling party address against the node prefix associated with the UNI logical port that receives the call setup message. *Disabled* – The prefix is not used to validate calling party addresses.
Route Determination	One of the following: *Enabled* – OSPF uses this node prefix for routing aggregation, and PVC/PVP termination is supported. *Disabled* – OSPF does not use this node prefix for routing aggregation determination.
Address Registration	One of the following: *Enabled* – The node prefix is used for Interim Local Management Interface (ILMI) address registration for all UNI-DCE “network-to-endsystem” logical ports that support ILMI. If the node prefix address type is AESA, the prefix must be 13 bytes (104 bits) long in order for Address Registration to be enabled. *Disabled* – The node prefix is not used for ILMI address registration for all UNI-DCE “network-to-endsystem” logical ports that support ILMI. If the node prefix address type is AESA, and the prefix is other than 13 bytes (104 bits) long, the Address Registration attribute is disabled.
Internal Management	One of the following: *Enabled* – The node prefix of the switch is to be used as the management base address (that is, as an addressable entity). The internal management base address identifies this node as an endpoint for internal SVC signaling. If enabled, the node prefix supplies the calling party address for management SPVCs, and can be used by NHRP (if supported). *Disabled* – The node prefix of the switch is not to be used as the management base address.
VNN External Name	One of the following: *Enabled* – The address (i.e., “name”) can be advertised within the Virtual Network Navigator (VNN) routing domain as an external name. An external name identifies a node that is reachable within another VNN routing domain. *Disabled* – The node is reachable from within its own routing domain only.
PNNI External Name	One of the following: *Enabled* – The address (i.e., “name”) can be advertised within the PNNI routing domain as an external name. An external name identifies a node that is reachable within another PNNI routing domain. *Disabled* – The node is reachable from within its own routing domain only.

Table 13-20. Show All Node Prefixes Fields (ATM SVCs) (Continued)

Field	Displays...
Scope	The organizational scope of the node prefix. The organizational scope determines the extent to which (i.e., how far up the routing hierarchy) an address may be advertised. Possible scopes include *Global*, *InterRegional*, *Regional*, *IntraCommunity*, *CommunityMinusOne*, *OrganizationPlusOne*, *IntraSite*, *SiteMinusOne*, *LocalNetworkPlusTwo*, *LocalNetworkPlusOne*, *LocalNetwork*.
OSPF Area Summary	One of the following: *Enabled* – The OSPF Area Summary attribute for this node prefix is enabled, allowing this node to be an area border router. If you enable this setting, you must configure an OSPF area ID. *Disabled* – The OSPF Area Summary attribute for this node prefix is disabled.
OSPF Area ID	The ID of the OSPF area, if one is configured. You configure an OSPF area ID if you enable the OSPF Area Summary setting.
Admin Cost	The administrative cost associated with the node prefix. When an SVC is created, if more than one node in the network is found with the same node prefix, the call is routed to the node that has the lowest administrative cost associated with the prefix.

Viewing All Port Prefixes

SVC port prefixes define how calls are routed to a logical port. To view all port prefixes defined for a selected logical port:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port Prefixes. The Show All Port Prefixes dialog box appears (see Figure 13-27).

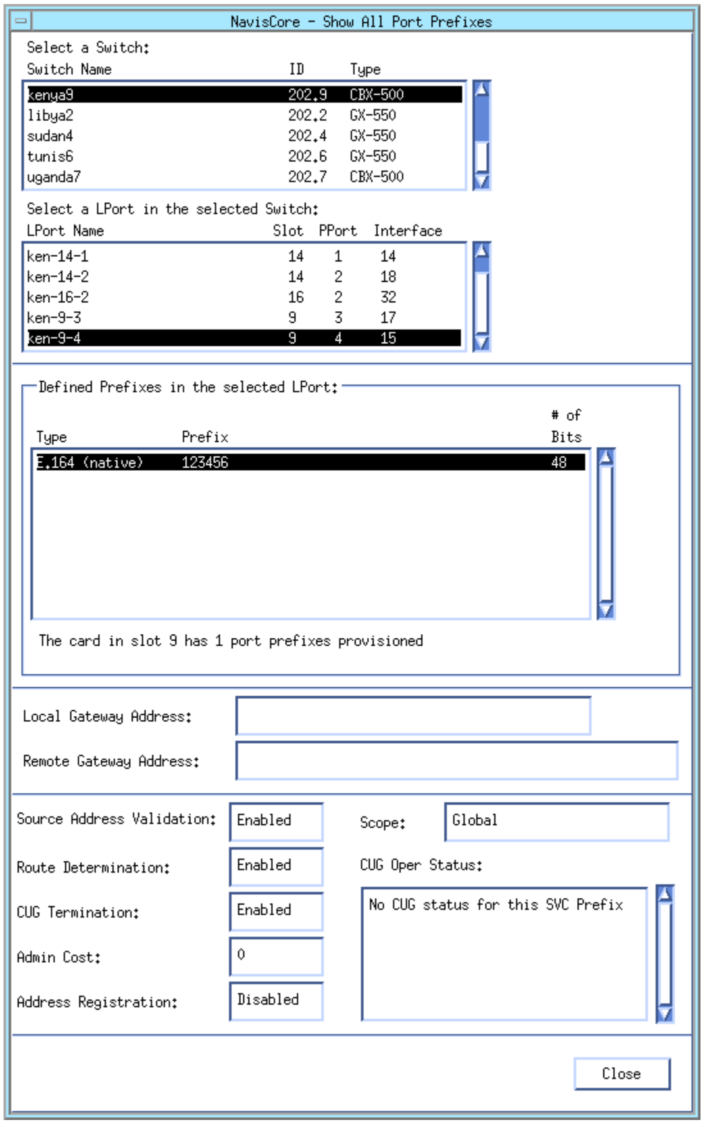


Figure 13-27. Show All Port Prefixes Dialog Box (ATM SVCs)

2. Select a switch.
3. Select a logical port. The dialog box displays the defined prefixes for the logical port, as well as the admin cost and local and remote gateway addresses for the logical port.
4. When you finish viewing the information, choose Close to return to the map.

Table 13-21 describes the Show All Port Prefix fields.

Table 13-21. Show All Port Prefix Fields (ATM SVCs)

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch number used as the host assignment in the switch's internal IP address.
Type	The switch type (e.g., GX 550).
Logical Port Information	
LPort Name	The name of the logical port associated with the prefix.
Slot	The slot number of the IOM used by the logical port.
PPort	The number of the physical port on which the logical port is configured.
Interface	The logical port's internal interface number.
Defined Port Prefixes	
Type	The configured SVC address format. See Table 13-20 on page 13-56 for a description of formats.
Prefix	The configured port prefix.
# of Bits	The number of address bits that are checked during call screening and call routing.
Local Gateway Address	The address of the local gateway, which is the gateway that is on the same side of the public network as the switch. This address is specified only for logical ports that provide network-to-network connections.
Remote Gateway Address	The address of the remote gateway, which is the gateway on the other side of the public network. This address is specified only for logical ports that provide network-to-network connections.
Source Address Validation	One of the following: *Enabled* – The port prefix is used to validate the calling party address against the port prefix associated with the UNI port which received the call setup message. *Disabled* – The port prefix is not used to validate calling party addresses.
Route Determination	One of the following: *Enabled* – OSPF uses the port prefix for route determination. *Disabled* – OSPF does not use the port prefix for route determination.

Table 13-21. Show All Port Prefix Fields (ATM SVCs) (Continued)

Field	Displays...
CUG Termination	One of the following: *Enabled* – The prefix is used as part of a closed user group (CUG). Incoming and outgoing calls, with a calling or called party address that matches this prefix, are subject to CUG security checks. For more information about CUGs, see the *NavisCore ATM Configuration Guide*. *Disabled* – The prefix is not used as part of a CUG.
Admin Cost	The administrative cost associated with the port prefix. When an SVC is being created, if more than one port in the network is found with the same port prefix, the call is routed to the port in the network that has the lowest administrative cost associated with the port prefix.
Address Registration	One of the following: *Enabled* – The port prefix is used for ILMI address registration if ILMI is enabled on this logical port. If the port prefix address type is AESA, the prefix must be 13 bytes (104 bits) long in order for Address Registration to be enabled. *Disabled* – The port prefix is not used for ILMI address registration. If the port prefix address type is AESA, and the prefix is other than 13 bytes (104 bits) long, the Address Registration attribute is disabled.
Scope	The organizational scope of the port prefix. The organizational scope determines the extent to which (i.e., high in the routing hierarchy) an address may be advertised. Possible scopes include Global, InterRegional, Regional, IntraCommunity, CommunityMinusOne, OrganizationPlusOne, IntraSite, SiteMinusOne, LocalNetworkPlusTwo, LocalNetworkPlusOne, LocalNetwork.
CUG Oper Status	The current CUG status. Possible address and prefix status messages include: • A CUG configuration error has occurred at this SVC address (or prefix). • An ambiguous condition exists at this SVC address (or prefix). Decisions will be made at call time. • This SVC address (or prefix) has: Outgoing access, Incoming access. • This SVC does not belong to any CUGs. • This SVC Address belongs to CUGs: [*CUG name and ID*].

Viewing All Port Addresses

SVC addresses can be configured for all logical ports on a physical port if the device attached to the physical port does not support address registration. To view all SVC port addresses:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port Addresses. The Show All Port Addresses dialog box appears (see Figure 13-28).

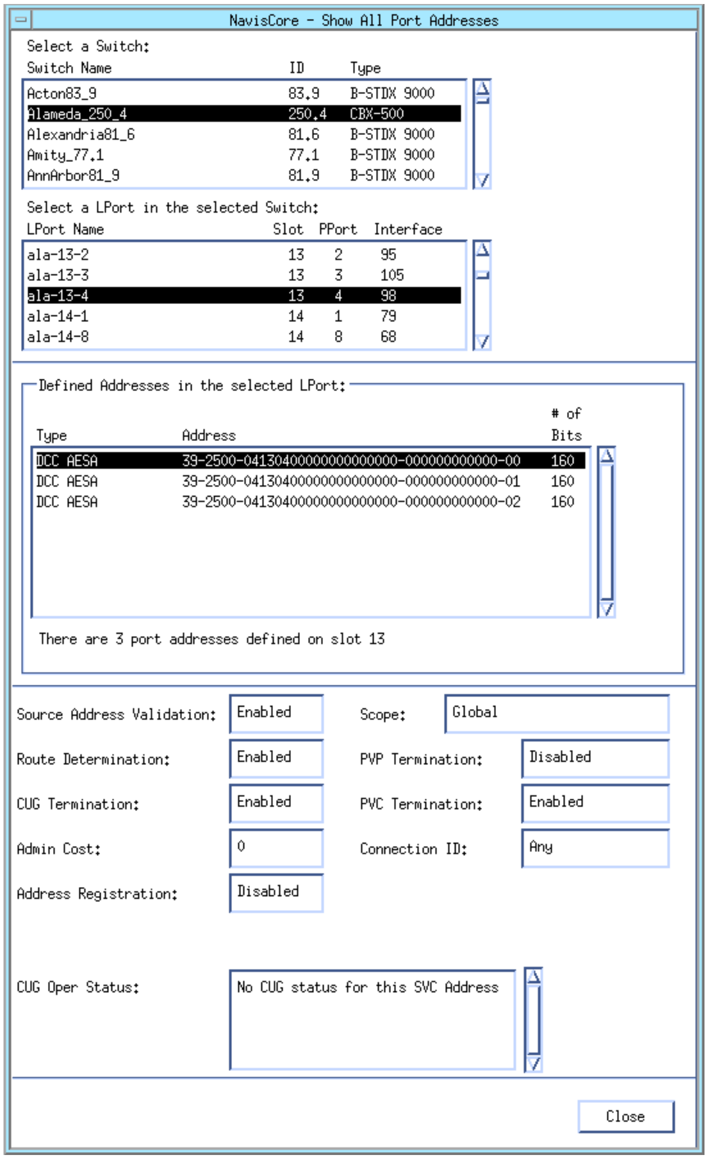


Figure 13-28. Show All Port Addresses Dialog Box

2. Select a switch.
3. Select a logical port. The dialog box displays the defined addresses for the logical port.

4. When you finish, choose Close to return to the network map.

Table 13-22 describes the Show All Port Addresses fields.

Table 13-22. Show All Port Addresses Fields (ATM SVCs)

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch number used as the host assignment in the switch's internal IP address.
Type	The switch type (e.g., GX 550).
Logical Port Information	
LPort Name	The name of the logical port associated with the addresses.
Slot	The slot number of the IOM used by the logical port.
PPort	The number of the physical port on which the logical port is configured.
Interface	The logical port's internal interface number.
Defined Addresses for the Selected Logical Port	
Type	The configured SVC address format. See Table 13-20 on page 13-56 for a description of address formats.
Address	The configured address.
# of Bits	The number of address bits checked during call screening and call routing.
Source Address Validation	One of the following: *Enabled* – The address is used to validate the calling party address against the address associated with the UNI port that received the call setup message. *Disabled* – The address is not used to validate calling party addresses.
Route Determination	One of the following: *Enabled* – OSPF uses the address for route determination. *Disabled* – OSPF does not use the address for route determination.
CUG Termination	One of the following: *Enabled* – The address is used as part of a closed user group (CUG). Incoming and outgoing calls, with a calling or called party address that matches this address, are subject to CUG security checks. For more information about CUGs, see the *NavisCore ATM Configuration Guide*. *Disabled* – The address is not used as part of a CUG.

Table 13-22. Show All Port Addresses Fields (ATM SVCs) (Continued)

Field	Displays...
Admin Cost	The administrative cost associated with the address. When an SVC is being created, if more than one port in the network is found with the same address, the call is routed to the port in the network that has the lowest administrative cost associated with the address.
Address Registration	One of the following: *Enabled* – The port address is used for ILMI address registration if ILMI is enabled on this logical port. If the port address type is AESA, the address must be 13 bytes (104 bits) long in order for Address Registration to be enabled. *Disabled* – The port address is not used for ILMI address registration. If the port address type is AESA, and the address is other than 13 bytes (104 bits) long, the Address Registration attribute is disabled.
CUG Oper Status	The current CUG status. Possible address and prefix status messages include: • A CUG configuration error has occurred at this SVC address (or prefix). • An ambiguous condition exists at this SVC address (or prefix). Decisions will be made at call time. • This SVC address (or prefix) has: Outgoing access, Incoming access. • This SVC does not belong to any CUGs. • This SVC Address belongs to CUGs: [*CUG name and ID*].
Scope	The organizational scope of the address. The organizational scope determines the extent to which (i.e., how far up the routing hierarchy) an address may be advertised. Possible scopes include Global, InterRegional, Regional, IntraCommunity, CommunityMinusOne, OrganizationPlusOne, IntraSite, SiteMinusOne, LocalNetworkPlusTwo, LocalNetworkPlusOne, LocalNetwork.
PVP Termination	One of the following: *Enabled* – A soft permanent virtual path connection (SPVPC) may be terminated to this address on this logical port. See the section "Viewing Soft PVCs" on page 13-47 for more information on SPVPCs. *Disabled* – An SPVPC may not be terminated on this logical port.
PVC Termination	One of the following: *Enabled* – A soft permanent virtual channel connection (SPVCC) may be terminated to this address on this logical port. See the section "Viewing Soft PVCs" on page 13-47 for more information on SPVCCs. *Disabled* – An SPVCC may not be terminated on this logical port.

Table 13-22. Show All Port Addresses Fields (ATM SVCs) (Continued)

Field	Displays...
Connection ID	The connection ID associated with the address. This field applies only if either (but not both of) the PVC termination or the PVP termination attributes are set. The connection ID is interpreted as a 32-bit integer with the VPI field in bits 0-15 and the VCI/DCLI field in bits 16-31. For ATM PVC/PVP termination, a VPI of 0 and VCI of 0 indicate that the switch may select any VPI/VCI as appropriate.
VPI	The VPI in the connection ID.
VCI	The VCI in the connection ID.

Viewing All Port User Parts

The user part of an AESA address is used for DTE (user) ports on a Ascend switch. The user part is used to construct the address table on the DCE device attached to the public side of the UNI. When the DCE broadcasts its network prefixes, the DTE responds by sending its configured user parts; this enables the DCE to build the ILMI address table. For more information, see the *NavisCore ATM Configuration Guide*.

To view all user parts defined for a logical port:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port User Parts. The Show All Port User Parts dialog box appears (see Figure 13-29).

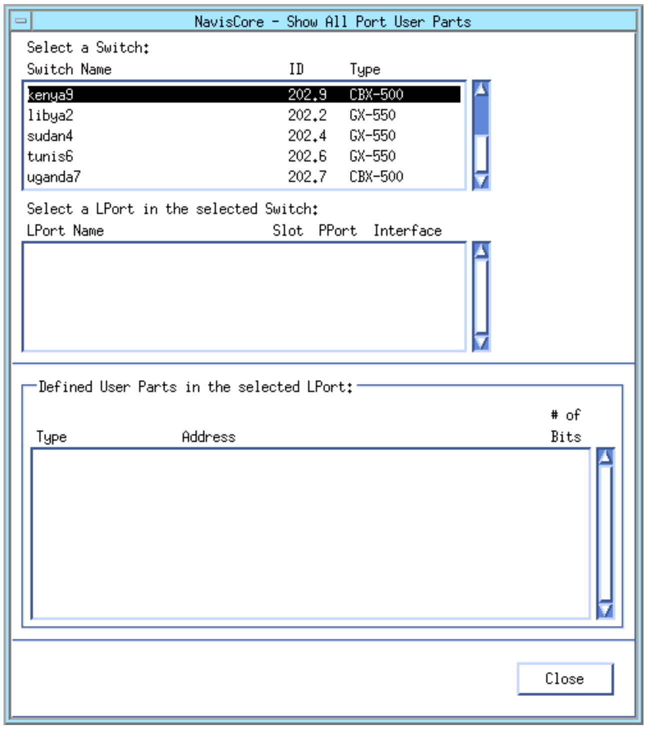


Figure 13-29. Show All Port User Parts Dialog Box

2. Select a switch.
3. Select a logical port. The dialog box displays the user part type, address, and number of bits assigned to the logical port.
4. Choose Close to return to the network map.

Table 13-23 describes the fields on the Show All User Parts dialog box.

Table 13-23. Show All Port User Parts Fields

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch number used as the host assignment in the switch's internal IP address.
Type	The switch type (e.g., GX 550).
Logical Port Information	
LPort Name	The name of the logical port associated with the user part.
Slot	The slot number of the IOM used by the logical port.

Table 13-23. Show All Port User Parts Fields (Continued)

Field	Displays...
PPort	The number of the physical port on which the logical port is configured.
Interface	The logical port's internal interface number.
Defined User Parts for the Selected Logical Port	
Type	A value of *User Part*.
Address	The user part of an AESA address, which consists of the End System Identifier (ESI) and Selector (SEL) parts of the address. The ESI is a 6-octet field that identifies the end system (typically an IEEE MAC address). The SEL is a 1-octet field that is not used for ATM routing but may be used by the end system.
# of Bits	The number of address bits that are checked during call screening and call routing.

Viewing All Port Network IDs

Network IDs can be defined for specific logical ports. To view all port network IDs defined for a selected logical port:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port Network IDs. The Show All Port Network IDs dialog box appears (see Figure 13-30).

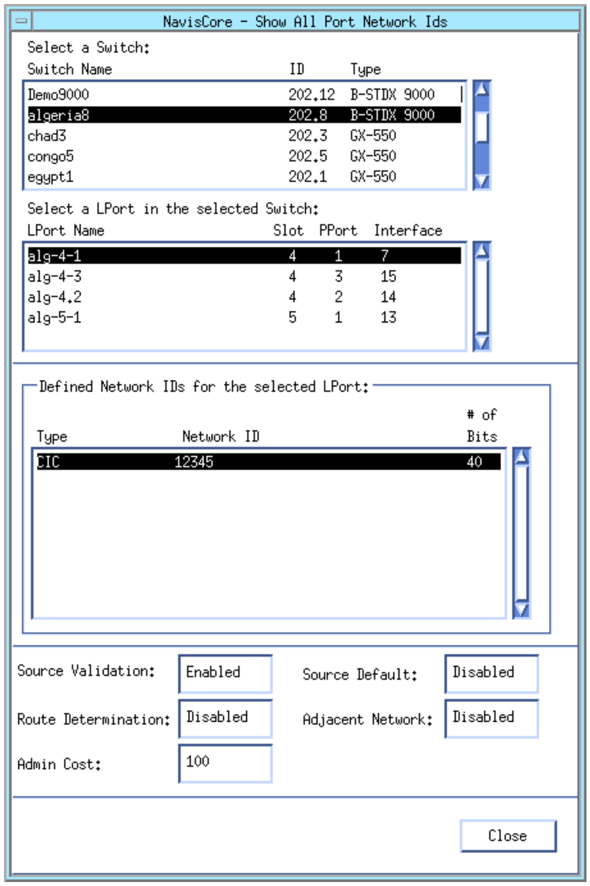


Figure 13-30. Show All Port Network IDs Dialog Box (ATM SVCs)

2. Select a switch.
3. Select a logical port. The dialog box displays the defined network IDs and related information for the logical port.
4. When you finish viewing the information, choose Close to return to the map.

Table 13-24 describes the Show All Port Network IDs fields.

Table 13-24. Show All Port Network IDs Fields (ATM SVCs)

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch number used as the host assignment in the switch's internal IP address.
Type	The switch type (e.g., GX 550).

Table 13-24. Show All Port Network IDs Fields (ATM SVCs) (Continued)

Field	Displays...
Logical Port Information	
LPort Name	The name of the logical port associated with the network ID.
Slot	The slot number of the IOM used by the logical port.
PPort	The number of the physical port on which the logical port is configured.
Interface	The logical port's internal interface number.
Defined Network IDs	
Type	The Carrier Identification Code (CIC) address format. This format supports 3-digit, 4-digit, or 8-digit addresses.
Network ID	The configured network ID, which is used to uniquely identify an Inter-Exchange Carrier (IXC). Depending on the addressing authority, the network ID can be in CIC format.
# of Bits	The number of address bits that are checked during call routing.
Source Validation	One of the following: *Enabled* – The network ID is used for source validation. The switch can use the network ID to screen a signaled transit network selection (TNS), which is a value supplied by the calling party during call setup. The switch matches the TNS against all pre-subscribed source validation network IDs on this interface. If a match occurs, the call is progressed. Otherwise, the call is rejected. *Disabled* – The network ID is not used for source validation.
Route Determination	One of the following: *Enabled* – The network ID is used for route determination. For route determination, the network ID allows an Inter-Exchange Carrier (IXC) to be reached. When a calling party signals for the network ID during call setup, the switch routes the call to the IXC via the logical port associated with the network ID. *Disabled* – The network ID is not used for route determination.
Admin Cost	The administrative cost associated with the network ID. When an SVC is being created, if more than one port in the network is found with the same network ID, the call is routed to the port in the network that has the lowest administrative cost associated with the network ID.

Table 13-24. Show All Port Network IDs Fields (ATM SVCs) (Continued)

Field	Displays...
Source Default	One of the following: *Enabled* – The network ID is the default (i.e., subscription) network ID for the logical port. The source default network ID is provisioned as a substitute when a signaled TNS is not provided during the call setup process. That is, if no TNS is signaled, and the network does not know the called party number, the network uses the default network ID when it attempts to route the call. Only one source validation network ID may be designated as the source default. *Disabled* – The network ID is not the default network ID for the logical port.
Adjacent Network	One of the following: *Enabled* – The network ID is the route determination network ID that the switch uses as the default for billing purposes (for PVCs and SVCs). This network ID identifies a directly connected (or adjacent) network. A TNS matching this network ID will not be signaled on egress. Only one route determination network ID may be designated as the adjacent network ID. *Disabled* – The network ID is not the route determination network ID that the switch uses as the default for billing purposes. For example, this field displays *Disabled* if the network identified by the network ID is not reached directly, but is instead reached by way of a directly connected network.

Viewing All Active ATM SVCs

The Show All Active SVCs function enables you to:

- Upload SVC information for a selected ATM or Frame Relay logical port, which provides a hop-by-hop trace of all active ATM and Frame Relay SVCs that traverse the network.
- View a list of SVC records with attributes for each record.
- Select an SVC record and view its SVC attributes. The specific attributes that appear depend on the type of service that the SVC supports: ATM or Frame Relay.

For information on monitoring active Frame Relay SVCs, see "Viewing All Active Frame Relay SVCs" on page 14-42.

To view a list of SVC records:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Active SVCs. The Show All Active SVCs dialog box appears (see Figure 13-31).

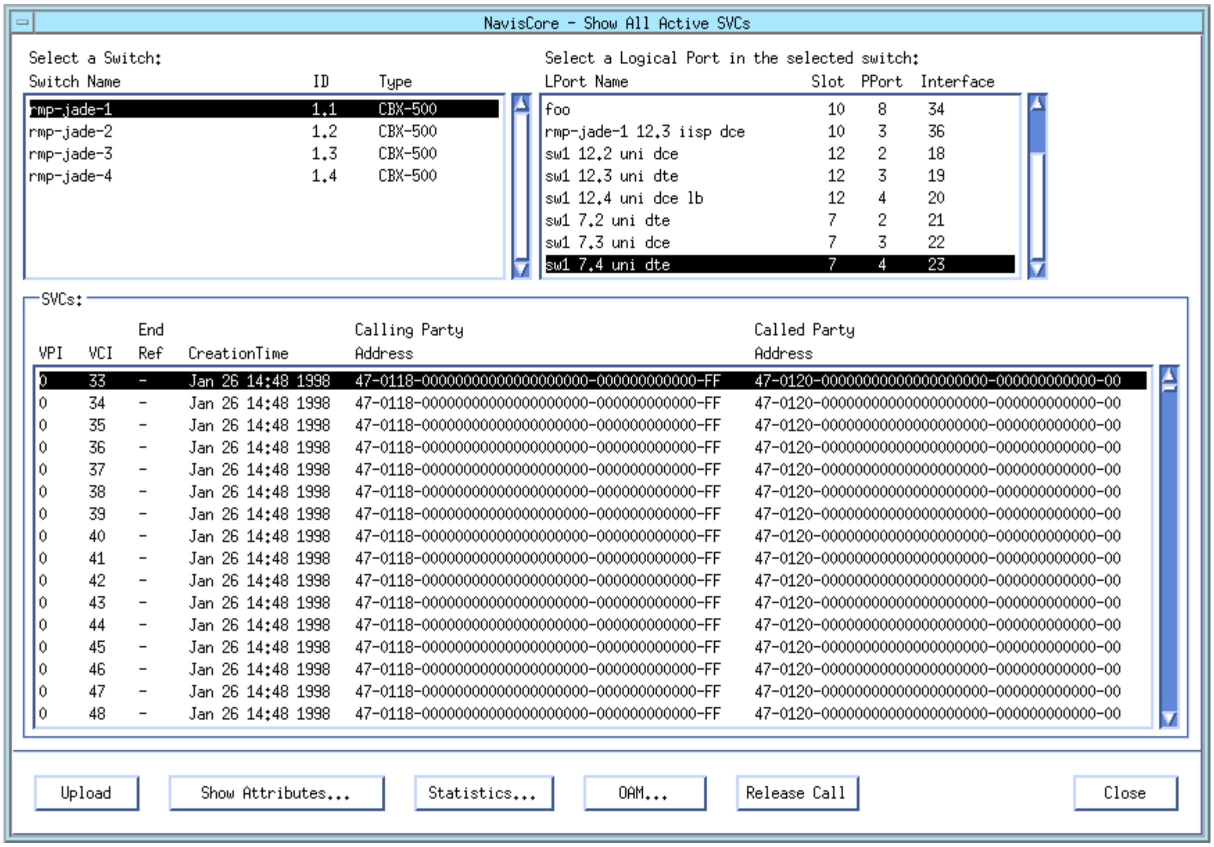


Figure 13-31. Show All Active SVCs Dialog Box (ATM)

2. Select a switch.
3. Select a logical port.
4. Choose Upload to upload all SVC records for the selected logical port. The records appear when the upload is completed.

Table 13-25 describes the Show All Active SVCs dialog box buttons. Table 13-26 describes the fields that appear for ATM SVCs.

Table 13-25. Show All Active SVCs Buttons (ATM)

Button	Function
Upload	Uploads a list of active SVCs for the logical port you select.
Show Attributes	Displays call attributes for the SVC you select.
Statistics	Displays SVC statistics.
OAM	Enables you to initiate an OAM loopback test for the selected SVC. See "Testing ATM Circuits" on page 13-90 for more information.

Table 13-25. Show All Active SVCs Buttons (ATM) (Continued)

Button	Function
Release Call	Enables you to release individual SVCs on a UNI port without affecting other SVCs on the same port.

Table 13-26. Show All Active SVCs Fields (ATM)

Field	Displays...
VPI	The ID of the virtual path between the SVC endpoints. This number is equivalent to the VPI value in the ATM cell header and is used to route cell traffic. See the *NavisCore ATM Configuration Guide* for more information.
VCI	The ID of the virtual channel between the SVC endpoints. This number is equivalent to the VCI value in the ATM cell header. See the *NavisCore ATM Configuration Guide* for more information.
End Ref	(*Point-to-multipoint SPVCs only*) The number used to reference a leaf endpoint on a point-to-multipoint SPVC. For point-to-point SVCs, this field displays a dash (-).
Creation Time	The time at which the connection was established.
Calling Party Address	The address of the party that initiated the call. This field is optional and may be blank.
Called Party Address	The address of the party that accepted the call.

Viewing ATM SVC Attributes

The Show Attributes button on the Show All Active SVCs dialog box enables you to view information about a specific SVC. The specific information that appears depends on the type of service that the SVC supports: ATM or Frame Relay. For information on viewing Frame Relay SVC attributes, see "Viewing Frame Relay SVC Attributes" on page 14-44.

To view ATM SVC attributes:

1. From the Show All Active SVCs dialog box (Figure 13-31 on page 13-71), select an SVC record.
2. Choose Show Attributes. The Show Active SVC Attributes dialog box appears (see Figure 13-32).

> SVCs are dynamic and can be set up and taken down by the CPE. A SVC may be released by the CPE between the time you choose Upload and Show Attributes. In this instance, you will not be able to access the SVC's attributes.

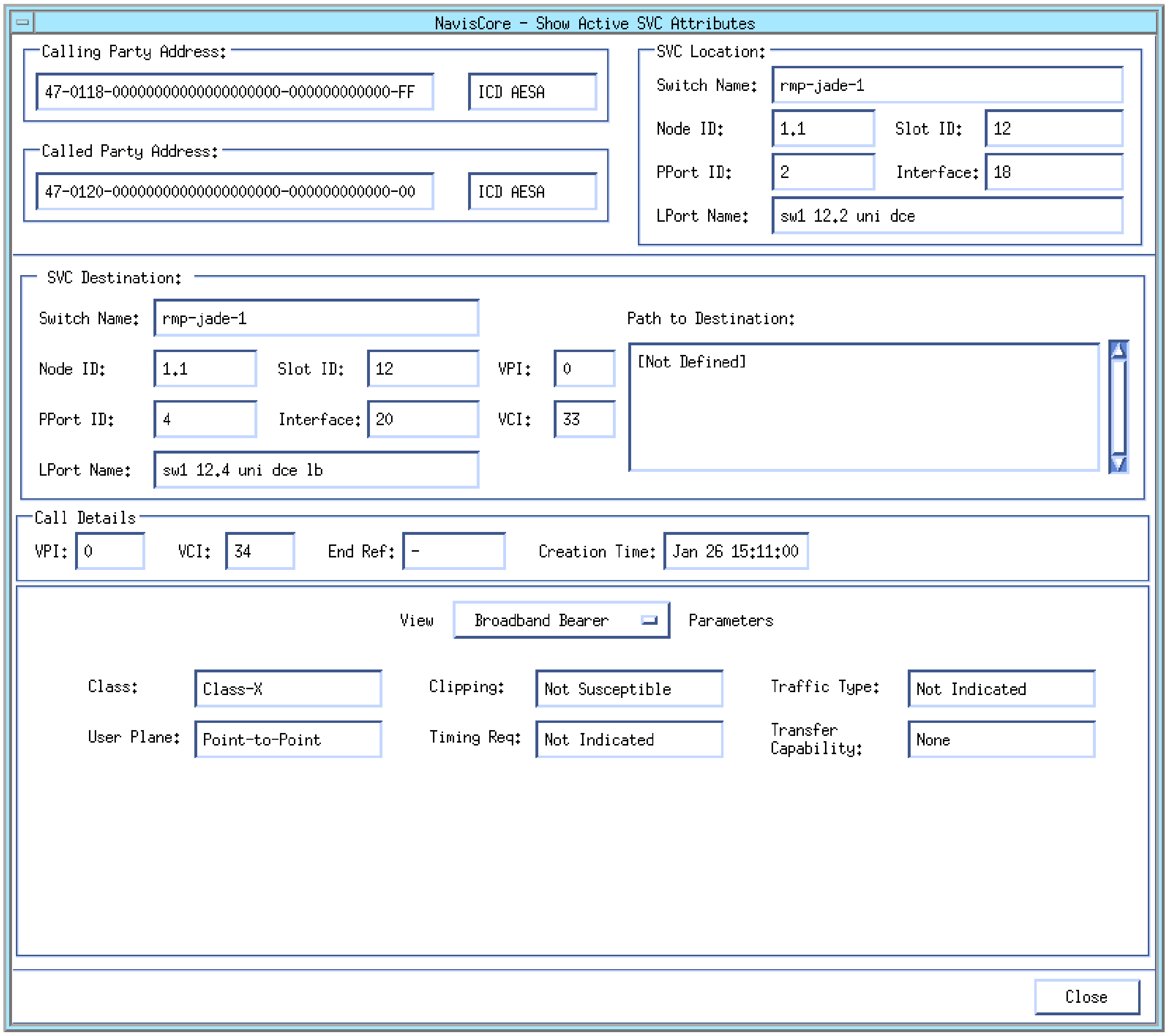


Figure 13-32. Show Active SVC Attributes Dialog Box (ATM)

3. Use the View Parameters option menu to view broadband bearer, QoS, traffic descriptor, or ABR parameters.
4. When you finish viewing SVC attributes, choose Close to return to the Show All Active SVCs dialog box.

Table 13-27 describes the Show Active SVC Attributes fields for ATM SVCs.

Table 13-27. Show Active SVC Attributes Fields (ATM)

Field	Displays...
Calling Party Address	The entire SVC calling party address and lists the address type. See Table 13-21 on page 13-60 for more information on address formats.
Called Party Address	The entire SVC called party address and lists the address type. See Table 13-21 on page 13-60 for more information on address formats.
SVC Location	Information that identifies the local SVC location, including switch, logical port, and physical port IDs.
SVC Destination	Information that identifies the remote SVC location, including switch, logical port, and physical port IDs, and VPI/VCI addresses. This section also displays a “Path to Destination” listing which provides the hop count and trunk name if the call was routed over OSPF trunks.
SVC Call Details	The local VPI/VCI and call creation time. This section also displays the endpoint reference and AAL Type.
View Parameters (Option Menu)	
Broadband Bearer	The fields that provide the contents of the broadband bearer capability information element from the SETUP or ADD PARTY message. For more information on ATM broadband bearer capabilities, see Appendix D, “Signalled QoS, BBC, ATC, and BEI Service Category Mappings.”
QoS	The configured forward and reverse QoS class: either CBR, VBR-RT, VBR-NRT, or Unspecified. For more information on ATM QoS parameters, see Appendix D, “Signalled QoS, BBC, ATC, and BEI Service Category Mappings” and the *NavisCore ATM Configuration Guide*. ***Note**: The signalled QoS parameters are displayed only. Under some conditions, the signalled QoS received by the switch may be different from the actual QoS in the switch.*
Traffic Descriptor	The forward and reverse ATM traffic descriptors. For more information on ATM traffic descriptors, see Appendix D, “Signalled QoS, BBC, ATC, and BEI Service Category Mappings” and the *NavisCore ATM Configuration Guide*.

Table 13-27. Show Active SVC Attributes Fields (ATM) (Continued)

Field	Displays...
ABR	The configured forward and reverse ABR parameters for the SVC. Parameters include: *FRMRTT* – The ABR fixed RM round trip time (in microseconds) for this SVC. *ICR (cells/sec)* – The initial cell rate (ICR) is the rate (in cells per second) at which the source may send. *RIF* – The rate increase factor (RIF) controls how much the cell transmission rate may increase upon receipt of an RM cell. RIF is a power of two ranging from 1/32768 to 1. *RDF* – The rate decrease factor (RDF) controls the decrease in the cell transmission rate. RDF is a power of two ranging from 1/32768 to 1. *TBE (cells)* – The transient buffer exposure (TBE) is the negotiated number of cells that the network would like to limit the source to sending during start-up periods – before the first RM cell returns. Values range from 0 to 16,777,215. *NRM* – Nrm is the maximum number of cells a source may send for each forward RM cell. Nrm is a power of 2 that ranges from 2 to 256. *MRM* – Mrm controls allocation of bandwidth between forward RM cells, backward RM cells, and data cells. Mrm is a constant fixed at 2. *CDF* – The cutoff decrease factor (CDF) controls the decrease in ACR (available cell rate) associated with CRM (missing RM-cell count). *ADTF* – The ACR decrease time factor (ADTF) is the time (in seconds) allowed between sending RM cells before the rate is decreased to ICR. For more information on ABR parameters, see the *NavisCore ATM Configuration Guide* and the *ATM Forum Traffic Management Specification, Version 4.0*. You can access the ATM Forum Web site at http://www.atmforum.com.

Viewing All ILMI Addresses

This section describes how to view dynamic address (i.e., ILMI) information for a logical port. To view ILMI information for a selected logical port:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All ILMI Addresses. The Show All ILMI Addresses dialog box appears (see Figure 13-33).

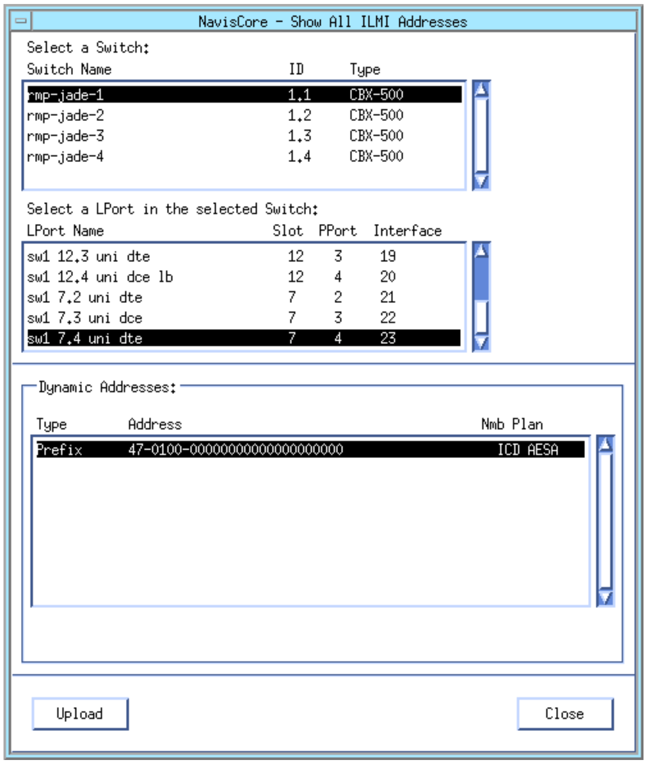


Figure 13-33. Show All ILMI Addresses Dialog Box

2. Select a switch.
3. Select a logical port.
4. Choose Upload to display the ILMI dynamic addresses assigned to the logical port.
5. Choose Close to return to the network map.

Viewing ATM SVC Failed Calls

You can view failed-call information for failed ATM SVCs, which help you determine why an SVC call failed.

Before you can view SVC failed calls, you must upload SVC call-failure information. To upload and view SVC failed-call information:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Failed SVCs. The Show All Failed SVCs dialog box appears (see Figure 13-34).

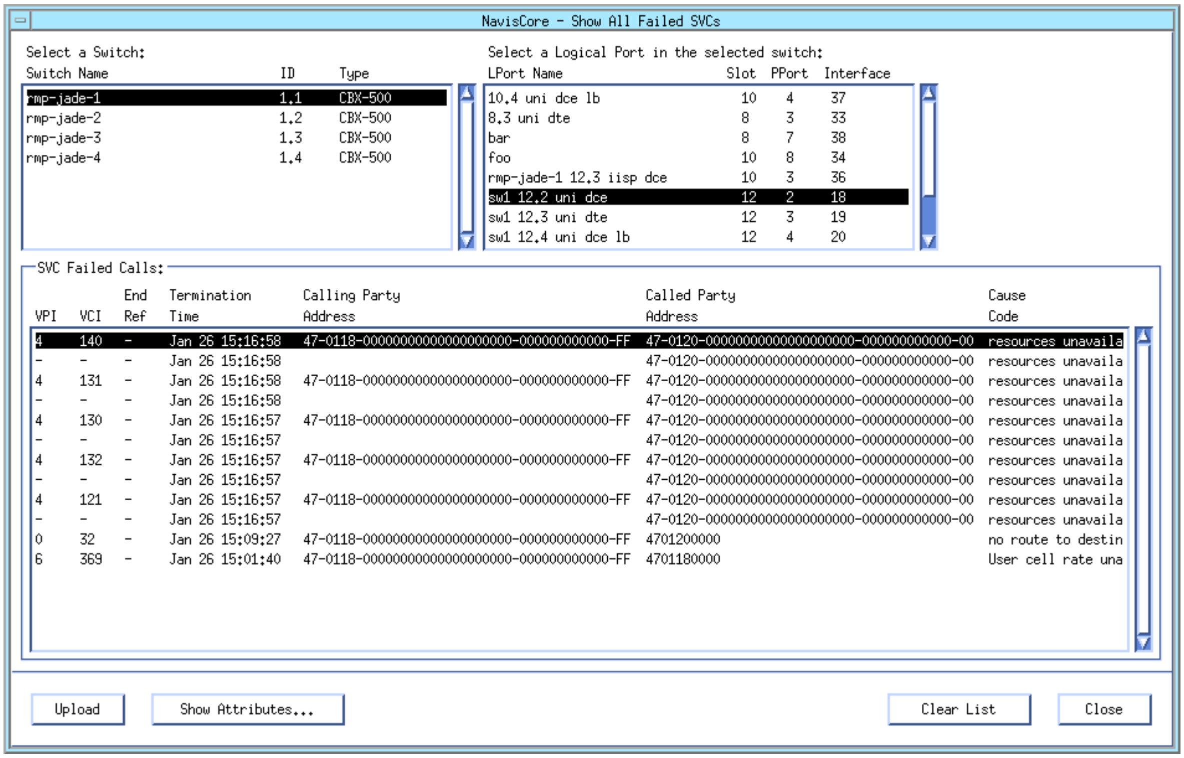


Figure 13-34. Show All Failed SVCs Dialog Box (ATM)

2. Select a switch.
3. Select a logical port.
4. Choose Upload to view the failed SVC calls for the logical port. The records associated with the calls appear when the upload is completed.
5. Choose Close to return to the network map.

Table 13-28 describes the Show All Failed SVCs dialog box buttons. Table 13-29 describes the fields on the Show All Failed SVCs dialog box.

Table 13-28. Show All Failed SVCs Buttons (ATM)

Button	Function
Upload	Uploads a list of active SVCs for the logical port you select.
Show Attributes	Displays information about the failed SVC call you select. See "Viewing ATM SVC Failed-Call Attributes" on page 13-79 for information.
Clear List	Deletes the list of failed calls for this logical port from the switch. ***Note****: This action permanently deletes the current list from the switch; however, new failures will continue to be logged.*
Close	Closes the dialog box.

Table 13-29. Show All Failed SVCs Fields (ATM)

Field	Displays...
VPI	The ID of the virtual path between the SVC endpoints. This number is equivalent to the VPI value in the ATM cell header and is used to route cell traffic. See the *NavisCore ATM Configuration Guide* for more information.
VCI	The ID of the virtual channel between the SVC endpoints. This number is equivalent to the VCI value in the ATM cell header. See the *NavisCore ATM Configuration Guide* for more information.
End Ref	(*Point-to-multipoint SPVCs only*) The number used to reference a leaf endpoint on a point-to-multipoint SPVC. For point-to-point SPVCs, this field displays a dash (-).
Termination Time	The time at which the connection terminated.
Calling Party Address	The address of the party that initiated the call. This field is optional and may be blank.
Called Party Address	The address of the party that accepted the call.
Cause Code	A message describing this failure. The failure cause text is based on the standard ATM forum UNI signalling cause codes. See Appendix E, "Using SVC Failure Information" for more information.

Viewing ATM SVC Failed-Call Attributes

You can view information for a failed SVC call, such as calling party address, failure time, and terminating PDU.

To view failed attributes:

1. From the Show All Failed SVCs dialog box (Figure 13-34 on page 13-77), select an SVC failed-call record.
2. Choose Show Attributes. The Show Failed SVC Attributes dialog box appears (see Figure 13-35).

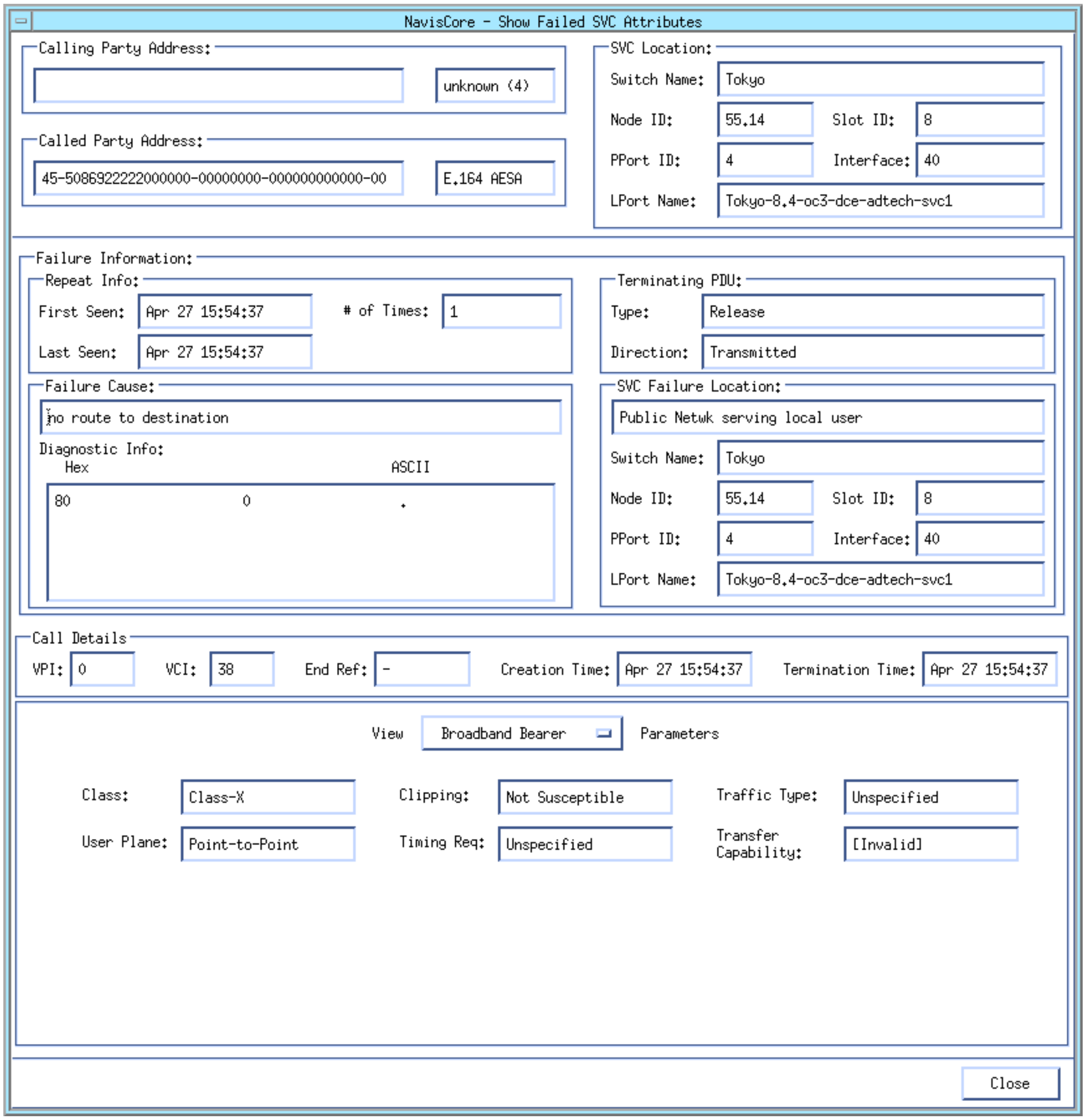


Figure 13-35. Show Failed SVC Attributes Dialog Box (ATM)

3. Use the View Parameters option menu to select broadband bearer, QoS, or traffic descriptor parameters.
4. When you finish viewing failed SVC attributes, choose Close to return to the Show All Failed SVCs dialog box.

Table 13-30 describes the Show Failed SVC Attributes fields.

Table 13-30. Show Failed SVC Attributes Fields (ATM)

Field	Displays...
Calling Party Address	The entire SVC calling party address and the address type. See Table 13-21 on page 13-60 for more information on address formats.
Called Party Address	The entire SVC called party address and the address type. See Table 13-21 on page 13-60 for more information on address formats.
SVC Location	Information that identifies the local SVC location, including switch, logical port, and physical port IDs.
Repeat Info	The dates and times of the failure's first occurrence and most recent occurrence. Also displays the number of consecutive times this same failure has occurred on this port.
Terminating PDU	The type of signalling PDU used to terminate the call and indicates whether it was sent from or received by the logical port.
Failure Cause	A message describing this failure. The failure cause text is based on the standard ATM Forum UNI signalling cause codes. See Appendix E, "Using SVC Failure Information" for more information.
Diagnostic Info	The HEX and ASCII values from the release message diagnostic field. This information may help diagnose certain types of SVC failures.
SVC Failure Location	A message describing the location of this failure, as well as the switch name, logical port ID and physical port ID information. The failure may be located locally (the location as identified by the SVC Location field) or remotely.
Call Details	The VPI/VCI and endpoint reference. This field also displays the call creation and termination times.
View Parameters (Option Menu)	
Broadband Bearer	The fields that provide the contents of the broadband bearer capability information element from the SETUP or ADD PARTY message. For more information on ATM broadband bearer capabilities, see Appendix D, "Signalled QoS, BBC, ATC, and BEI Service Category Mappings."
Traffic Descriptor	The forward and reverse ATM traffic descriptors. For more information on ATM traffic descriptors, see Appendix D, "Signalled QoS, BBC, ATC, and BEI Service Category Mappings" and the *NavisCore ATM Configuration Guide*.

Table 13-30. Show Failed SVC Attributes Fields (ATM) (Continued)

Field	Displays...
QoS	The configured forward and reverse QoS class: CBR, VBR-RT, VBR-NRT, or Unspecified. For more information on ATM QoS parameters, see Appendix D, “Signalled QoS, BBC, ATC, and BEI Service Category Mappings” and the *NavisCore ATM Configuration Guide*. ***Note**: Only the signalled QoS parameters are displayed. Under some conditions, the signalled QoS received by the switch may be different from the actual QoS in the switch.*
PNNI	The PNNI node ID and port ID of the failure location, if applicable.

Viewing Closed User Groups and Their Members

A closed user group (CUG) is a set of users (or members) who share specific calling privileges in networks that use SVCs. Members of one CUG may have calling privileges that members of another CUG may not have. CUGs provide a level of security, allowing only authorized nodes to call each other.

Closed user group standards are defined in *ITU-T Draft Recommendation Q.2955.1* and apply to both ATM SVCs and Frame Relay SVCs.

You cannot monitor CUGs through the Monitor menus. Closed user groups must be configured and monitored through the Administer menus. You must also log on in order to access CUG information.

To access CUG and CUG member information:

- Select Ascend Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUGs.
- Select Ascend Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUG Members.

See the *NavisCore ATM Configuration Guide* for more information on CUGs for ATM SVCs. See the *NavisCore Frame Relay Configuration Guide* for more information on CUGs for Frame Relay SVCs.

Viewing Port Security Screens

The Port Security Screening feature enables you to protect your network from unauthorized callers. You do this by creating screens that can allow/disallow incoming and outgoing calls.

You can apply the screens to any ATM UNI or ATM NNI logical port in your network. You can use a maximum of 16 different screens per port. Using these screens, the port checks every call it receives for matching criteria. If the call meets the matching criteria specified in at least one of these screens, the port either passes or blocks that call, according to the security screen criteria. See the *NavisCore ATM Configuration Guide* for information on configuring port security screening.

To view port security screens:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port Security Screens. The Configuration of Port Security Screens dialog box appears (see Figure 13-36).

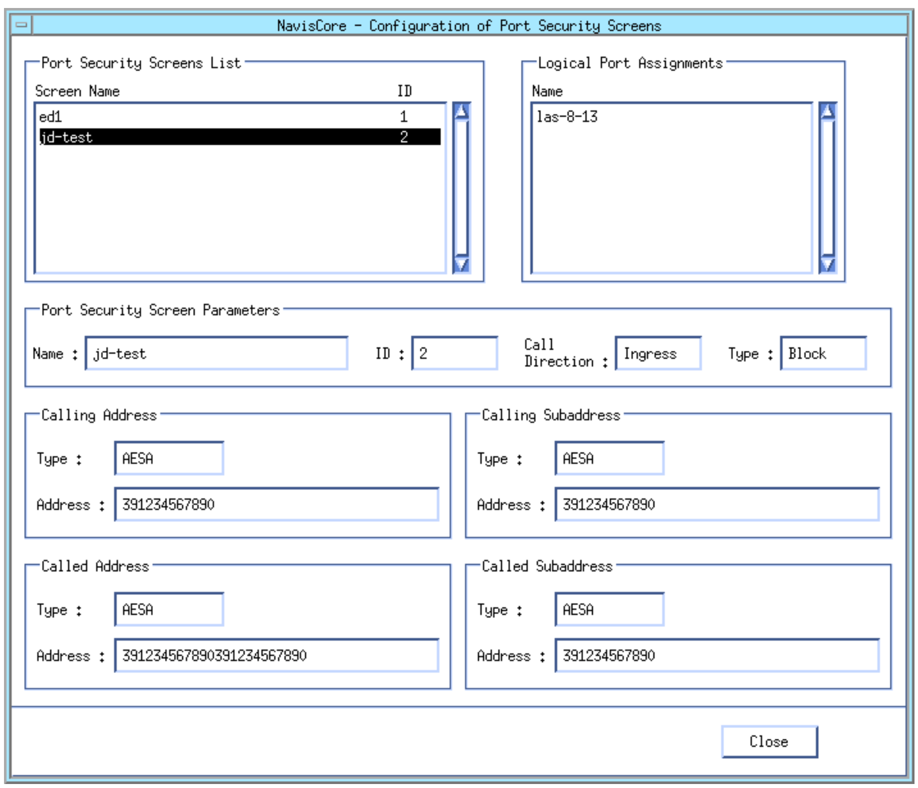


Figure 13-36. Configuration of Port Security Screens Dialog Box

2. When you finish viewing port security screen information, choose Close to return to the map.

Table 13-31 describes the Configuration of Port Security Screens dialog box fields.

Table 13-31. Configuration of Port Security Screens Fields

Field	Displays...
Name	A name (up to 32 characters) for this security screen.
Call Direction	The configured call direction screen: *Ingress* (default) – Screens incoming calls. *Egress* – Screens outgoing calls.
Type	The configured screen type which determines the action this screen performs: *Block* (default) – Blocks all calls that match the criteria. *Pass* – Passes all calls that match the criteria.
Calling Address	The calling address for incoming calls.
Calling Subaddress	The calling subaddress for incoming calls. This parameter provides an optional level of screening.
Called Address	The called address if this screen is for outgoing calls.
Called Subaddress	The called subaddress for outgoing calls. This parameter provides an optional level of screening.

Viewing ATM SVC Summary Statistics

To view ATM SVC summary statistics:

> ▶ For ATM SVCs, Resource Management (RM) cells are counted as passed CLP=0 or passed CLP=1 cells. The Logical Port Statistics dialog box provides separate RM cell statistics on a per logical port basis (see "Viewing Logical Port Summary Statistics" on page 6-19).

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Active SVCs. The Show All Active SVCs dialog box appears (Figure 13-31 on page 13-71).
2. Select a switch.
3. Select a logical port.
4. Choose Upload to display a list of SVC records for the logical port. The records display when the upload is completed.
5. Select an SVC record.

6. Choose Statistics to view the SVC Summary Statistics dialog box (see Figure 13-37).

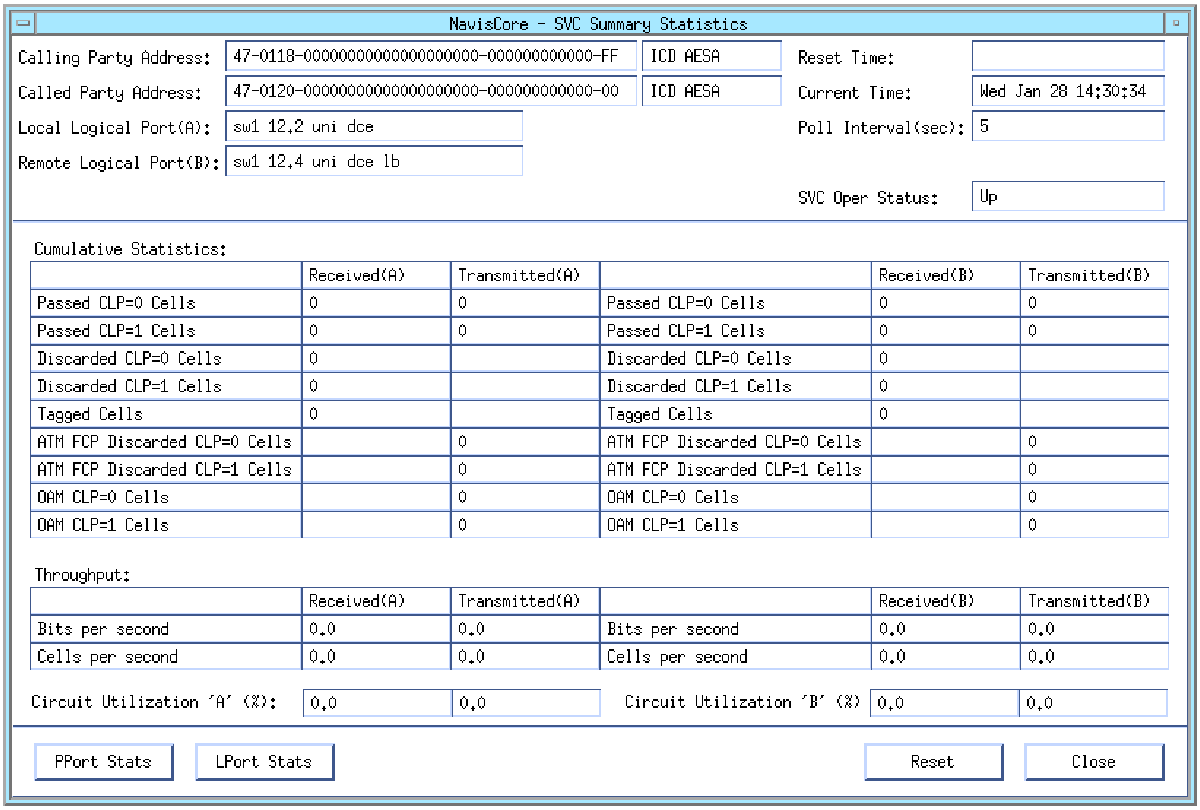


Figure 13-37. ATM SVC Summary Statistics Dialog Box

The dialog box displays data in separate columns to reflect the transmission and receipt of data on each side of the circuit. The dialog box displays the following types of statistics:

Cumulative Statistics — The number of each type of cell (passed, dropped, or tagged) and whether those cells are being transmitted or dropped due to conditions in the network.

Throughput Statistics — The cells per second and bits per second for each side of the circuit.

Utilization Statistics — The amount of traffic queued for transmission on a circuit measured as a percentage of link speed.

Table 13-32 describes the ATM SVC summary statistics fields.

Table 13-32. ATM SVC Summary Statistics Fields

Statistic	Description
Calling Party Address	The entire SVC calling party address and the address type. See Table 13-21 on page 13-60 for more information on address formats.
Called Party Address	The entire SVC called party address and the address type. See Table 13-21 on page 13-60 for more information on address formats.
Local Logical Port (A)	The logical port at one circuit endpoint.
Remote Logical Port (B)	The logical port at one circuit endpoint.
Reset Time	The time of the last statistics reset (i.e., the last time you clicked the Reset button).
Current Time	The current system time.
Poll Interval (sec)	The time interval for the collection of statistical data.
SVC Oper Status	The operating status of the SVC (*Up* or *Down*).
Cumulative Statistics	
Passed CLP=0 Cells	The total number of cells that were received and transmitted.
Passed CLP=1 Cells	The total number of CLP=1 cells received at the port. This does not include CLP=0 cells that were received and then tagged as CLP=1 cells because of a traffic descriptor violation (they are counted as tagged cells). ***Note**: Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells fields indicate that either the source may need to slow transmission, or that you should reconfigure the traffic descriptors to reflect the source speed.*
Discarded CLP=0 Cells	The total number of received CLP=0 cells that are dropped because the cell violates the defined traffic descriptor. ***Note**: Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells fields indicate that either the source may need to slow transmission, or that you should reconfigure the traffic descriptors to reflect the source speed.*
Discarded CLP=1 Cells	The total number of CLP=1 cells that are discarded because the cells violate the defined traffic descriptor. ***Note**: Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells fields indicate that either the source may need to slow transmission, or that you should reconfigure the traffic descriptors to reflect the source speed.*

Table 13-32. ATM SVC Summary Statistics Fields (Continued)

Statistic	Description
Tagged Cells	The total number of CLP=0 cells that were tagged as CLP=1 cells. Cells are tagged if they do not conform to the defined traffic descriptor for the circuit.
ATM FCP Discarded CLP=0 Cells	The total number of received CLP=0 cells that are received and discarded by the ATM Flow Control Processor (FCP).
ATM FCP Discarded CLP=1 Cells	The total number of CLP=1 cells that are received and discarded by the ATM FCP.
OAM CLP=0 Cells	The total number of F4 and F5 OAM CLP=0 cells that were transmitted by the circuit.
OAM CLP=1 Cells	The total number of F4 and F5 OAM CLP=1 cells that were transmitted by the circuit.
Throughput Statistics	
Bits per second	The number of bits transmitted and/or received each second.
Cells per second	The number of cells transmitted and/or received each second.
Utilization Statistics	
Circuit Utilization A (%)	The amount of traffic queued for transmission on a circuit as a percentage of link speed. Therefore, the circuit utilization value can exceed 100%.
Circuit Utilization B (%)	The amount of traffic queued for transmission on a circuit as a percentage of link speed. Therefore, the circuit utilization value can exceed 100%.

Viewing CAC Parameters for ATM Circuits

The Ascend Call Admission Control (CAC) feature is responsible for the bandwidth allocation on all ATM cards on the CBX 500, GX 550, and B-STDX. It is also responsible for bandwidth allocation on all Frame Relay IOMs equipped with the Priority Frame™ capability.

When creating a circuit, the CAC function computes a bandwidth allocation for that circuit and updates the bandwidth allocation for the circuit's QoS class. This bandwidth allocation depends on the specified CAC implementation, the circuit's QoS class, and the circuit's specified traffic descriptor. If you try to create a circuit that exceeds the bandwidth available for a QoS class, the circuit will not be created.

The CAC configuration option enables you to choose between the following CAC implementations:

Ascend — Enables you to control the Quality of Service and bandwidth allocation by specifying CLR and CDV objectives. You can tune the CLR and CDV parameters.

Customize VBR-NRT and ABR — Enables you to control the amount of bandwidth that is reserved for VBR-NRT and ABR circuits. You can tune the CLR, CDV, and customized CAC parameters. For customized CAC parameters, you control the amount of reserved bandwidth based on the physical port type, the configurable ranges of SCR values, or both. You can also control the establishment of circuits based on configurable ranges of maximum MBS values.

Customized VBR-RT, VBR-NRT, and ABR — Enables you to control the amount of bandwidth that is reserved for VBR-RT, VBR-NRT, and ABR circuits. You can tune customized CAC parameters only. For customized CAC parameters, you control the amount of reserved bandwidth based on the physical port type, the configurable ranges of SCR values, or both. You can also control the establishment of circuits based on configurable ranges of maximum MBS values.

For more information on configuring CAC parameters for ATM circuits, see the *NavisCore ATM Configuration Guide*.

To view CAC parameters, from the Monitor menu, select Ascend Objects ⇒ Show All CAC Parameters. The Show CAC Parameters dialog box appears (see Figure 13-38).

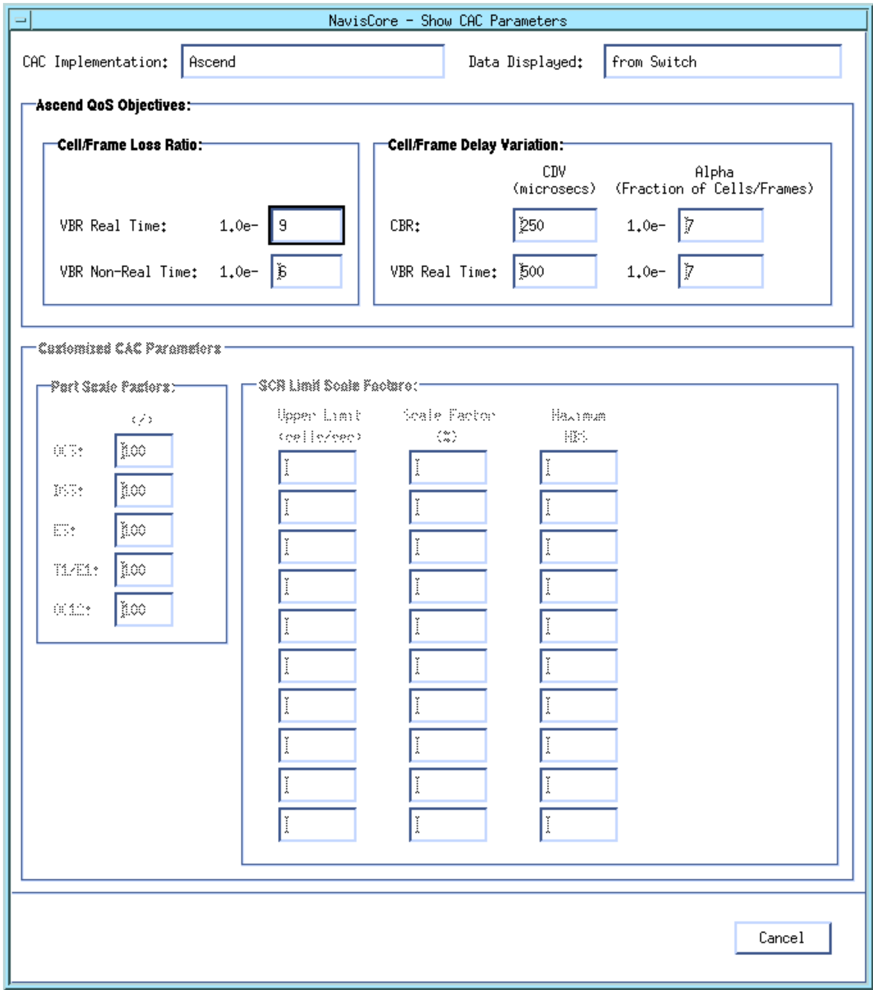


Figure 13-38. Show CAC Parameters Dialog Box

Table 13-33 describes the fields on the Show CAC Parameters dialog box. For details on these fields, see the *NavisCore ATM Configuration Guide*.

> The QoS objectives (cell/frame loss ratio and cell/frame delay variation) also apply to Frame Relay traffic. See "Viewing CAC Parameters for Frame Relay Circuits" on page 14-25 for more information.

Table 13-33. Show CAC Parameters Dialog Box Fields

Field	Displays...
CAC Implementation	The configured CAC implementation: Ascend, Customize VBR-NRT and ABR, or Customize VBR-RT, VBR-NRT, and ABR.
Data Displayed	The source of the data (from Switch in most cases).
Cell/Frame Loss Ratio (*ATM and Frame Relay*)	The cell/frame loss ratio objectives for VBR Real-Time (and VFR-RT) and VBR Non-Real Time (and VFRnrt).
Cell/Frame Delay Variation (*ATM and Frame Relay*)	The CDV values (in microseconds) for CBR and VBR Real Time (and VFR-RT), and (in the Alpha field) the fraction of the CBR cells or VBR Real Time (and VFR-RT) cells/frames that can exceed the CDV objective.
The fields below are grayed out if Ascend is the configured CAC implementation.	
Port Scale Factors	The scale factor percentage that the switch uses for calculating bandwidth requirements for each listed physical port. For example, if a value of 125% appears in the DS3 field, a circuit that would normally reserve bandwidth based on an SCR of 10,000 cells/sec would be allocated bandwidth of 12,500 cells/sec.
SCR Limit Scale Factors	The following three columns: *Upper Limit* – Lists the upper limit of each SCR range for which you want to customize the bandwidth reserved. *Scale Factor* – Lists the scale factor percentage that the switch uses when it computes bandwidth requirements for circuits in each of the defined SCR ranges. For example, if the scale factor percentage is 125%, a circuit with an SCR of 12,000 cells/second would be allocated a bandwidth of 15,000 cells/second (assuming you did not define physical port scale factors). *Maximum MBS* – Lists the maximum MBS value allowed for each range of SCR values. For example, if the maximum MBS value is 256 for the range of SCR values 0-10000, a circuit with an SCR of 7,000 cells/second and MBS of 300 cells will be rejected by the CAC function because its MBS exceeds the specified maximum MBS.

Testing ATM Circuits

The CBX 500 and GX 550 support the Operation, Administration, and Maintenance (OAM) functions described in the *ATM Forum UNI 3.0/3.1/4.0 Specifications*.

On the CBX 500 and GX 550, OAM functions test connectivity on the following circuit types:

- ATM PVCs
- ATM SVCs
- ATM Point-to-Point SPVCs

This section describes how OAM cells are used with ATM layer fault management to provide the following functions:

- OAM connectivity verification
- OAM alarm surveillance

The CBX 500 and GX 550 do not support OAM performance monitoring (pm) functions.

For more information on OAM, see the *ATM Forum UNI 3.0, 3.1 or 4.0 Specificatio*ns.

Before You Begin

Before you run an OAM loopback test, make sure that all of the equipment to be tested supports OAM.

You should also be aware of a phenomenon called an *OAM storm*. OAM storms are characterized by an IOM/IOP physical port receiving OAM cells at a rate greater than one OAM cell per second per virtual circuit. This event is extremely rare and is caused by defective equipment.

Ascend switches protect against OAM storms. If a physical port receives OAM cells at a rate that exceeds approximately 800 cells per second for any particular VC on that port, the VC shuts down for two minutes. When the shutdown occurs, the switch sends the following trap to the NMS:

```
OAM overload detected on [circuit name] at [switch name] on
lport [lport name]
```

If the OAM storm is temporary, the circuit resumes normal operation after two minutes. If the OAM storm persists, the circuit remains down, and the trap continues to appear every two minutes. In this case, you can either delete the circuit or change the Admin Status of the physical port to Down.

In the event of an OAM storm, you should determine why the attached device is sending OAM cells at a rate that triggers the protection circuitry. No network conditions should ever cause such a fast rate of OAM cells to be sent to the switch.

OAM Connectivity Verification

The CBX 500 and GX 550 support two types of OAM connectivity verification:

- OAM cells sent to a CBX 500 or GX 550 UNI/NNI port from an attached device
- OAM loopback cell generation

OAM Cells Sent to a CBX 500/GX 550 UNI Port from an Attached Device

When OAM virtual path (VP) (F4) or virtual channel (VC) (F5) segment loopback cells are sent to a CBX 500 or GX 550 UNI logical port, the cell's Loopback Indication field decrements and the switch sends the cell back to the originating device (in most cases). If no VP or VC associated with the VPI or VCI of the OAM cell exists on the UNI logical port that received the cell, the OAM cell is discarded. The OAM cell is also discarded if it is improperly formatted.

In most cases, the CBX 500 or GX 550 assumes the role of an intermediate switch from an OAM perspective. If OAM F4 or F5 end-to-end (not segment) loopback cells are sent to a CBX 500 or GX 550 UNI port, the cells are passed through the switch unmodified over the VP or VC. Since the CBX 500 or GX 550 is only the intermediate switch for the VP or VC, no action is taken. The device at the circuit's terminating point performs the loopback action for an end-to-end loopback cell.

OAM Loopback Cell Generation

You can generate loopbacks on PVCs, SVCs, and SPVCs. Using the OAM loopback function, you can generate OAM loopback cells from a CBX 500 or GX 550 UNI/NNI interface toward the attached device as shown in Figure 13-39, or into the Ascend network as shown in Figure 13-40.

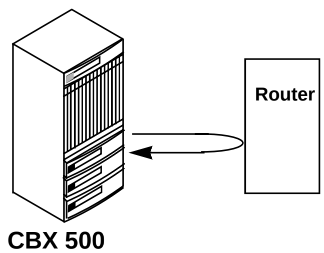


Figure 13-39. OAM Loopback Process From UNI/NNI Interface

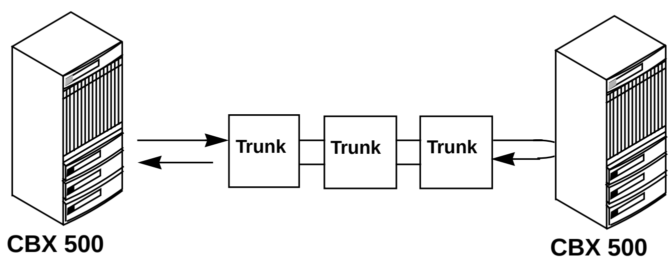


Figure 13-40. OAM Loopback Process Through Ascend Network

Running OAM Loopback Tests

On the CBX 500 and GX 550, you can perform the following types of OAM loopback tests:

- OAM PVC loopback
- OAM SPVC loopback
- OAM SVC loopback

The procedure for running each OAM loopback test similar. To run the OAM loopback test, use the following sequence:

Step 1. (*Optional*) Set the OAM loopback time interval or accept the default polling interval (5 seconds).

Step 2. Access the OAM loopback functions (page 13-93).

Step 3. Run the loopback test (page 13-94).

Setting the OAM Loopback Time Interval

NavisCore monitors the progress of the loopback once per polling interval. Slow response time indicates network congestion. To set a time interval other than the default interval (5 seconds):

1. From the Misc menu, select Ascend Time Intervals ⇒ Set OAM Time Interval. The Change OAM Polling Interval dialog box appears (see Figure 13-41).

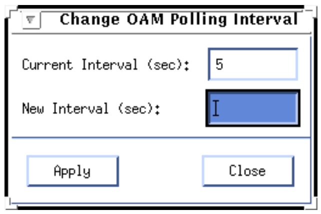


Figure 13-41. Change OAM Polling Interval Dialog Box

2. Enter the new time interval (in seconds) for collecting loopback diagnostics.

3. Choose Apply, the Close.

Accessing OAM Loopback Test Functions for PVCs

To access the OAM loopback test functions for PVCs:

1. On the network map, select the appropriate switch object.

2. From the Monitor menu, select Ascend Objects ⇒ Show Circuits and select one of the following options:

All by Name — Enter a specific circuit name. To use wild-card characters to search by name, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

All on Switch — Select a switch on the current map, then use this option to view a list of all the circuits configured for this switch.

All on Switch and by Name — Select a switch on the current map, then use this option to enter a specific circuit to search by name. To use wild-card characters, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

All on Map — Displays a list of all the circuits configured for the current map.

All by Defined Path — Displays a list of all circuits that have a defined path.

All Point-to-Multipoint — Displays a list of all point-to-multipoint circuits. See "Viewing Point-to-Multipoint PVCs" on page 13-23 for more information.

After you select one of these options, the Show All PVCs dialog box appears (Figure 13-1 on page 13-2), displaying a list of PVCs.

3. Select a PVC with a UNI logical port at both endpoints.
4. Choose OAM. The OAM Loopback dialog box appears. See "Starting PVC, SVC, and SPVC OAM Loopback Tests" on page 13-94 for more information.

Accessing the OAM Loopback Test Functions for SVCs

To access the OAM loopback test functions for SVCs:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Active SVCs. The Show All Active SVCs dialog box appears (Figure 13-31 on page 13-71).
2. Select a switch.
3. Select an ATM logical port.
4. Choose Upload to upload all SVC records from the selected logical port. A list of SVC records appears.
5. Select the SVC to be tested.
6. Choose OAM. The OAM Loopback dialog box appears. See "Starting PVC, SVC, and SPVC OAM Loopback Tests" on page 13-94 for more information.

Accessing the OAM Loopback Test Functions for SPVCs

To access the OAM loopback test functions for point-to-point SPVCs:

1. From the Monitor menu, select Ascend Objects ⇒ Show All Soft PVC Parameters ⇒ Point-to-Point. The Show All Point-to-Point SPVCs dialog box appears (Figure 13-23 on page 13-48).
2. Select the name of the SPVC to be tested.
3. Choose OAM. The OAM Loopback dialog box appears. See "Starting PVC, SVC, and SPVC OAM Loopback Tests" on page 13-94 for more information.

Starting PVC, SVC, and SPVC OAM Loopback Tests

To start a PVC, SVC, and SPVC OAM loopback test:

1. Access the loopback test functions as described in the previous sections. Figure 13-42 and Figure 13-43 show sample OAM Loopback dialog boxes.

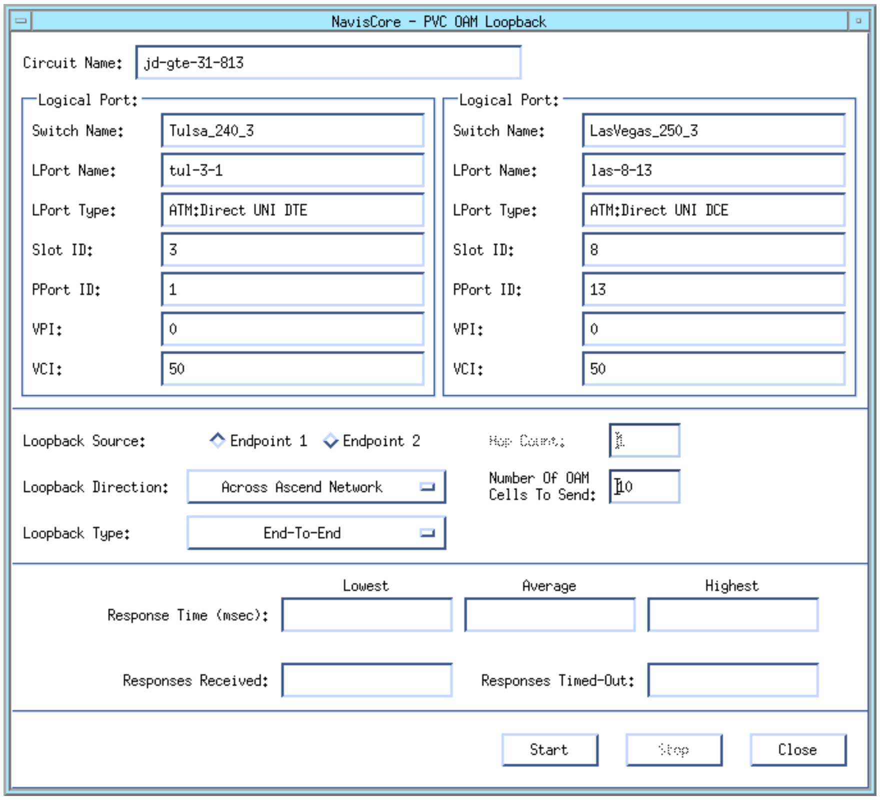


Figure 13-42. PVC OAM Loopback Dialog Box

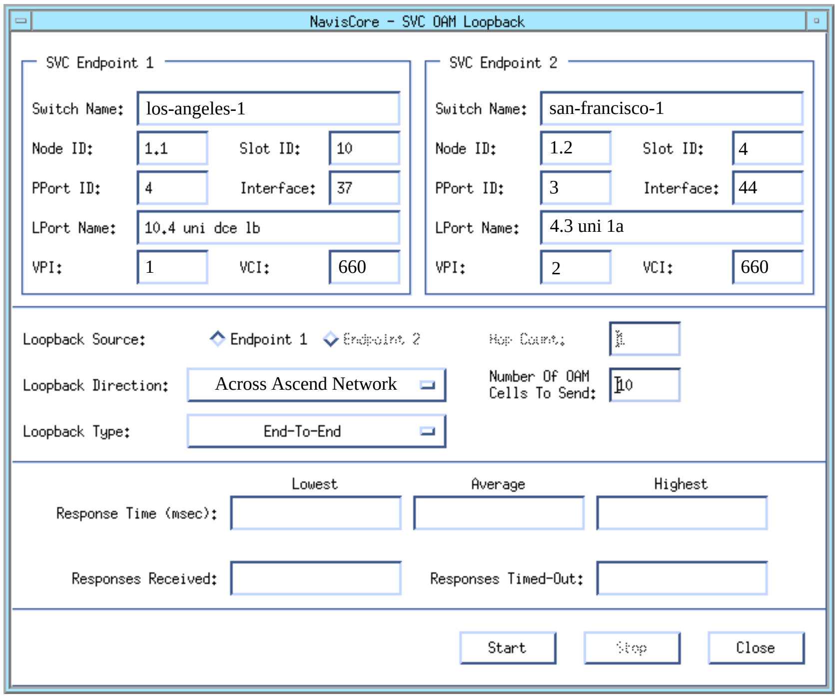


Figure 13-43. SVC OAM Loopback Dialog Box

2. Complete the fields (except for the display fields) described in Table 13-34.

Table 13-34. PVC, SVC, and SPVC OAM Loopback Fields

Field	Action/Description
Loopback Source	Select either *Endpoint 1* or *Endpoint 2* as the source of the loopback signal.
Loopback Direction	Select one of the following options: *Out Interface* – Enables you to send the OAM cells out the UNI/NNI port to the attached ATM device, such as a router. *Across Ascend Network* – Enables you to send the OAM cells over the trunk to the connected Ascend switch.
Loopback Type	Select one of the following options: *Segment* – Sends OAM loopback segment cells to the next attached device. If you send the loopback across the Ascend network, this option sends the loopback cells to the other endpoint switch (unless the specified Hop Count is less than the number of hops required to reach the other endpoint). *End-To-End* – Sends a signal across the network to the circuit endpoint.
Hop Count	Specify the number of hops for this circuit. This option is available only if you select *Across the Ascend Network* in the Loopback Direction field and *Segment* in the Loopback Type field. Initially you specify a minimum number of hops and gradually increase this number until you isolate the problem.
Number of OAM Cells to Send	Specify the number of OAM cells to send. Initially, send a minimum number of cells, for example, 10 cells.
Display Fields Only	
Response Time (msec)	The lowest, average, and highest response time.
Responses Received	The number of responses received.
Responses Timed-Out	The number of responses that timed out.

3. Choose Start to begin loopback testing. The system displays the test results at the bottom of the OAM Loopback dialog box.

   NavisCore updates the following information at each polling interval until you choose Stop to end the test:

   - Response time
   - Responses received
   - Responses timed-out

4. Choose Stop to stop the test and return to a normal operating state.

14

Monitoring Frame Relay Circuits

This chapter describes how to monitor Frame Relay circuits. Ascend switches support Frame Relay communications over the following types of circuits:

- Permanent virtual circuits (PVCs)
- Switched virtual circuits (SVCs)

Viewing Frame Relay PVCs

This section describes how to view the status of Frame Relay PVCs, Frame Relay Quality of Service (QoS) statistics for PVCs, and Frame Relay PVC summary statistics.

Viewing Frame Relay PVC Status

To view the current configuration, status, and routing information for all point-to-point PVCs in the network:

1. From the Monitor menu, select Ascend Objects ⇒ Show Circuits and select one of the following options:

All by Name — Enter a circuit name. To use wild-card characters to search by name, type an asterisk (*) to replace several characters or a question mark (?) to replace one character.

All on Switch — Select a switch on the current map, then select this option to view a list of all the circuits configured for this switch.

All on Switch and by Name — Select a switch on the current map, then use this option to enter a specific circuit to search by name. To use wild-card characters. type an asterisk (*) to replace several characters or a question mark (?) to replace one character.

All on Map — Displays a list of all circuits configured for the current map.

All by Defined Path — Displays a list of all circuits that have a defined path.

All Point-to-Multipoint — Displays a list of all point-to-multipoint circuits. See "Viewing Point-to-Multipoint PVCs" on page 13-23 for more information.

After you select an option, the Show All PVCs dialog box appears. Figure 14-1 shows a sample dialog box with a selected Frame Relay PVC.

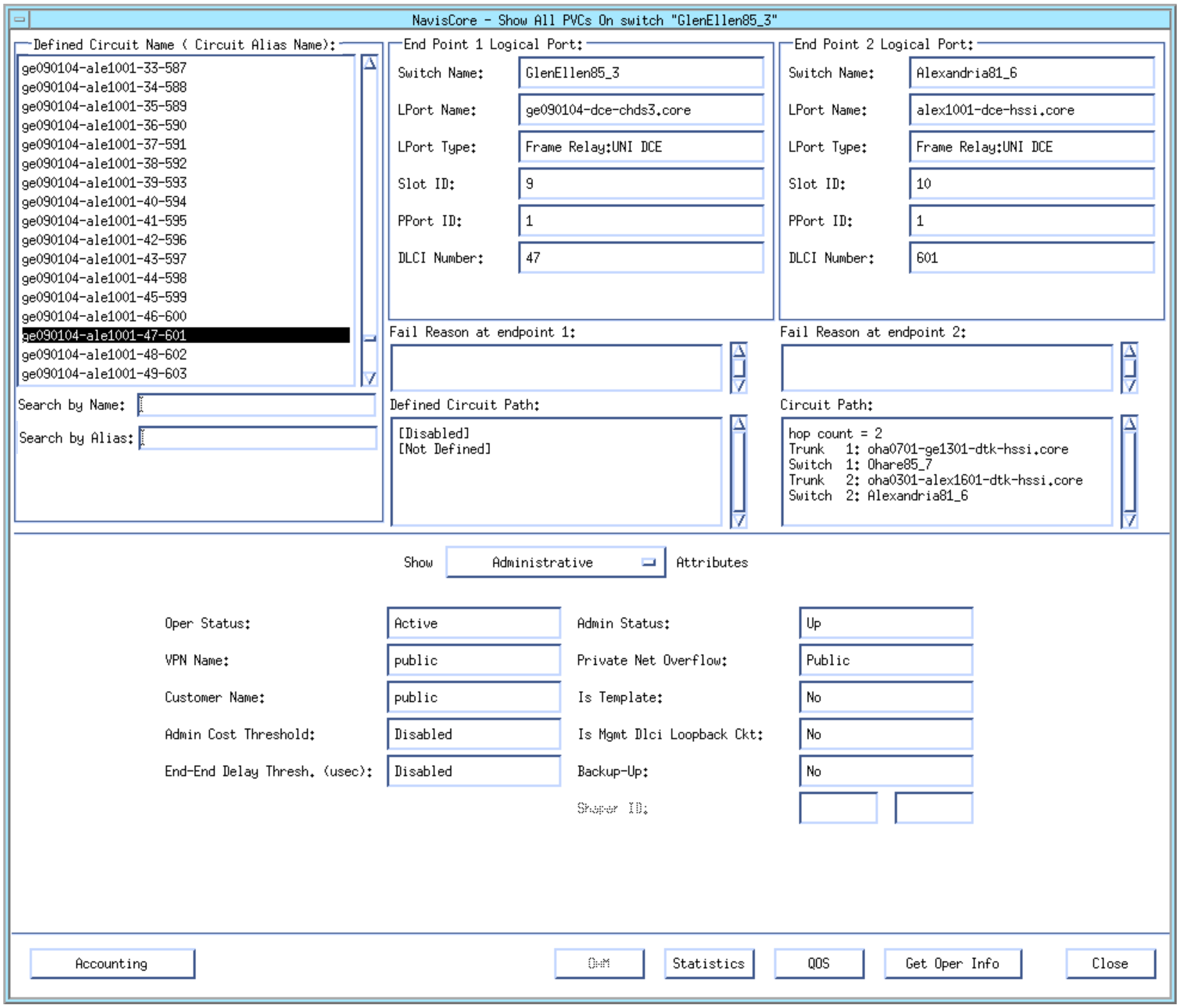


Figure 14-1. Show All PVCs Dialog Box (Frame Relay PVC and Administrative Attributes)

> ▶ If the circuit names do not appear immediately in the Defined Circuit Name list box, insert the cursor in the blank Search by Name field and press Return. This action will display a list of configured circuits.

2. Select the name of the circuit for which you want to retrieve status information. Use the Search by Name and Search by Alias fields to enter wild-card characters:
   - Use an * to match any number of characters
   - Use a ? to match a single character
   - Type ***** to match the * character
   - Type **?** to match the ? character
   - Type \\ to match the \ character

The fields on the Show All PVCs dialog box vary, depending on how the selected PVC is configured. For example, Frame Relay PVC fields differ from ATM PVC fields. See Chapter 13, "Monitoring ATM Circuits" for information about ATM PVCs.

The Show All PVCs dialog box displays general PVC information at the top of the dialog box and provides an option menu at the bottom of the dialog box, enabling you to select and view different PVC attributes.

See the following sections to view PVC attribute information:

PVC Attribute	See...
Administrative	"Viewing Frame Relay PVC Administrative Attributes" on page 14-8.
Common User Preference	"Viewing Frame Relay PVC Common User-Preference Attributes" on page 14-10.
Frame User Preference	"Viewing Frame Relay PVC Frame User-Preference Attributes" on page 14-11.
Traffic Type	"Viewing Frame Relay PVC Traffic Type Attributes" on page 14-13.

Table 14-1 describes general PVC field information.

Table 14-1. General PVC Information Fields (Frame Relay PVCs)

Field	Displays...
Defined Circuit Name	A list of the PVCs in the network.
Logical Port – Information about the two logical-port endpoints.	
Switch Name	The switch name at each circuit endpoint.
LPort Name	The logical-port name at each circuit endpoint.
LPort Type	The configured logical port type.
Slot ID	The slot number of the circuit's I/O module.
PPort ID	The number of the physical port on which the circuit is configured.
DLCI Number	The data link connection identifier (DLCI) number configured for the circuit endpoint. See the *NavisCore Frame Relay Configuration Guide* for a complete description of this field and its use.
Fail Reason at endpoint 1 (2)	The reason a selected circuit failed (if any) for a given endpoint. See Table 14-3 for information about inactive-PVC status codes.
Defined Circuit Path	The configured circuit path.
Actual Circuit Path	The actual path that OSPF used to direct this circuit.

▶ The Show All PVCs dialog box displays the circuit names and circuit attributes as configured in the NMS. The Status, Path, and Fail Reasons are extracted directly from the switch.

Table 14-2 describes the option menu and buttons on the dialog box.

Table 14-2. Show All PVCs Buttons

Button	Function
Show Attributes (option menu)	Displays an option menu from which you can select Frame Relay PVC attributes.
Accounting	Accesses the accounting functions for a PVC. For more information, see the *NavisXtend Accounting Server Administrator's Guide.*
Statistics	Displays the summary statistics for the selected circuit.
QOS	Displays Quality of Service/class of service statistics for the selected circuit. See the section "Viewing QOS Statistics for Frame Relay PVCs" on page 14-15 for details.
Get Oper Info	Updates the values in the fields.
Close	Exits the dialog box.

Table 14-3 describes the inactive-PVC operational status codes.

Table 14-3. Inactive-PVC Operational Status Codes

Fail Reason	Description	Solution
Circuit Admin Status is Down	Circuit activity is disabled; the admin status is set to Down.	Reconfigure the circuit's admin status to Up.
Internal Error: No VC Buffer at [*node*]	A shortage of virtual circuit buffers exists at the node.	**Serious Error! Report problem to the Ascend Technical Assistance Center.**
Not enough bandwidth on trunk at [*node*]	One of the trunks in the circuit path does not have enough bandwidth to accommodate the circuit.	Reconfigure the circuit to a lower bandwidth or increase the physical or virtual bandwidth of the trunk. You can also add more parallel trunks. Keep in mind that increasing the physical or virtual trunk bandwidth will temporarily disrupt traffic on the trunk.
Destination node is unreachable at [*node*]	The destination node is not accessible from the higher numbered node.	Troubleshoot a possible connectivity problem with the unreachable switch.
Ascend circuit segment call has timed out	Attempts to establish the circuit (PVC) through the network have failed and timed out.	This problem may occur on a defined path where the alternate path option is disabled.
Internal error: No circuit PDU buffer at [*node*]	A shortage of protocol buffers exists.	**This is a serious problem! Report this error to the Ascend Technical Assistance Center.**

Table 14-3. Inactive-PVC Operational Status Codes (Continued)

Fail Reason	Description	Solution
OPTimum path flow is blocked at [*node*]	Data flow through the public data network is temporarily blocked due to the flow-control mechanism.	This condition should correct itself. If the problem persists, check for congestion in the OPTimum path.
Trunk is down at [*node*]	A trunk line in the circuit path is down.	The circuit automatically reroutes if alternate paths are defined.
UNI/NNI is down at [*node, lport*]	The UNI or NNI is down at the node/interface number (ifnum).	Make sure the switch is connected to the user device. Display traffic in and out of the port by generating summary statistics.
PVC segments are not ready to receive beyond [*lport, node*]	(NNI specific problem.) The PVC segment(s) beyond this logical port sent a flow block message stating that it cannot receive data.	A trunk line in the circuit path may be down. Check the status of all PVC segments in the network beyond the logical port noted in the Fail Reason.
Warning: Defined Path is not available. The alternate path is in use. PVC segments are inactive beyond [*lport, node*]	The caller node cannot be reached through the defined path. This problem may be caused by a connection failure.	Verify the integrity of the trunk that is being used on the defined circuit path. Once the defined path is re-established, the circuit is routed back to the defined path within 20 seconds of availability.
IOP/IOM is down	An IOM used by the circuit is down.	Check the status of the IOM. See Chapter 2, “Viewing Switch, Module, and Physical Port Details” for more information.
No PVC Manager PDU msg buffer	The PVC manager has no user message buffer for the PDU.	**This is a serious problem! Report this error to the Ascend Technical Assistance Center**.
Port is not configured	No logical port is configured for use by the PVC.	Configure a logical port for the PVC. See the *NavisCore Frame Relay Configuration Guide* for details.
Mis-configuration	Configuration error.	Check the PVC attributes as described in this chapter.
Source is in a ‘backup’ condition	The PVC switched over to a backup.	Check PVC attributes and statistics. See “Viewing Frame Relay PVCs” on page 14-1.
Source is unknown.	The PVC source is unknown.	Check PVC attributes and statistics. See “Viewing Frame Relay PVCs” on page 14-1.

Table 14-3. Inactive-PVC Operational Status Codes (Continued)

Fail Reason	Description	Solution
Destination is unknown	The PVC destination is unknown.	Check PVC attributes and statistics. See "Viewing Frame Relay PVCs" on page 14-1.
DLCI collision on backup	DLCI collision occurred during backup.	Check PVC attributes and statistics. See "Viewing Frame Relay PVCs" on page 14-1.
Node running incompatible version of switch software exists in circuit path	A switch that is running an incompatible version of software is in the circuit path.	Verify that all switches in the circuit path are running compatible versions of switch software.
SMDS management trunk	The PVC attempted to traverse an SMDS management trunk.	Reroute the PVC so that it does not traverse an SMDS management trunk.
Endpoint never called	The PVC connection was never established.	Check PVC attributes and statistics. See "Viewing Frame Relay PVCs" on page 14-1.
Both endpoints in 'backup'	Both PVC endpoints are in a backup condition (that is, they are switching to backup PVCs).	Check PVC attributes and statistics. See "Viewing Frame Relay PVCs" on page 14-1.
Attempting to route through management trunk	The PVC attempted to traverse a management trunk.	Reroute the PVC so that it does not traverse a management trunk.
Route changed during setup	The PVC route failed because it changed during PVC setup.	Make sure that the route that the PVC is to take is stable during setup.
Circuit path registration failed	Problems were encountered during PVC path registration.	Check PVC attributes and statistics. See "Viewing Frame Relay PVCs" on page 14-1.
No available bandwidth in reverse direction	No bandwidth in the reverse direction is available.	Check the PVC configuration to see if sufficient bandwidth is available.
PVC reset internally – reuse path	The PVC reset internally as a result of multicast DLCI configuration problems.	Check the multicast DLCI configuration. See "Viewing the Status of Multicast DLCIs" on page 9-25 for details.
Disrupted due to priority routing	High-priority circuit is in the PVC's path. The PVC is disrupted due to priority routing.	Network congestion or other problems initiated priority-routing algorithms, which disrupted the PVC. This condition should clear as soon as the problem(s) is corrected.

Table 14-3. Inactive-PVC Operational Status Codes (Continued)

Fail Reason	Description	Solution
Couldn't allocate negative priority bandwidth	No negative priority bandwidth could be allocated.	Check the PVC configuration to see if sufficient bandwidth is available.

Viewing Frame Relay PVC Administrative Attributes

To view Frame Relay PVC administrative attributes, from the Show All PVCs dialog box (Figure 14-1 on page 14-2), select the Frame Relay PVC you want to view. The administrative attributes appear by default.

Table 14-4 describes the Frame Relay PVC administrative attributes fields.

Table 14-4. Frame Relay PVC Administrative Attributes Fields

Field	Displays...
Oper Status	The operational status of the PVC. There are four possible values: *Active* – The PVC is operational between the two endpoints. *Inactive* – The PVC is not operational between the two endpoints. A status of Inactive could mean that LMI operator status for the PVC's logical port is Down. See "Troubleshooting a Frame Relay Logical Port" on page 9-28 for more information. *Invalid* – The PVC configuration is not contained within the calling node. *Unknown* – The calling node did not respond to the NMS' request for PVC status.
VPN Name	The VPN name for the PVC (if applicable); *Public* if the PVC is not reserved for a VPN.
Customer Name	The customer name for the selected PVC (if applicable); otherwise, *Public*.
Admin Cost Threshold	The maximum administrative cost for the circuit. The circuit cannot be established unless at least one path with a cost less than or equal to the admin cost is available. This cost allows administrators to create paths manually. If the switch encounters problems establishing circuits over manually defined paths, increase the cost.
End-End Delay Thresh (µsec)	One of the following: *Enabled* – The end-to-end delay feature is enabled. *Disabled* – The end-to-end delay feature is disabled.
Admin Status	One of the following: *Up* – The admin status of the circuit is up. *Down* – The admin status of the circuit is down.

Table 14-4. Frame Relay PVC Administrative Attributes Fields (Continued)

Field	Displays...
Private Net Overflow	One of the following: *Public* – The customer is allowed to use a public trunk in the event of overflow or trunk failure. *Restrict* – The customer is restricted to its own VPN trunks during overflow or trunk failure.
Is Template	One of the following: *Yes* – This circuit connection was defined as a template. *No* – This connection is not a template.
Is Mgmt Dlci Loopback Ckt	One of the following: *Yes* – The circuit is the management DLCI loopback circuit. *No* – The circuit is not the management DLCI loopback circuit.
Backed-Up	One of the following: *Yes* – This circuit has a backup circuit. *No* – This circuit does not have a backup circuit.

Viewing Frame Relay PVC Common User-Preference Attributes

To view Frame Relay PVC common user-preference attributes:

1. From the Show All PVCs dialog box (Figure 14-1 on page 14-2), select the Frame Relay PVC you want to view.
2. Choose Show Common User Preference Attributes. The attributes fields appear (see Figure 14-2).

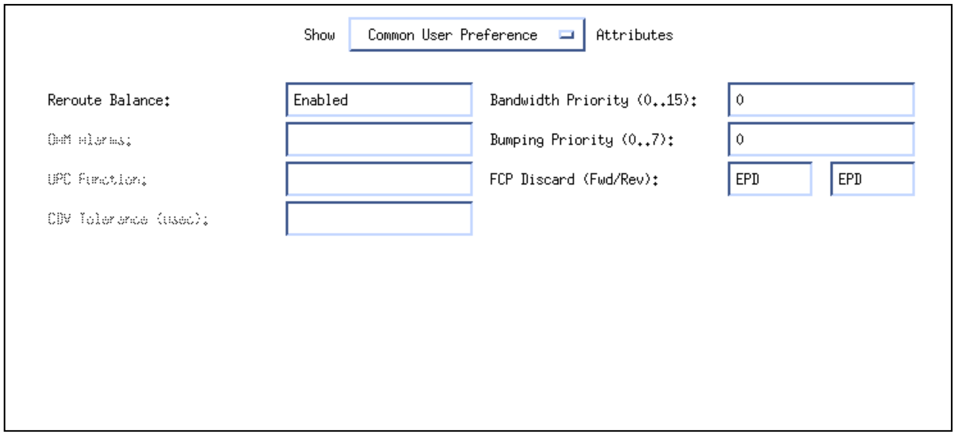


Figure 14-2. Frame Relay PVC Common User-Preference Attributes Fields

Table 14-5 describes the common user-preference attributes fields.

Table 14-5. Frame Relay PVC Common User-Preference Attributes Fields

Field	Displays...
Reroute Balance	One of the following: *Enabled* (the default) – Switch tuning parameters take effect for the circuit. *Disabled* – Switch tuning parameters are ignored for the circuit.
Bandwidth Priority	The bandwidth priority for the circuit, which is a value from 0 through 15 where 0 indicates the highest priority. In the event of provisioning, trunk failure recovery, or load balance rerouting, VCs use the combination of bandwidth priority and bumping priority to preserve proper routing priority. See "Viewing SVC Routing Priorities" on page 9-12 for a description of bandwidth priority.
Bumping Priority	The bumping priority for the circuit, which is a number from 0 through 7 where 0 indicates the highest priority. In the event of provisioning, trunk failure recovery, or load balance rerouting, VCs use the combination of bandwidth priority and bumping priority to preserve proper routing priority. See "Viewing SVC Routing Priorities" on page 9-12 for a description of bumping priority.

Table 14-5. Frame Relay PVC Common User-Preference Attributes Fields (Continued)

Field	Displays...
FCP Discard (Fwd/Rev)	One of the following values for both the forward and reverse directions: *CLP1* – For UBR, ABR, and VBRnrt PVCs, the ATM Flow Control Processor (FCP) discards each cell with CLP set to 1 that causes the PVC queue to exceed the discard thresholds. This flow control technique is also known as “Selective Discard.” *EPD* – For UBR, ABR, and VBRnrt PVCs, the FCP performs early packet discard (EPD). If a cell causes the queue for a PVC to exceed the discard thresholds, the PVC enters the EPD state. This means that the cells in the current packet are admitted to the queue. However, when the end of the current packet is detected, all of the cells in the next packet are discarded.

Viewing Frame Relay PVC Frame User-Preference Attributes

To view Frame Relay PVC frame user-preference attributes:

1. From the Show All PVCs dialog box (see Figure 14-1 on page 14-2), select the Frame Relay PVC you want to view.
2. Choose Show Frame User Preference Attributes. The attributes fields appear (see Figure 14-3).

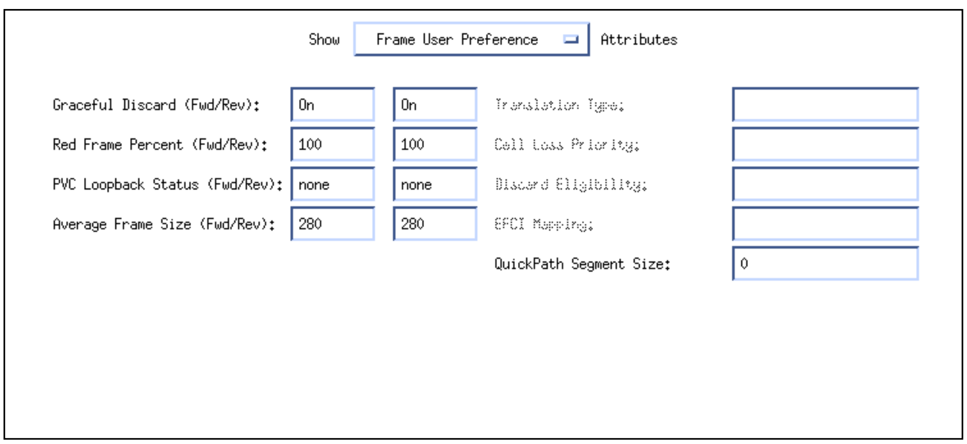


Figure 14-3. Frame Relay PVC Frame User-Preference Attributes Fields

Table 14-6 describes the frame user-preference attributes fields.

Table 14-6. Frame Relay PVC Frame User-Preference Attributes Fields

Field	Displays...
Graceful Discard (Fwd/Rev)	How “red” frames are handled on the selected circuit, either forwarded (On) or discarded (Off). Red frames are designated as the bits that are received during the current time interval, including the current frame that exceeds Excess Burst Size (Be).
Red Frame Percent (Fwd/Rev)	The percentage of red frames that were discarded (when graceful discard is not set to on). The default value for this field is 100% when graceful discard is set to on.
PVC Loopback Status (Fwd/Rev)	The loopback status of each endpoint. Possible settings are *None, Local, Remote,* or *Both.* See “Testing Frame Relay PVCs” on page 14-54 for more information.
Average Frame Size (Fwd/Rev)	The average frame size (in bytes) of the frames on the circuit. This value is used to calculate Call Admission Control (CAC) parameters for the circuit. See “Viewing CAC Parameters for Frame Relay Circuits” on page 14-25 for more information.
Translation Type (ATM-to-Frame Internetworking Circuits only)	The translation method used for an ATM protocol: *None* – Each end of the circuit uses the 1490 protocol. *RFC 1490 ⟺ 1483* – Indicates that you have a Frame Relay logical port on endpoint 1 and an ATM logical port on endpoint 2. *RFC 1483 ⟺ 1490* – Indicates that you have an ATM logical port on endpoint 1 and a Frame Relay logical port on endpoint 2.
Cell Loss Priority (CLP) (ATM-to-Frame Internetworking Circuits only)	The CLP setting for ATM-to-Frame internetworking. Valid values are: *clp0* – Sets the CLP bit in the cell header to 0, making CLP0 cells eligible for discard. *clp1* – Sets the CLP bit in the cell header to 1, making CLP1 cells eligible for discard. *fr-de* – Sets the CLP bit in the cell header to the same value as the DE bit in the frames. This action maps the DE bit in frames to the CLP bit in cells.
Discard Eligibility (DE) (ATM-to-Frame Internetworking Circuits only)	The DE setting for ATM-to-Frame internetworking. Valid values are: *de0* – Sets the DE bit in the frame header to 0, making DE0 frames eligible for discard. *de1* – Sets the DE bit in the frame header to 1, making DE1 frames eligible for discard. *atm-clp* – Sets the CLP bit in the header of the last cell in the frame to the value of the DE bit in the frame header.

Table 14-6. Frame Relay PVC Frame User-Preference Attributes Fields (Continued)

Field	Displays...
EFCI Marking (ATM-to-Frame Internetworking Circuits only)	The EFCI bit mapping for frames that are to be segmented for transmission on an ATM trunk. Possible values are as follows: *fr-fecn* – When the switch segments the frame into cells for transmission, the switch sets the value of the EFCI bit to the value of the congestion (FECN) bit. The mapping occurs just before the frame passes to the hardware for segmentation. *efci0* – The value of the EFCI bit is 0 for all cells (that is, the frame segments) that are transmitted on the trunk.
QuickPath Segment Size	The QuickPath segment size.

Viewing Frame Relay PVC Traffic Type Attributes

To view Frame Relay PVC traffic type attributes:

1. From the Show All PVCs dialog box (Figure 14-1 on page 14-2), select the Frame Relay PVC you want to view.
2. Choose Show Traffic Type Attributes. The attributes fields appear (see Figure 14-4).

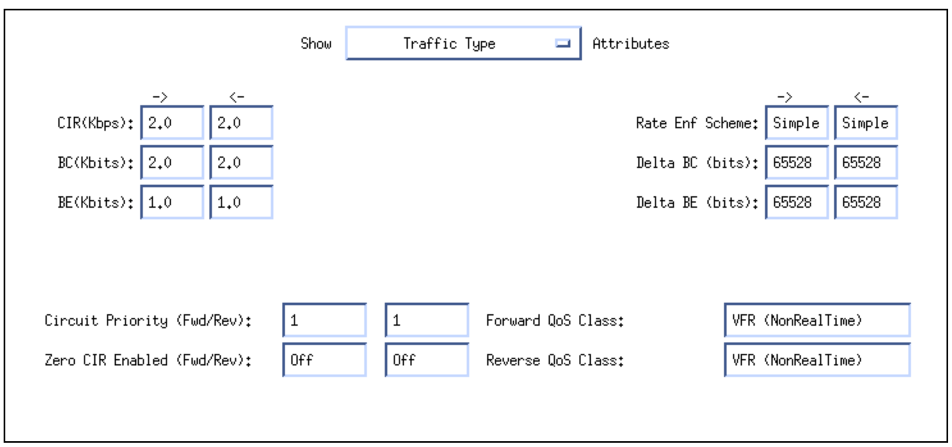


Figure 14-4. Frame Relay PVC Traffic Type Attributes Fields

Table 14-7 describes the traffic type attributes fields.

Table 14-7. Frame Relay PVC Traffic Type Attributes Fields

Field	Displays...
CIR (Committed Information Rate) (Kbps)	The configured CIR rate, in Kbps, at which the network transfers information under normal operating conditions for the selected circuit. The rate is averaged over a minimum increment of Tc. Values are displayed for both forward and reverse directions.
BC (Committed Burst Size) (Kbits)	The maximum amount of bits during time interval T that the network agrees to accept under normal conditions. Bc is defined for each circuit. Values are displayed for both forward and reverse directions.
BE (Excess Burst Size) (Kbits)	The maximum number of uncommitted bits during time interval T that the network agrees to accept above the committed burst size, Bc. The network considers this data eligible for discard by the network if you do not enable the Graceful Discard option. Values are displayed for both forward and reverse directions.
Rate Enf Scheme	One of the following configurable rate enforcement schemes (values are displayed for both forward and reverse directions): *Simple* – Provides better switch performance (but less accurate rate enforcement) than the *Jump* scheme. *Jump* – Provides more accurate rate enforcement (but slightly worse switch performance) than the *Simple* scheme. See the *NavisCore Frame Relay Configuration Guide* for more information.
Delta BC (bits)	The maximum number of bits the network agrees to transfer over the circuit (as committed bits) during the measurement interval provided. There is positive committed bit (Bc) credits before receiving the frame, but negative Bc credits after accepting the frame. Values are displayed for both forward and reverse directions.
Delta BE (bits)	The maximum number of bits the network agrees to transfer over the circuit (as committed bits) during the measurement interval provided. There is positive committed bit (Be) credits before receiving the frame, but negative Be credits after accepting the frame. Values are displayed for both forward and reverse directions.
Circuit Priority	The value used to control the priority of green frames traveling over the circuit—the lower the value, the higher the priority. The specific value that appears depends on the combination of switches where the endpoints reside, and the service they use to communicate: CBX 500 <--> CBX 500 – 1 (ATM); 2 (Frame Relay) CBX 500 <--> B-STDX 9000 – 2 (All Services) B-STDX 9000 <--> B-STDX 9000 – 2 (All Services)

Table 14-7. Frame Relay PVC Traffic Type Attributes Fields (Continued)

Field	Displays...
Zero CIR Enabled	One of the following: *On* – The PVC has an assigned CIR value of zero and is a best-effort delivery service. Customers who subscribe to zero CIR service are allowed to burst to the port speed if there is network bandwidth available to deliver frames. However, no guarantees are made to deliver frames. All frames entering the network on a zero CIR PVC have DE set to one. *Off* – The PVC does not have an assigned CIR value of zero.
Forward QoS Class	The Quality of Service (QoS) class for forward traffic.
Reverse QoS Class	The QoS class for reverse traffic (it does not have to be the same as the forward QoS class).

Viewing QOS Statistics for Frame Relay PVCs

To view Quality of Service (QOS) statistics for Frame Relay circuits:

1. From the Monitor menu, select Ascend Objects ⇒ Show Circuits and select one of the following options:

   All by Name — Enter a specific circuit name. To use wild-card characters to search by name, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

   All on Switch — Select a switch on the current map, then use this option to view a list of all the circuits configured for this switch.

   All on Switch and by Name — Select a switch on the current map, then use this option to enter a specific circuit to search by name. To use wild-card characters, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

   All on Map — Displays a list of all the circuits configured for the current map.

   All by Defined Path — Displays a list of all circuits that have a defined path.

   All Point-to-Multipoint — Displays a list of all point-to-multipoint circuits. See “Viewing Point-to-Multipoint PVCs” on page 13-23 for more information.

   The Show All PVCs dialog box appears (Figure 14-1 on page 14-2).

2. Select a Frame Relay circuit from the Defined Circuit Name list box. Use **one of the following methods** to select the circuit:
   – Point and click on the circuit name.
   – Specify the name of the circuit in the Search by Name field and press Return.

3. Choose QOS to view the Circuit Quality of Service Statistics dialog box (see Figure 14-5).

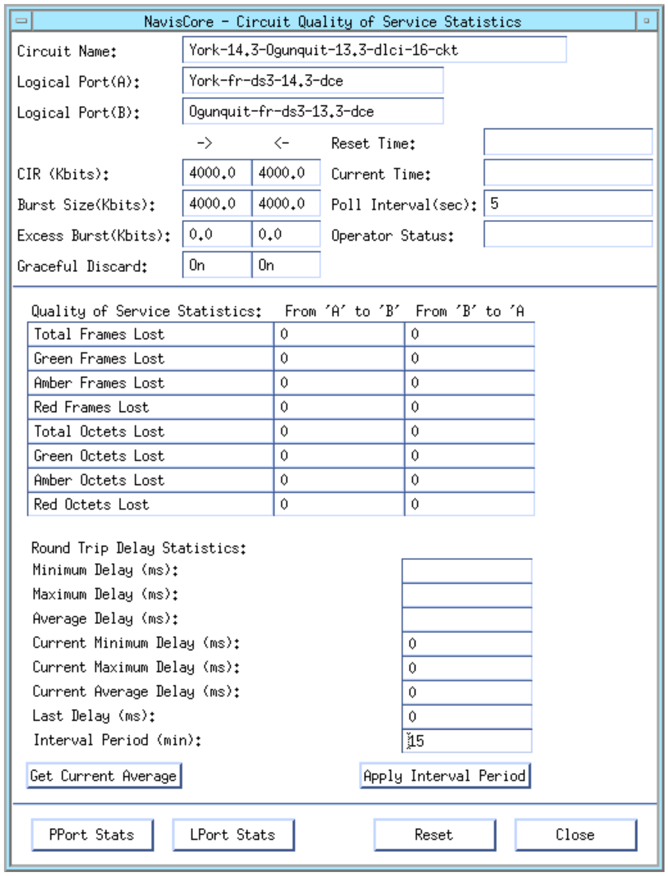


Figure 14-5. Circuit Quality of Service Statistics Dialog Box (Frame Relay)

The Quality of Service Statistics measure the various classes of packets in the network for the selected circuit, as well as the number of packets discarded. In addition, they provide round-trip delay statistics for the selected circuit.

The NMS takes round-trip delay measurements during a modifiable interval period and uses these measurements to maintain two sets of statistics:

Current — Minimum/maximum/average statistics for the current interval period.

Previous — Minimum/maximum/average statistics for the previous interval period.

For example, if you set the Interval Period field to 60, the NMS takes measurements over the next hour. During that time, it calculates the Current Minimum Delay, Current Maximum Delay, and Current Average Delay statistics values. When the hour is up, the NMS stores the Current Min/Max/Avg Delay values for that time period in the Min/Max/Avg Delay fields, and starts calculating Current Min/Max/Avg values for the new 1-hour time period.

Table 14-8 describes the buttons on the Circuit Quality of Service Statistics dialog box.

Table 14-8. Circuit Quality of Service Statistics Buttons (Frame Relay)

Button	Function
Get Current Average	Updates the Current Average Delay field.
Apply Interval Period	Updates the interval period with any changes you have made in the Interval Period field.
PPort Stats	Retrieves statistics on physical port activity at both ends of the PVC. Two Physical Port Summary Statistics dialog boxes appear—one for each end of the PVC.
LPort Stats	Retrieves statistics on logical port activity at both ends of the PVC. Two Logical Port Summary Statistics dialog boxes appear—one for each end of the PVC.
Reset	Resets cumulative statistics only. This button does not reset round-trip delay statistics.
Close	Exits the dialog box.

Table 14-9 describes the Circuit Quality of Service Summary Statistics fields.

Table 14-9. Circuit Quality of Service Statistics (Frame Relay PVCs)

Statistic	Description
Configuration Information	
Circuit Name	The name of the circuit.
Logical Port A	The logical port defined as endpoint 1 of the circuit configuration.
Logical Port B	The logical port defined as endpoint 2 of the circuit configuration.
CIR (Kbits)	The rate at which the network transfers data under normal conditions. Normal conditions refer to a properly designed network with ample bandwidth and switch capacity. The rate is averaged over a minimum increment of the Committed Rate Measurement Interval (Tc).
Burst Size (Kbits)	The maximum amount of data, in Kbits, that the network will attempt to transfer under normal conditions during a specified time interval, Tc. Tc is calculated as BC/CIR. This value must be greater than zero and is typically set to the same value as CIR.
Excess Burst (Kbits)	The maximum amount of uncommitted data, in Kbits, that the network will attempt to deliver during a specified time interval, Tc. Tc is calculated as BC/CIR. The network treats this data as Discard Eligible (DE) data. NavisCore manages DE frames according to the Graceful Discard setting.

Table 14-9. Circuit Quality of Service Statistics (Frame Relay PVCs) (Continued)

Statistic	Description
Graceful Discard	A value of *On* or *Off* to indicate how this circuit handles red packets. Red packets are designated as those bits received during the current time interval that exceed the committed burst size (Bc) and excess burst size (Be) thresholds, including the current frame. The discard eligible (DE) bit for a red packet is set to 1, meaning that the network can discard this packet unless Graceful Discard is set to *On*.
Reset Time	The time of the last reset of the switch.
Current Time	The current system time.
Poll Interval (sec)	The time interval for the collection of statistical data.
Operator Status	The operational status of the PVC. There are four possible values: *Active* – The PVC is operational between the two endpoints. *Inactive* – The PVC is not operational between the two endpoints. *Invalid* – The PVC configuration is not contained within the calling node. *Unknown* – The calling node did not respond to the NMS' request for PVC status.
Cumulative Statistics	
Total Frames Lost	The total number of frames that were discarded over the specified logical ports since the last reset.
Green Frames Lost	The number of discarded green frames. Green frames are never discarded by the network, except under extreme circumstances (such as node or link failure). Green frames identify packets where the number of bits received during the current time interval, including the current frame, is less than the committed burst size (Bc).
Amber Frames Lost	The number of discarded amber frames. Amber frames are forwarded with the DE bit set and are eligible for discard if they pass through a congested node. Amber frames identify packets where the number of bits received during the current time interval, including the current frame, is greater than the committed burst size (Bc), but less than the excess burst size (Be).
Red Frames Lost	The number of discarded red frames. Red packets are forwarded with the DE bit set when the Graceful Discard feature is set to On. When the Graceful Discard feature is set to Off, red packets are discarded. Red packets are designated as those bits received during the current time interval that exceed the committed burst size (Bc) and excess burst size (Be) thresholds, including the current frame.
Total Octets Lost	The total number of octets (bytes) discarded over the specified logical ports since the last reset.

Table 14-9. Circuit Quality of Service Statistics (Frame Relay PVCs) (Continued)

Statistic	Description
Green Octets Lost	The number of discarded green octets. Green octets are never discarded by the network, except under extreme circumstances (such as node or link failure).
Amber Octets Lost	The number of discarded amber octets. Amber octets are eligible for discard if they pass through a congested node.
Red Octets Lost	The number of discarded red octets. Red octets are forwarded with the DE bit set when the Graceful Discard feature is set to On. When the Graceful Discard feature is set to Off, red octets are discarded.
Round Trip Delay Statistics	
Minimum Delay (ms)	The minimum time (in microseconds) that it took to transfer a packet from point A to point B of a circuit and then back to point A in the previous interval period.
Maximum Delay (ms)	The maximum time (in microseconds) that it took to transfer a packet from point A to point B of a circuit and then back to point A in the previous interval period.
Average Delay (ms)	The average time (in microseconds) that it took to transfer a packet from point A to point B of a circuit and then back to point A in the previous interval period.
Current Minimum Delay (ms)	The minimum time (in microseconds) that it takes to transfer a packet from point A to point B of a circuit and then back to point A in the current interval period.
Current Maximum Delay (ms)	The maximum time (in microseconds) that it takes to transfer a packet from point A to point B of a circuit and then back to point A in the current interval period.
Current Average Delay (ms)	The average time (in microseconds) that it takes to transfer a packet from point A to point B of a circuit and then back to point A in the current interval period. You can retrieve the latest average by choosing “Get Current Average.”
Last Delay (ms)	The most recent measurement of the time (in microseconds) that it takes to transfer a packet from point A to point B of a circuit and back to point A.
Interval Period (min)	The current interval period in minutes. The current interval period defines a span of time during which round-trip delay measurements are taken. You can modify this value by typing in a new one and choosing “Apply Interval Period.” The Interval Period can be from 5 minutes to 1440 minutes (24 hours). Any modification you make takes effect immediately, and begins a new time interval.

Viewing Frame Relay PVC Summary Statistics

Frame Relay circuit summary statistics display the packets a circuit has sent and received, the round-trip delay, and other QoS statistics for the circuit.

To view Frame Relay PVC statistics:

1. From the Monitor menu, select Ascend Objects ⇒ Show Circuits.
2. Select one of the following options:

   All by Name — Enter a specific circuit name. To use wild-card characters to search by name, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

   All on Switch — Select a switch on the current map, then use this option to view a list of all the circuits configured for this switch.

   All on Switch and by Name — Select a switch on the current map, then enter a specific circuit to search by name. To use wild-card characters, type an asterisk (*) to replace several characters or type a question mark (?) to replace one character.

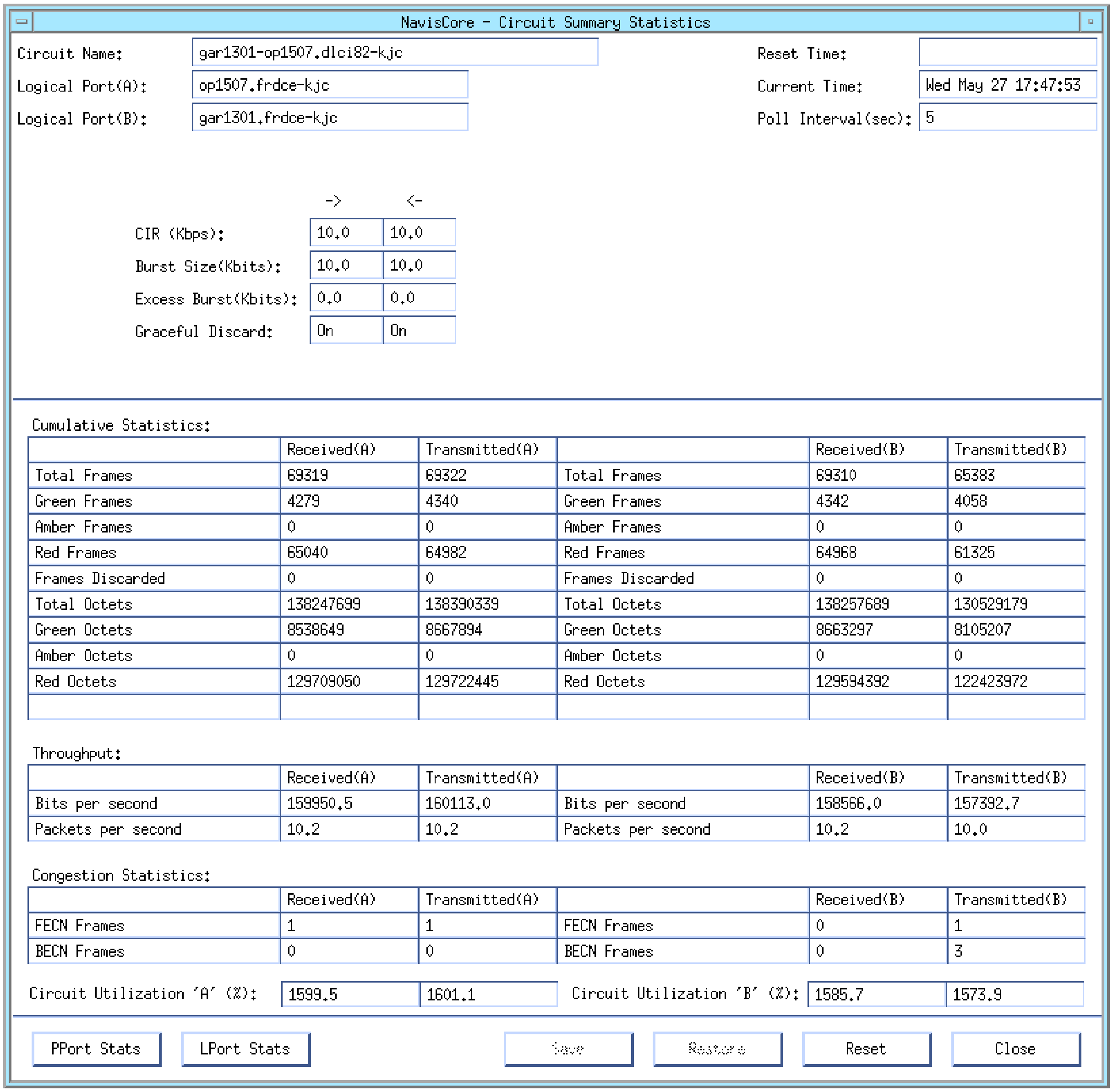
   All on Map — Displays a list of all the circuits configured for the current map.

   All by Defined Path — Displays a list of all circuits that have a defined path.

   All Point-to-Multipoint — Displays a list of all point-to-multipoint circuits. See “Viewing Point-to-Multipoint PVCs” on page 13-23 for more information.

   After you select an option, the Show All PVCs dialog box appears (Figure 14-1 on page 14-2).

3. Choose Statistics to view the PVC summary statistics. Figure 14-6 shows the Circuit Summary Statistics dialog box for Frame Relay circuits. Figure 14-7 shows the Circuit Summary Statistics dialog box for Frame-to-ATM circuits. See “Viewing Point-to-Point ATM PVC Summary Statistics” on page 13-18 for information about ATM circuit summary statistics.


NavisCore - Circuit Summary Statistics

Circuit Name: gar1301-op1507.dlci82-kjc
Logical Port(A): op1507.frdce-kjc
Logical Port(B): gar1301.frdce-kjc
Reset Time:
Current Time: Wed May 27 17:47:53
Poll Interval(sec): 5

	->	<-
CIR (Kbps):	10.0	10.0
Burst Size(Kbits):	10.0	10.0
Excess Burst(Kbits):	0.0	0.0
Graceful Discard:	On	On

Cumulative Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Total Frames	69319	69322	Total Frames	69310	65383
Green Frames	4279	4340	Green Frames	4342	4058
Amber Frames	0	0	Amber Frames	0	0
Red Frames	65040	64982	Red Frames	64968	61325
Frames Discarded	0	0	Frames Discarded	0	0
Total Octets	138247699	138390339	Total Octets	138257689	130529179
Green Octets	8538649	8667894	Green Octets	8663297	8105207
Amber Octets	0	0	Amber Octets	0	0
Red Octets	129709050	129722445	Red Octets	129594392	122423972

Throughput:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Bits per second	159950.5	160113.0	Bits per second	158566.0	157392.7
Packets per second	10.2	10.2	Packets per second	10.2	10.0

Congestion Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
FECN Frames	1	1	FECN Frames	0	1
BECN Frames	0	0	BECN Frames	0	3

Circuit Utilization 'A' (%): 1599.5 1601.1
Circuit Utilization 'B' (%): 1585.7 1573.9

PPort Stats | LPort Stats | Save | Restore | Reset | Close

Figure 14-6. Circuit Summary Statistics Dialog Box (Frame Relay)

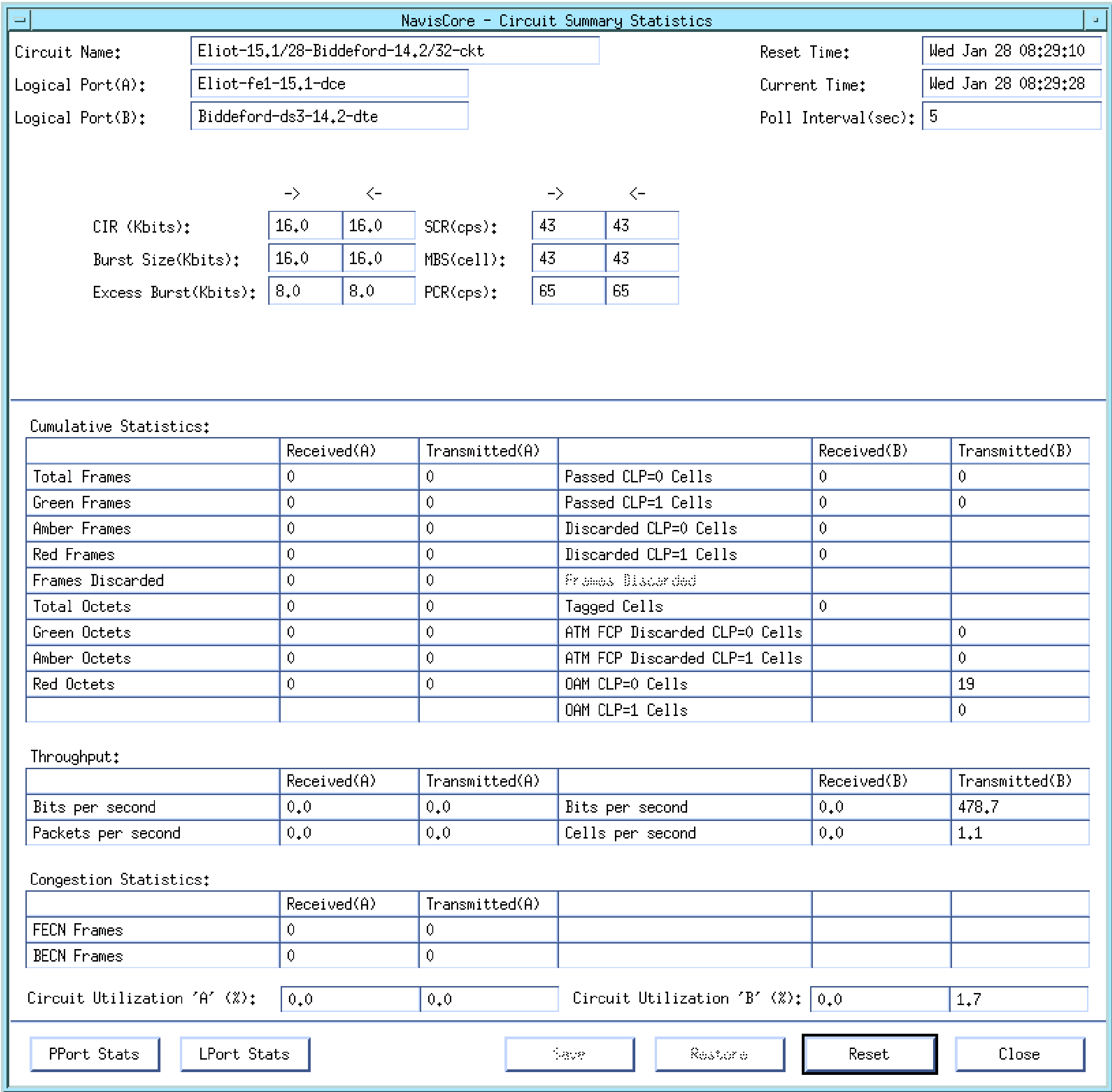


Figure 14-7. Circuit Summary Statistics Dialog Box (Frame-to-ATM)

This dialog box displays statistics for transmitted and received data for each circuit logical port endpoint (A and B). These statistics reflect how a circuit's data is used over the network.

For Frame-to-ATM circuits, ATM statistics appear for the ATM end of the circuit, and Frame Relay statistics appear for the Frame Relay end of the circuit. See "Viewing Point-to-Point ATM PVC Summary Statistics" on page 13-18 for information about ATM circuit summary statistics.

Table 14-10 describes the Frame Relay circuit summary statistics fields.

Table 14-10. Circuit Summary Statistics Fields (Frame Relay)

Statistic	Description
Circuit Name	The name of the circuit.
Logical Port (A)	The logical port at one circuit endpoint.
Logical Port (B)	The logical port at the other circuit endpoint.
Reset Time	The time of the last reset of the selected switch (if you are viewing all PVCs on switch).
Current Time	The current system time (if you are viewing all PVCs on switch).
Poll Interval (sec)	The time interval for the collection of statistical data.
CIR (Kbits)	The configured committed information rate (CIR), in Kbits, at which the network transfers information under normal operating conditions for the selected circuit.
Burst Size (Kbits)	The maximum amount of bits during a time interval that the network agrees to accept under normal conditions.
Excess Burst Size (Kbits)	The maximum number of uncommitted bits during a time interval that the network agrees to accept above the committed burst size. The network considers this data eligible for discard by the network if you do not enable the Graceful Discard option.
Graceful Discard	How "red" packets are handled on the selected circuit, either forwarded (*On*) or discarded (*Off*). Red packets are designated as the bits that are received during the current time interval, including the current frame that exceeds excess burst size.
Cumulative Statistics	
Total Frames	The total number of frames received and transmitted over the specified logical ports since the last reset.
Green Frames	The total number of green frames received and transmitted over the specified logical ports since the last reset. Green frames are never discarded by the network, except under extreme circumstances (such as node or link failure). Green frames identify packets where the number of bits received during the current time interval, including the current frame, is less than the committed burst size.

Table 14-10. Circuit Summary Statistics Fields (Frame Relay) (Continued)

Statistic	Description
Amber Frames	The total number of amber frames received and transmitted over the specified logical ports since the last reset. Amber frames are forwarded with the DE bit set and are eligible for discard if they pass through a congested node. Amber frames identify packets where the number of bits received during the current time interval, including the current frame, is greater than the committed burst size, but less than the excess burst size.
Red Frames	The total number of red frames received and transmitted over the specified logical ports since the last reset. Red packets are forwarded with the DE bit set when the Graceful Discard feature is set to On. When the Graceful Discard feature is set to Off, red packets are discarded. Red packets are designated as those bits received during the current time interval that exceed the committed burst size and excess burst size thresholds, including the current frame.
Total Octets	The total number of octets (bytes) received and transmitted over the specified logical ports since the last reset.
Green Octets	The total number of green octets (bytes) received and transmitted over the specified logical ports since the last reset. Green octets are never discarded by the network, except under extreme circumstances (such as node or link failure).
Amber Octets	The total number of amber octets (bytes) received and transmitted over the specified logical ports since the last reset. Amber octets are eligible for discard if they pass through a congested node.
Red Octets	The total number of red octets (bytes) received and transmitted over the specified logical ports since the last reset. Red octets are forwarded with the DE bit set when the Graceful Discard feature is set to On. When the Graceful Discard feature is set to Off, red octets are discarded.
Frames Discarded	The number of frames discarded. Congested nodes within the network that must discard packets use the color designations to determine which frames to discard. Red frames are discarded first, followed by amber and green.
Throughput Statistics	
Bits per Second	The number of bits transmitted and/or received each second.
Packets per second	The number of packet frames transmitted and/or received each second.

Table 14-10. Circuit Summary Statistics Fields (Frame Relay) (Continued)

Statistic	Description
Congestion Statistics	
FECN Frames	The number of frames that were received or transmitted with the Forward Explicit Congestion Notification (FECN) bit set to one. The network sets a FECN bit to one if the network is encountering congestion. FECN frames indicate that there may not be sufficient network resources to continue handling the submitted traffic at the current rate. See the *Networking Services Technology Overview* for more information.
BECN Frames	The number of frames that were received or transmitted with the Backward Explicit Congestion Notification (BECN) bit set to one. The network sets a BECN bit to one if the network is encountering congestion. BECN frames indicate that there may not be sufficient network resources to continue handling the submitted traffic at the current rate. See the *Networking Services Technology Overview* for more information.
Utilization Statistics	
Circuit Utilization A	The amount of traffic queued for transmission on a circuit as a percentage of the CIR. For this reason, the value displayed in circuit utilization A can exceed 100%.
Circuit Utilization B	The amount of traffic queued for transmission on a circuit as a percentage of the CIR. For this reason, the value displayed in circuit utilization B can exceed 100%.

Viewing CAC Parameters for Frame Relay Circuits

ATM and Frame Relay I/O modules that support Priority Frame™ share common Call Admission Control (CAC) QoS objectives that can be configured and monitored through NavisCore. For information on viewing QoS objectives, see "Viewing CAC Parameters for ATM Circuits" on page 13-87.

The switch uses a fixed average frame size and Frame Relay traffic descriptors to calculate the maximum burst size (MBS), sustained frame rate (SFR) and peak frame rate (PFR) for each circuit, as follows:

MBS = Bc/Avg. Frame Size
SFR = CIR/Avg. Frame Size
PFR = (CIR + EIR)/Avg. Frame Size
EIR = Be/Tc (where Tc = Bc/CIR)

See Table 14-7 on page 14-14 for descriptions of Bc, CIR, Be, and Tc. EIR is the information rate during excess traffic periods.

Troubleshooting Frame Relay PVCs

This section provides generic guidelines on troubleshooting Frame Relay PVCs. Use this section in conjunction with "Troubleshooting a Frame Relay Logical Port" on page 9-28.

Frame Relay PVC problems can be categorized as follows:

- PVC is inactive
- PVC is active but has performance issues (slow response or packet loss)
- PVC is active but the endpoints cannot communicate

Use traps and NavisCore (PVC status, PVC statistics, logical port status, logical port statistics, etc.) to determine the appropriate category. For example, if the Show All PVCs dialog box (see Figure 14-1 on page 14-2) indicates that the operational status (Oper Status) of the PVC is *Inactive*, then you know that the problem is in the inactive category.

After you place the problem into one of these categories, you can take certain steps to correct the problem. Regardless of the problem category, the first thing you should do is to access the Show All PVCs dialog box (see Figure 14-1 on page 14-2).

The following flowcharts provide generic guidelines for troubleshooting problems in each category.

Figure 14-8.   Troubleshooting an Inactive PVC

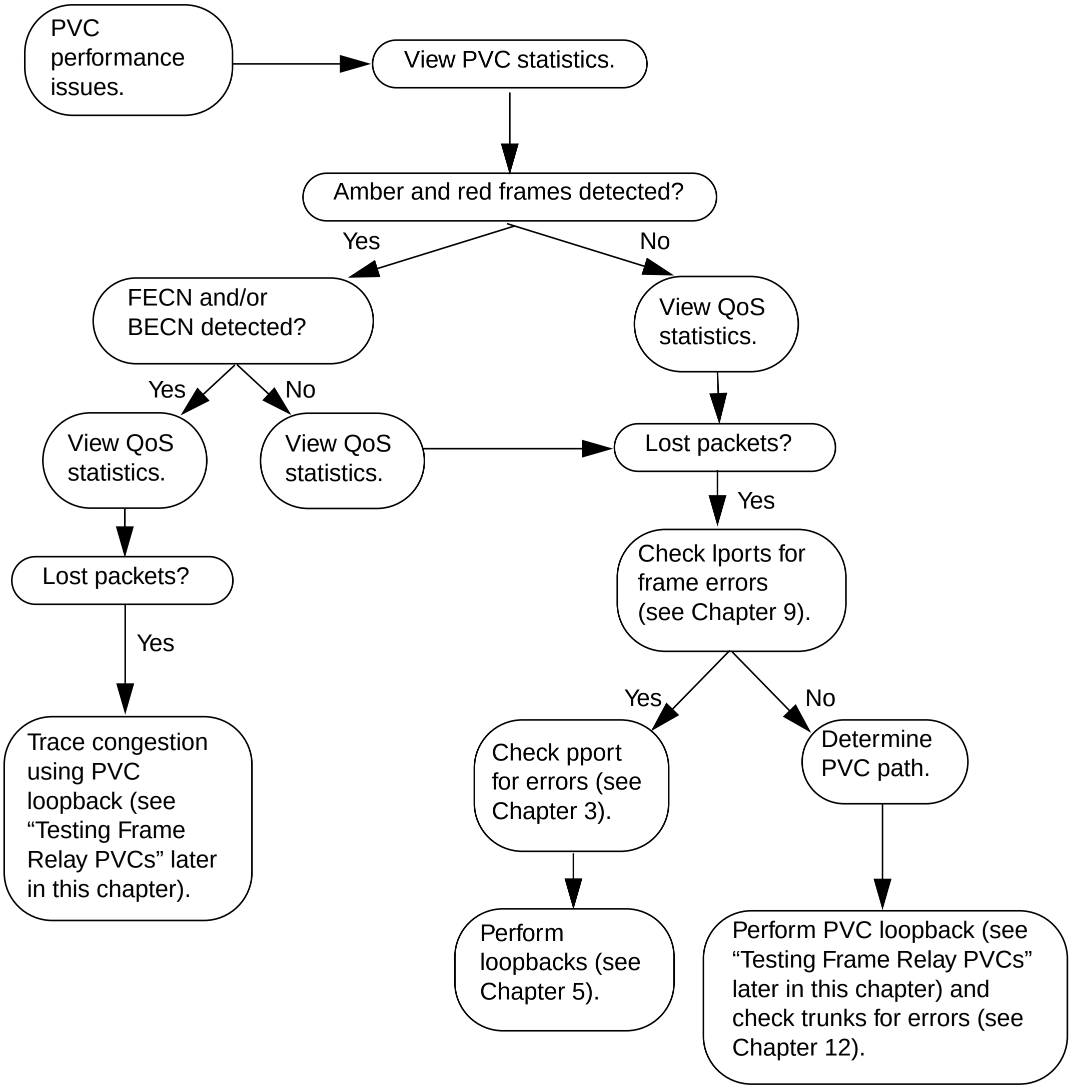


Figure 14-9. Troubleshooting an Active PVC With Performance Issues

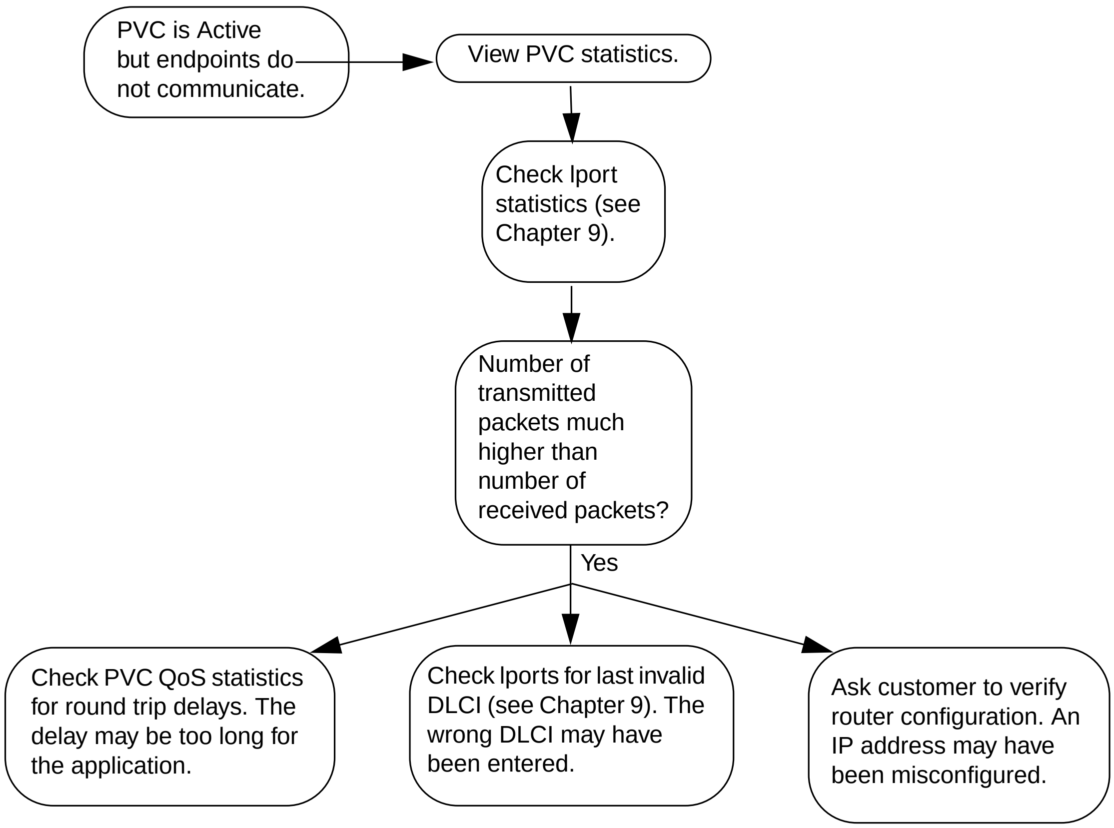


Figure 14-10. Troubleshooting an Active PVC With No Communication Between Endpoints

Viewing Frame Relay SVCs

This section describes how to view Frame Relay SVCs in an Ascend network. You can check the status of Frame Relay SVC parameters and view statistics on circuit activity. For more information, see the *NavisCore Frame Relay Configuration Guide*.

Viewing All Node Prefixes

Node prefixes apply to all ports on the switch and are used for routing aggregation. To view all node prefix formats on a switch:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Node Prefixes. The Show All Node Prefixes dialog box appears (see Figure 14-11).

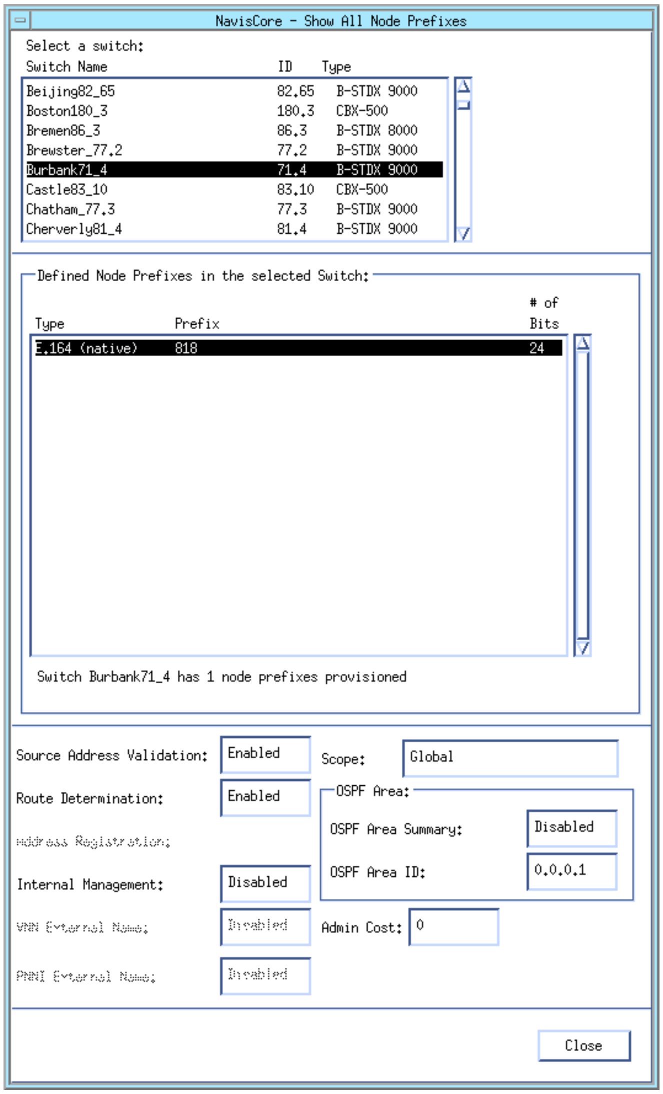


Figure 14-11. Show All Node Prefixes Dialog Box

2. Select the switch whose node prefixes you want to view. The dialog box displays the defined node prefixes for the switch.
3. When you finish viewing the information, choose Close to return to the network map.

Table 14-11 describes the Show All Node Prefixes fields.

Table 14-11. Show All Node Prefixes Fields (Frame Relay SVCs)

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch ID number.
Type	The switch type (e.g., B-STDX 9000).
Defined Node Prefixes	
Type	One of the following address formats: *E.164 (Native)* – Standard 1-15 digit ISDN number, which includes telephone numbers. *X.121* – A 1-14 digit number commonly used in X.25 networks.
Prefix	The configured node prefix.
# of Bits	The number of address bits that are checked during call screening and call routing.
Source Address Validation	One of the following: *Enabled* – The prefix is used to validate the calling party address against the node prefix associated with the UNI logical port that receives the call setup message. *Disabled* – The prefix is not used to validate calling party addresses.
Route Determination	One of the following: *Enabled* – OSPF uses this node prefix for routing aggregation. *Disabled* – OSPF does not use this node prefix for routing aggregation determination.
Internal Management	One of the following: *Enabled* – The node prefix of the switch is to be used as the management base address (that is, as an addressable entity). The internal management base address identifies this node as an endpoint for internal SVC signaling. *Disabled* – The node prefix of the switch is not to be used as the management base address.

Table 14-11. Show All Node Prefixes Fields (Frame Relay SVCs) (Continued)

Field	Displays...
Scope	The organizational scope of the node prefix. The organizational scope determines how far up the routing hierarchy an address can be advertised. Possible values: Global, InterRegional, Regional, IntraCommunity, CommunityMinusOne, OrganizationPlusOne, IntraSite, SiteMinusOne, LocalNetworkPlusTwo, LocalNetworkPlusOne, LocalNetwork.
OSPF Area Summary	One of the following: *Enabled* – The OSPF Area Summary attribute for this node prefix is enabled, allowing this node to be an area border router. If you enable this setting, you must configure an OSPF area ID. *Disabled* – The OSPF Area Summary attribute for this node prefix is disabled.
OSPF Area ID	The ID of the OSPF area. You must configure an OSPF area ID if you enable the OSPF Area Summary setting.
Admin Cost	The administrative cost associated with the node prefix. When an SVC is created, if more than one node in the network is found with the same node prefix, the call is routed to the node with the lowest administrative cost.

Viewing All Port Prefixes

SVC port prefixes define how calls are routed to a logical port. To view all port prefixes defined for a selected logical port:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port Prefixes. The Show All Port Prefixes dialog box appears (see Figure 14-12).

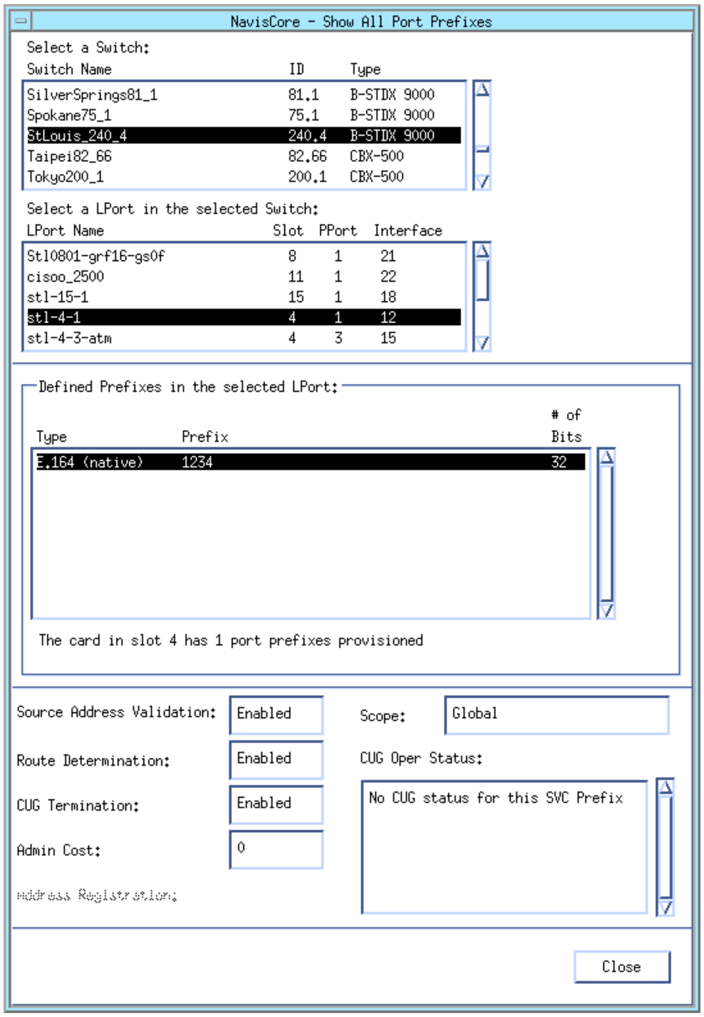


Figure 14-12. Show All Port Prefixes Dialog Box

2. Select a switch.
3. Select a logical port. The dialog box displays the defined prefixes for the logical port, as well as the admin cost and local and remote gateway addresses for the logical port.
4. When you finish viewing the information, choose Close to return to the map.

Table 14-12 describes the Show All Port Prefix fields.

Table 14-12. Show All Port Prefix Fields (Frame Relay SVCs)

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch ID number.
Type	The switch type (e.g., CBX 500).
Logical Port Information	
LPort Name	The name of the logical port associated with the port prefix.
Slot	The slot number of the logical port's I/O module.
PPort	The number of the physical port to which the logical port is mapped.
Interface	The logical port's internal interface number.
Defined Port Prefixes	
Type	The configured SVC address format. See Table 14-11 on page 14-31 for a description of address formats.
Prefix	The configured port prefix.
# of Bits	The number of address bits that are checked during call screening and call routing.
Source Address Validation	One of the following: *Enabled* – The port prefix is used to validate the calling party address against the port prefix associated with the UNI port which received the call setup message. *Disabled* – The port prefix is not used to validate calling party addresses.
Route Determination	One of the following: *Enabled* – OSPF uses the port prefix for route determination. *Disabled* – OSPF does not use the port prefix for route determination.
CUG Termination	One of the following: *Enabled* – The prefix is used as part of a closed user group (CUG). Incoming and outgoing calls, with a calling or called party address that matches this prefix, are subject to CUG security checks. For more information about CUGs, see the *NavisCore Frame Relay Configuration Guide*. *Disabled* – The prefix is not used as part of a CUG.

Table 14-12. Show All Port Prefix Fields (Frame Relay SVCs) (Continued)

Field	Displays...
Admin Cost	The administrative cost associated with the port prefix. When an SVC is being created, if more than one port in the network is found with the same port prefix, the call is routed to the port with the lowest administrative cost.
Scope	The organizational scope of the port prefix. The organizational scope determines how far up the routing hierarchy an address can be advertised. Possible values: Global, InterRegional, Regional, IntraCommunity, CommunityMinusOne, OrganizationPlusOne, IntraSite, SiteMinusOne, LocalNetworkPlusTwo, LocalNetworkPlusOne, LocalNetwork.
CUG Oper Status	The current CUG status. Possible address and prefix status messages include: • A CUG configuration error has occurred at this SVC address (or prefix). • An ambiguous condition exists at this SVC address (or prefix). Decisions will be made at call time. • This SVC address (or prefix) has: Outgoing access, Incoming access. • This SVC does not belong to any CUGs. • This SVC Address belongs to CUGs: [*CUG name and ID*].

Viewing All Port Addresses

If the device attached to a given physical port does not support address registration, you can define SVC addresses for all logical ports on that physical port. To view all SVC port addresses:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port Addresses. The Show All Port Addresses dialog box appears (see Figure 14-13).

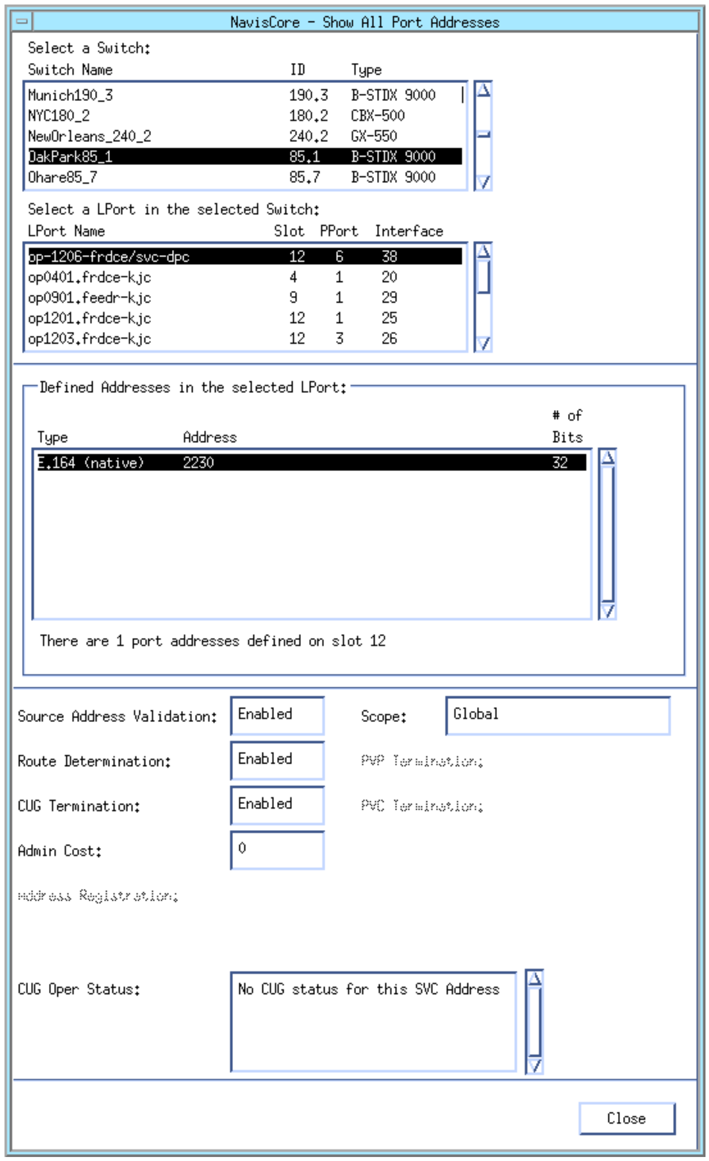


Figure 14-13. Show All Port Addresses Dialog Box

2. Select a switch.
3. Select a logical port. The dialog box displays the defined addresses for the logical port.
4. When you finish viewing information, choose Close to return to the map.

Table 14-13 describes the Show All Port Addresses fields.

Table 14-13. Show All Port Addresses Fields (Frame Relay SVCs)

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch ID number.
Type	The switch type (e.g., CBX 500).
Logical Port Information	
LPort Name	The name of the logical port associated with the addresses.
Slot	The slot number of the logical port's I/O module.
PPort	The number of the physical port to which the logical port is mapped.
Interface	The logical port's internal interface number.
Defined Addresses for the Selected Logical Port	
Type	The configured SVC address format. See Table 14-11 on page 14-31 for a description of address formats.
Address	The configured address.
# of Bits	The number of address bits that are checked during call screening and call routing.
Source Address Validation	One of the following: *Enabled* – The address is used to validate the calling party address against the address associated with the UNI port that received the call setup message. *Disabled* – The address is not used to validate calling party addresses.
Route Determination	One of the following: *Enabled* – OSPF uses the address for route determination. *Disabled* – OSPF does not use the address for route determination.

Table 14-13. Show All Port Addresses Fields (Frame Relay SVCs) (Continued)

Field	Displays...
CUG Termination	One of the following: *Enabled* – The address is used as part of a closed user group (CUG). Incoming and outgoing calls, with a calling or called party address that matches this address, are subject to CUG security checks. For more information about CUGs, see the *NavisCore Frame Relay Configuration Guide*. *Disabled* – The address is not used as part of a CUG.
Admin Cost	The administrative cost associated with the address. When an SVC is being created, if more than one port in the network is found with the same port prefix, the call is routed to the port with the lowest administrative cost.
Scope	The organizational scope of the address. The organizational scope determines how far up the routing hierarchy an address can be advertised. Possible values: Global, InterRegional, Regional, IntraCommunity, CommunityMinusOne, OrganizationPlusOne, IntraSite, SiteMinusOne, LocalNetworkPlusTwo, LocalNetworkPlusOne, LocalNetwork.
CUG Oper Status	The current CUG status. Possible address and prefix status messages include: • A CUG configuration error has occurred at this SVC address (or prefix). • An ambiguous condition exists at this SVC address (or prefix). Decisions will be made at call time. • This SVC address (or prefix) has: Outgoing access, Incoming access. • This SVC does not belong to any CUGs. • This SVC Address belongs to CUGs: [*CUG name and ID*].

Viewing All Port Network IDs

You can define network IDs for logical ports. To view all port network IDs defined for a selected logical port:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port Network IDs. The Show All Port Network IDs dialog box appears (see Figure 14-14).

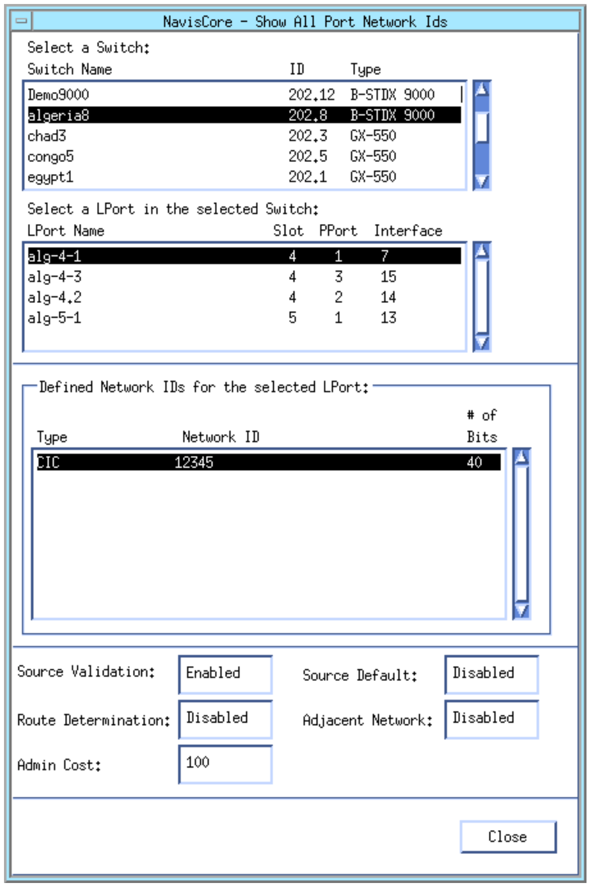


Figure 14-14. Show All Port Network IDs Dialog Box

2. Select a switch.
3. Select a logical port. The dialog box displays the defined network IDs and related information for the logical port.
4. When you finish viewing information, choose Close to return to the map.

Table 14-14 describes the Show All Port Network IDs fields.

Table 14-14. Show All Port Network IDs Fields (Frame Relay SVCs)

Field	Displays...
Switch Information	
Switch Name	The name of the switch.
ID	The switch ID number.
Type	The switch type (e.g., CBX 500).
Logical Port Information	
LPort Name	The logical port associated with the network ID.
Slot	The slot number of the logical port's I/O module.
PPort	The number of the physical port to which the logical port is mapped.
Interface	The logical port's internal interface number.
Defined Network IDs	
Type	One of the following address formats: *CIC* – A 3-digit, 4-digit, or 8-digit Carrier Identification Code (CIC) *DNIC* – A 4-digit Data Network Identification Code (DNIC, X.121)
Network ID	The configured network ID, which is used to uniquely identify an Inter-Exchange Carrier (IXC). Depending on the addressing authority, the network ID can be in either in CIC format or DNIC format.
# of Bits	The number of address bits that are checked during call routing.
Source Validation	One of the following: *Enabled* – The network ID is used for source validation. The switch can use the network ID to screen a signaled transit network selection (TNS), which is a value supplied by the calling party during call setup. The switch matches the TNS against all pre-subscribed source validation network IDs on this interface. If a match occurs, the call is progressed. Otherwise, the call is rejected. *Disabled* – The network ID is not used for source validation.
Route Determination	One of the following: *Enabled* – The network ID is used for route determination. For route determination, the network ID allows an Inter-Exchange Carrier (IXC) to be reached. When a calling party signals for the network ID during call setup, the switch routes the call to the IXC via the logical port associated with the network ID. *Disabled* – The network ID is not used for route determination.

Table 14-14. Show All Port Network IDs Fields (Frame Relay SVCs) (Continued)

Field	Displays...
Admin Cost	The administrative cost associated with the network ID. When an SVC is being created, if more than one port in the network is found with the same network ID, the call is routed to the port with the lowest administrative cost.
Source Default	One of the following: *Enabled* – The network ID is the default (i.e., subscription) network ID for the logical port. The source default network ID is provisioned as a substitute when a signaled TNS is not provided during the call setup process. That is, if no TNS is signaled, and the network does not know the called party number, the network uses the default network ID when it attempts to route the call. Only one source validation network ID may be designated as the source default. *Disabled* – The network ID is not the default network ID for the logical port.
Adjacent Network	One of the following: *Enabled* – The network ID is the route determination network ID that the switch uses as the default for billing purposes (for PVCs and SVCs). This network ID identifies a directly connected (or adjacent) network. A TNS matching this network ID will not be signaled on egress. Only one route determination network ID may be designated as the adjacent network ID. *Disabled* – The network ID is not the route determination network ID that the switch uses as the default for billing purposes. For example, this field displays *Disabled* if the network identified by the network ID is not reached directly, but is instead reached by way of a directly connected network.

Viewing All Active Frame Relay SVCs

The Show All Active SVCs function enables you to:

- Upload SVC information for a selected logical port
- View a hop-by-hop trace of all active SVCs that traverse the network
- Select and view a list of SVC records and attributes

Attributes vary, depending on the type of service (ATM or Frame Relay) the selected SVC supports. For information on viewing active ATM SVCs, see "Viewing All Active ATM SVCs" on page 13-70.

To view a list of Frame Relay SVC records:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Active SVCs. The Show All Active SVCs dialog box appears (see Figure 14-15).

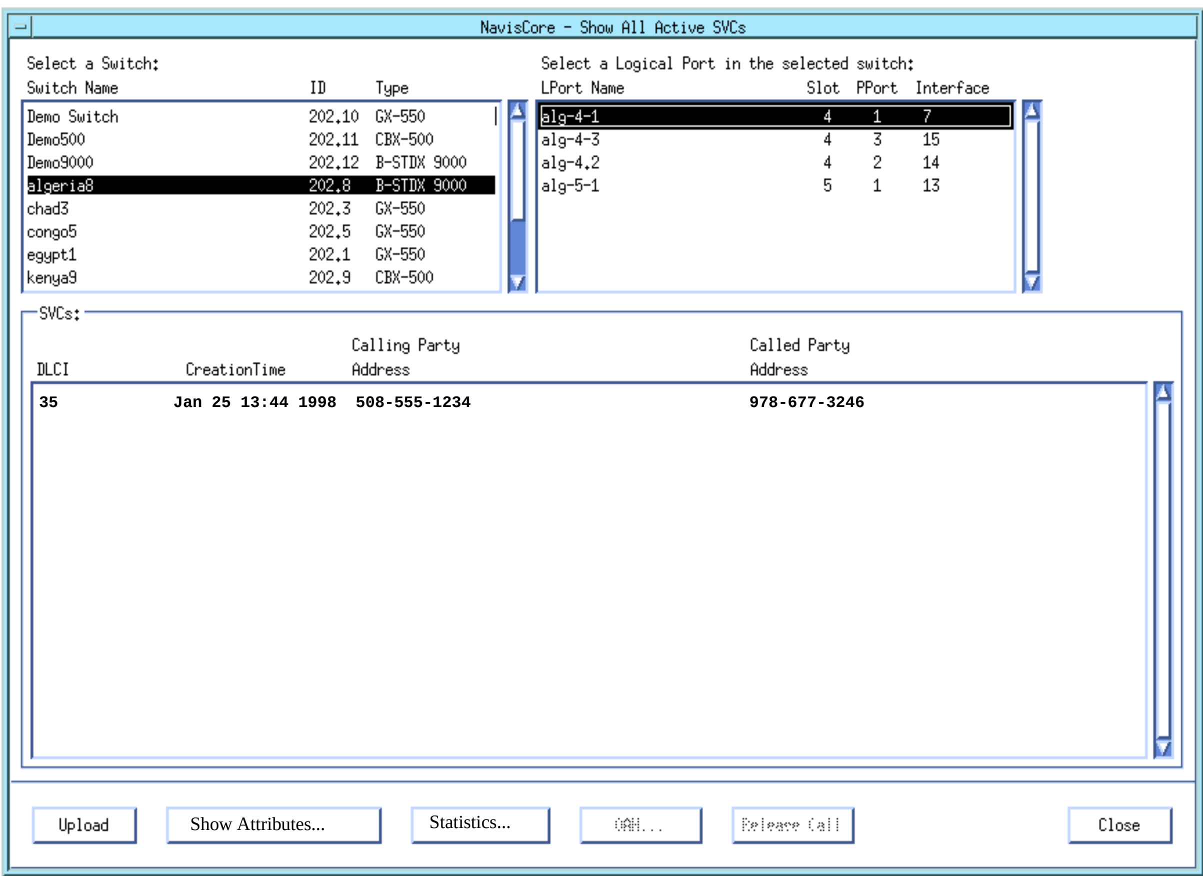


Figure 14-15. Show All Active SVCs Dialog Box (Frame Relay)

2. Select a switch.
3. Select a logical port.
4. Choose Upload to upload all SVC records for the selected logical port. The records appear when the upload is completed.

Table 14-15 describes the Show All Active SVCs dialog box buttons. Table 14-16 describes the Show All Active SVCs fields.

Table 14-15. Show All Active SVCs Buttons (Frame Relay)

Button	Function
Upload	Uploads a list of active SVCs for the logical port you select.
Show Attributes	Displays call details for the SVC you select.
Statistics	Displays SVC statistics.
Release Call	Enables you to release individual SVCs on a UNI port without affecting other SVCs on the same port.

Table 14-16. Show All Active SVCs Fields (Frame Relay)

Field	Displays...
DLCI	The unique Data Link Connection Identifier (DLCI) that the selected logical port uses to identify the SVC. Each end point uses a DLCI to recognize the SVC. Typically, the DLCI has local significance only. For example, one end of the SVC may use a DLCI of 120 to recognize the SVC, while the other end of the SVC may use DLCI 40 to recognize the SVC. See the *NavisCore Frame Relay Configuration Guide* for more information.
Creation Time	The time at which the connection was established.
Calling Party Address	The address of the party that initiated the call. This field is optional and may be blank.
Called Party Address	The address of the party that accepted the call.

Viewing Frame Relay SVC Attributes

The Show Attributes button on the Show All Active SVCs dialog box enables you to view information about a specific SVC. Information depends on the type of service (ATM or Frame Relay) the SVC supports. This section describes Frame Relay SVC attributes. See "Viewing ATM SVC Attributes" on page 13-72 for information about ATM SVC attributes.

To view Frame Relay SVC attributes:

1. From the Show All Active SVCs dialog box (Figure 14-15 on page 14-42), select an SVC record.
2. Choose Show Attributes. The Show Active SVC Attributes dialog box appears.

> SVCs are dynamic and can be set up and taken down by the CPE. A SVC may be released by the CPE between the time you choose Upload and Show Attributes. In this instance, you will not be able to access the SVC's attributes.

3. When you finish viewing attributes, choose Close to return to the Show All Active SVCs dialog box.

Table 14-17 describes the Show Active SVC Attributes fields.

Table 14-17. Show Active SVCs Attributes Fields (Frame Relay)

Field	Displays...
Calling Party Address	The entire SVC calling party address and the address type. See Table 14-12 on page 14-34 for more information on address formats.
Called Party Address	The entire SVC called party address and the address type. See Table 14-12 on page 14-34 for more information on address formats.
SVC Location	Information that identifies the local SVC location, including switch, logical port, and physical port IDs.
SVC Destination	Information that identifies the remote SVC location, including switch, logical port, and physical port IDs, and DLCI address. This section also displays a "Path to Destination" listing, which provides the hop count and trunk name if the call was routed over OSPF trunks.
Call Details	The local DLCI address and call creation time.

Viewing Frame Relay SVC Failed Calls

You can view failed-call information for failed Frame Relay SVCs, which helps you determine why an SVC call failed.

Before you can view SVC failed calls, you must upload SVC call-failure information. To upload and view SVC failed-call information:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Failed SVCs. The Show All Failed SVCs dialog box appears (see Figure 14-16).

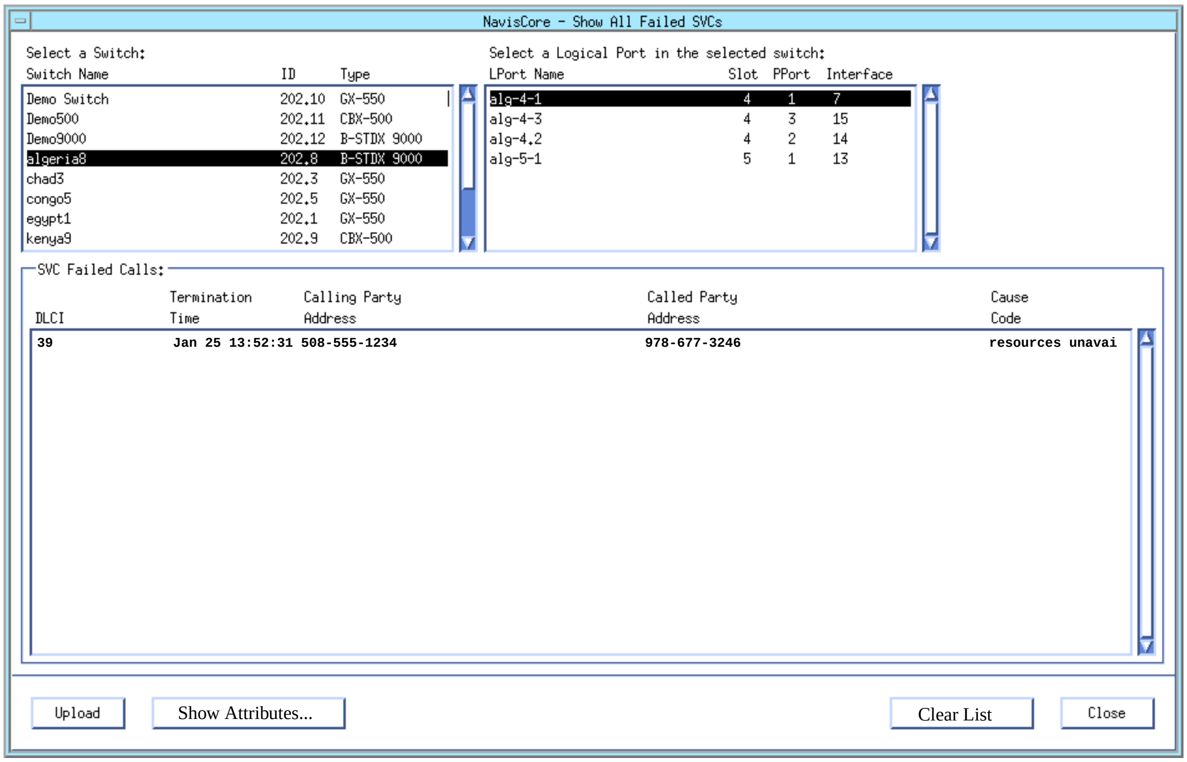


Figure 14-16. Show All Failed SVCs Dialog Box (Frame Relay)

2. Select a switch.

3. Select a logical port.

4. Choose Upload to view the failed SVC calls for the logical port. The records appear when the upload is completed.

5. Choose Close to return to the map.

Table 14-18 describes the Show All Failed SVCs dialog box buttons. Table 14-19 describes the fields on the Show All Failed SVCs dialog box.

Table 14-18. Show All Failed SVCs Buttons (Frame Relay)

Button	Function
Upload	Uploads a list of active SVCs for the logical port you select.
Show Attributes	Displays information about the failed SVC call you select. See page 14-47 for information.
Clear List	Deletes the list of failed calls for this logical port from the switch. ***Note***: *This action permanently deletes the current list from the switch. New failures, however, will continue to be logged.*
Close	Exits the dialog box.

Table 14-19. Show All Failed SVCs Fields (Frame Relay)

Field	Displays...
DLCI	The unique Data Link Connection Identifier (DLCI) that the selected logical port uses to identify the SVC. Each endpoint uses a DLCI to recognize the SVC. Typically, the DLCI has local significance only. For example, one end of the SVC may use a DLCI of 120 to recognize the SVC, while the other end of the SVC may use DLCI 40 to recognize the SVC. See the *NavisCore Frame Relay Configuration Guide* for more information.
Termination Time	The time at which the connection terminated.
Calling Party Address	The address of the party that initiated the call. This field is optional and may be blank.
Called Party Address	The address of the party that accepted the call.
Cause Code	A message describing this failure. The failure cause text is based on the standard Frame Relay Forum UNI signalling cause codes. See Appendix E, "Using SVC Failure Information" for more information.

Viewing Frame Relay SVC Failed-Call Attributes

You can view information, such as calling party address, failure time, and terminating PDU, for a failed SVC call.

To view failed-call information:

1. From the Show All Failed SVCs dialog box (Figure 14-16 on page 14-45), select an SVC failed-call record.
2. Choose Show Attributes. The Show Failed SVC Attributes dialog box appears.
3. When you finish viewing attributes, choose Close to return to the Show All Failed SVCs dialog box.

Table 14-20 describes the Show Failed SVC Attributes fields.

Table 14-20. Show Failed SVC Attributes Fields (Frame Relay)

Field	Displays...
Calling Party Address	The entire SVC calling party address and the address type. See Table 14-12 on page 14-34 for more information on address formats.
Called Party Address	The entire SVC called party address and the address type. See Table 14-12 on page 14-34 for more information on address formats.
SVC Location	Information that identifies the local SVC location, including switch, logical port, and physical port IDs.
Repeat Info	The dates and times of the failure first and most recent occurrence. This field displays the number of times this identical failure has consecutively occurred on this port.
Terminating PDU	The type of signalling PDU used to terminate the call and indicates whether it was sent from or received by the logical port.
Failure Cause	A message describing this failure. The failure cause text is based on the standard ATM and Frame Relay Forum UNI signalling cause codes.
Diagnostic Info	The HEX and ASCII values from the release message diagnostic field. This information may assist in troubleshooting certain types of SVC failures.
SVC Failure Location	A message describing the location of this failure, as well as the switch name, logical port ID and physical port ID information. The failure may be located locally (the location as identified by the SVC Location field) or remotely.
Call Details	The VPI/VCI and endpoint reference for ATM SVCs or the DLCI for Frame Relay SVCs. This field also displays the call creation and termination times.

Viewing Closed User Groups and Members

A closed user group (CUG) is a set of users (or members) who share specific calling privileges in networks that use SVCs to communicate. Members of one CUG may have calling privileges that members of another CUG may not have. CUGs provide a level of security, allowing only authorized nodes to call each other.

Closed user group standards are defined in *ITU-T Draft Recommendation Q.2955.1* and apply to both ATM SVCs and Frame Relay SVCs.

You cannot view CUGs through the Monitor menus. You must configure and monitor closed user groups through the Administer menus. You must also log on to access CUG information.

To access and monitor CUG or CUG member information:

- Select Ascend Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUGs

  or

- Select Ascend Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUG Members

See the *NavisCore ATM Configuration Guide* for more information on CUGs for ATM SVCs. See the *NavisCore Frame Relay Configuration Guide* for more information on CUGs for Frame Relay SVCs.

Viewing Port Security Screens

The Port Security Screening feature enables you to protect your network from unauthorized calls. You do this by creating screens that allow/disallow incoming and outgoing calls. You can apply the screens to any Frame Relay UNI logical port in your network. You can use a maximum of 16 different screens per port. Using these screens, the port checks every call it receives for matching criteria. If the call meets the criteria specified in at least one of these screens, the port either passes or blocks that call accordingly. See the *NavisCore Frame Relay Configuration Guide* for information on configuring port security screening.

To view port security screens:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Port Security Screens. The Configuration of Port Security Screens dialog box appears (see Figure 14-17).

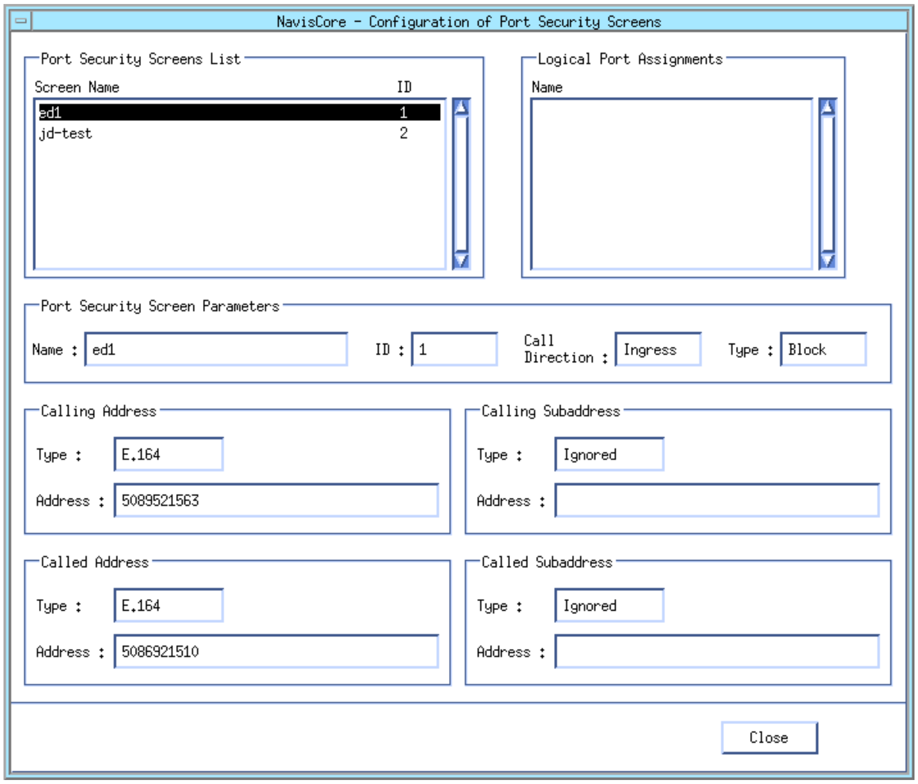


Figure 14-17. Configuration of Port Security Screens Dialog Box

2. When you finish viewing security information, choose Close to return to the map.

Table 14-21 describes the dialog box fields.

Table 14-21. Configuration of Port Security Screens Fields

Field	Displays...
Name	A name (up to 32 characters) for this security screen.
Call Direction	The configured call direction screen: *Ingress* (default) – Screens incoming calls. *Egress* – Screens outgoing calls.
Type	The configured screen type which determines the action this screen performs: *Block* (default) – Blocks all calls that match the criteria. *Pass* – Passes all calls that match the criteria.
Calling Address	The calling address for incoming calls.
Calling Subaddress	The calling subaddress for incoming calls. This parameter provides an optional level of screening.
Called Address	The called address if this screen is for outgoing calls.
Called Subaddress	The called subaddress for outgoing calls. This parameter provides an optional level of screening.

Viewing Frame Relay SVC Summary Statistics

To view Frame Relay SVC summary statistics:

1. From the Monitor menu, select Ascend Objects ⇒ Show All SVC Parameters ⇒ Show All Active SVCs. The Show All Active SVCs dialog box appears (Figure 14-15 on page 14-42).
2. Select a switch from the list box on the left.
3. Select a corresponding logical port from the list box on the right.
4. Choose Upload to upload all SVC records from the selected logical port. A list of SVC records appear.
5. Select an SVC record.
6. Choose Statistics to view SVC summary statistics. The SVC Summary Statistics dialog box displays data in separate columns to reflect the transmission and receipt of data on each side of the circuit. The dialog box displays the following types of statistics:

   Cumulative Statistics — The number of each type of frame (passed, dropped, or tagged) and whether those cells/frames are being transmitted or dropped due to conditions in the network.

Throughput Statistics — The frames per second and bits per second for each side of the circuit.

Utilization Statistics — The amount of traffic queued for transmission on a circuit measured as a percentage of link speed.

Table 14-22 lists and describes the Frame Relay SVC summary statistics fields.

Table 14-22. Frame Relay SVC Summary Statistics

Statistic	Description
Calling Party Address	The entire SVC calling party address and lists the address type. See Table 14-12 on page 14-34 for more information on address formats.
Called Party Address	The entire SVC called party address and lists the address type. See Table 14-12 on page 14-34 for more information on address formats.
Local Logical Port (A)	The logical port at one end of the circuit.
Remote Logical Port (B)	The logical port at the other end of the circuit.
Reset Time	The time of the last statistics reset (i.e., the last time you clicked the Reset button).
Current Time	The current system time.
Poll Interval (sec)	The time interval for the collection of statistical data.
SVC Oper Status	The operating status of the SVC (Up or Down).
Cumulative Statistics	
Total Frames	The total number of frames received and transmitted over the specified logical ports since the last reset.
Green Frames	The total number of green frames received and transmitted over the specified logical ports since the last reset. Green frames are never discarded by the network, except under extreme circumstances (such as node or link failure). Green frames identify packets where the number of bits received during the current time interval, including the current frame, is less than the committed burst size.
Amber Frames	The total number of amber frames received and transmitted over the specified logical ports since the last reset. Amber frames are forwarded with the DE bit set and are eligible for discard if they pass through a congested node. Amber frames identify packets where the number of bits received during the current time interval, including the current frame, is greater than the committed burst size, but less than the excess burst size.

Table 14-22. Frame Relay SVC Summary Statistics (Continued)

Statistic	Description
Red Frames	The total number of red frames received and transmitted over the specified logical ports since the last reset. Red packets are forwarded with the DE bit set when the Graceful Discard feature is set to On. When the Graceful Discard feature is set to Off, red packets are discarded. Red packets are designated as those bits received during the current time interval that exceed the committed burst size and excess burst size thresholds, including the current frame.
Total Octets	The total number of octets (bytes) received and transmitted over the specified logical ports since the last reset.
Green Octets	The total number of green octets (bytes) received and transmitted over the specified logical ports since the last reset. Green octets are never discarded by the network, except under extreme circumstances (such as node or link failure).
Amber Octets	The total number of amber octets (bytes) received and transmitted over the specified logical ports since the last reset. Amber octets are eligible for discard if they pass through a congested node.
Red Octets	The total number of red octets (bytes) received and transmitted over the specified logical ports since the last reset. Red octets are forwarded with the DE bit set when the Graceful Discard feature is set to On. When the Graceful Discard feature is set to Off, red octets are discarded.
Frames Discarded	The number of frames discarded. Congested nodes within the network that must discard packets use the color designations to determine which frames to discard. Red frames are discarded first, followed by amber and green.
Throughput Statistics	
Bits per Second	The number of bits transmitted and/or received each second.
Packets per second	The number of packet frames transmitted and/or received each second.
Congestion Statistics	
FECN Frames	The number of frames that were received or transmitted with the Forward Explicit Congestion Notification (FECN) bit set to one. The network sets a FECN bit to one if the network is encountering congestion. FECN frames indicate that there may not be sufficient network resources to continue handling the submitted traffic at the current rate. See the *Networking Services Technology Overview* for more information.

Table 14-22. Frame Relay SVC Summary Statistics (Continued)

Statistic	Description
BECN Frames	The number of frames that were received or transmitted with the Backward Explicit Congestion Notification (BECN) bit set to one. The network sets a BECN bit to one if the network is encountering congestion. BECN frames indicate that there may not be sufficient network resources to continue handling the submitted traffic at the current rate. See the *Networking Services Technology Overview* for more information.
Utilization Statistics	
Circuit Utilization A	The amount of traffic queued for transmission on a circuit as a percentage of the CIR. For this reason, the value displayed in circuit utilization A can exceed 100%.
Circuit Utilization B	The amount of traffic queued for transmission on a circuit as a percentage of the CIR. For this reason, the value displayed in circuit utilization B can exceed 100%.

Testing Frame Relay PVCs

The PVC Loopback option is a diagnostic tool for testing the transmission of data across a Frame Relay PVC at the UNI/NNI. The PVC loopback test loops back all data frames at the configured endpoint. You can set either endpoint of a PVC as a loopback endpoint. This means that all data sent to the PVC can be routed along the entire customer transmission path and be received on either the local or remote PVC endpoint.

> PVC loopback can be used on an ATM PVC if one end of the PVC resides on a B-STDX switch. PVC loopback is not available for ATM PVCs when both endpoints reside on either CBX 500 switches or GX 550 switches. In this case, use the OAM Loopback test instead. See "Testing ATM Circuits" on page 13-90 for more information.

PVC Loopback Settings

You can configure each PVC endpoint with one of the following loopback settings:

None — No loopback is in effect.

Local — Traffic arriving on the logical port from a CPE should be looped back to that CPE on the same logical port. See Figure 14-18 and Figure 14-20 for two examples of local PVC loopbacks. Figure 14-19 and Figure 14-21 illustrate the corresponding circuit summary statistics that result from a local setting on either Endpoint A or Endpoint B.

Remote — Traffic arriving from a far-end logical port/CPE should be looped back to that logical port/CPE. See Figure 14-22 and Figure 14-24 for two examples of remote PVC loopbacks. Figure 14-23 and Figure 14-25 illustrate the corresponding circuit summary statistics that result from a remote setting on either Endpoint A or Endpoint B.

Both — Both remote and local traffic should loop back.

Figure 14-18 through Figure 14-25 illustrate the direction of the different PVC loopback settings and the circuit summary statistics for each setting.

> In all of the figures that illustrate the PVC loopback settings, Router 1 and Router 2 transmit data over the PVC.
>
> Graceful Discard must be set to On for the PVC loopback function to operate correctly.

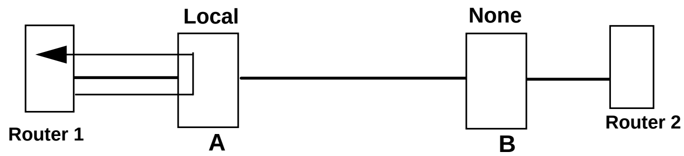
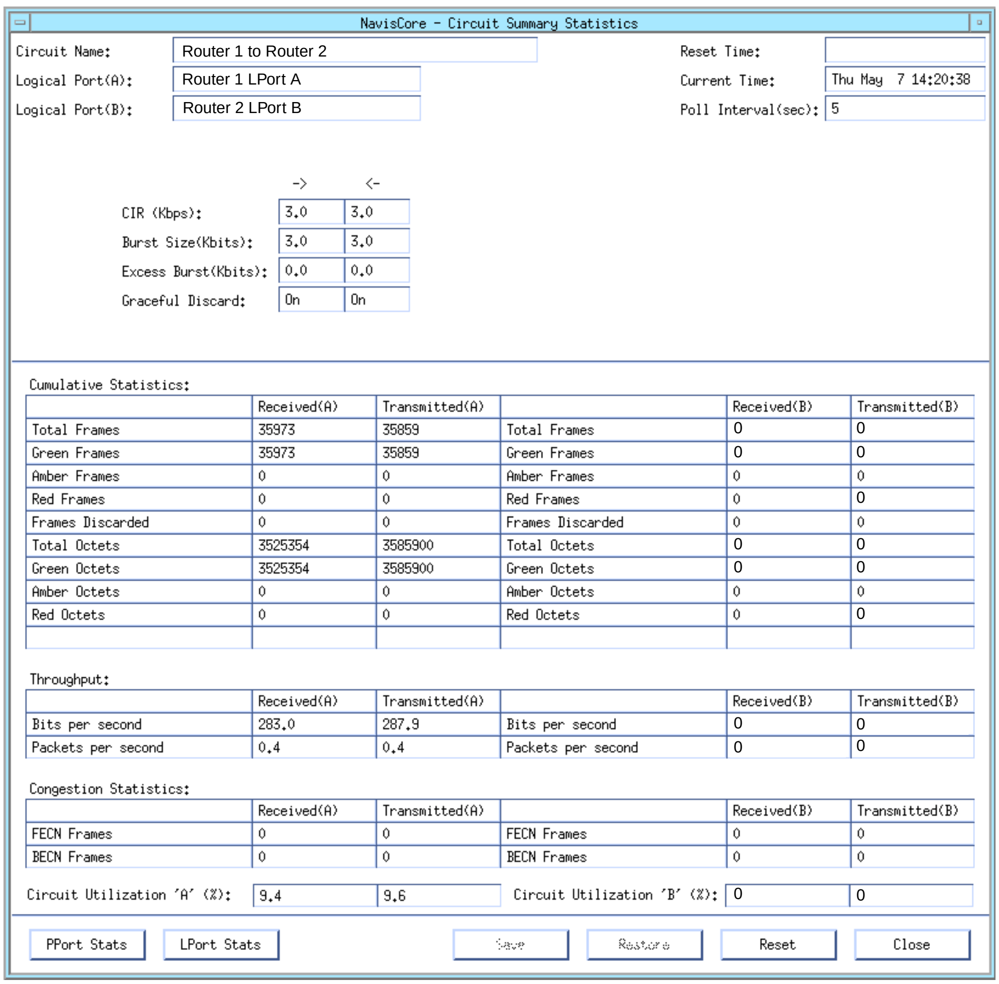


Figure 14-18. PVC Endpoint A Set to Local, Endpoint B Set to None

Figure 14-18 illustrates a PVC loopback that has Endpoint A set to Local and Endpoint B set to None.

Figure 14-19 illustrates the circuit summary statistics generated for a local PVC loopback at Endpoint A. The circuit summary statistics window would show packets received and sent on the same logical port (Endpoint A). No frames are forwarded to Endpoint B of the PVC.



	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Total Frames	35973	35859	Total Frames	0	0
Green Frames	35973	35859	Green Frames	0	0
Amber Frames	0	0	Amber Frames	0	0
Red Frames	0	0	Red Frames	0	0
Frames Discarded	0	0	Frames Discarded	0	0
Total Octets	3525354	3585900	Total Octets	0	0
Green Octets	3525354	3585900	Green Octets	0	0
Amber Octets	0	0	Amber Octets	0	0
Red Octets	0	0	Red Octets	0	0

Throughput:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Bits per second	283.0	287.9	Bits per second	0	0
Packets per second	0.4	0.4	Packets per second	0	0

Congestion Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
FECN Frames	0	0	FECN Frames	0	0
BECN Frames	0	0	BECN Frames	0	0

Figure 14-19. Statistics for A Set to Local and B Set to None

Figure 14-20 illustrates a PVC loopback that has Endpoint A set to None and Endpoint B set to Local.

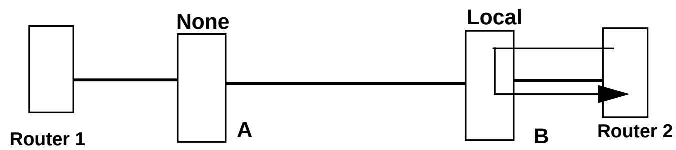


Figure 14-20. PVC Endpoint A Set to None, Endpoint B Set to Local

Figure 14-21 illustrates the circuit summary statistics generated for a local PVC loopback at Endpoint B.

Figure 14-21. Statistics for A Set to None and B Set to Local

Figure 14-22 illustrates a PVC loopback that has Endpoint A set to Remote and Endpoint B set to None.

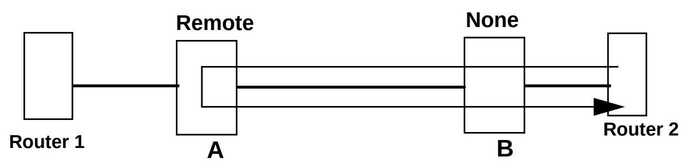


Figure 14-22. PVC Endpoint A Set to Remote, Endpoint B Set to None

Figure 14-23 illustrates the circuit summary statistics generated for a remote PVC loopback at Endpoint A.

NavisCore - Circuit Summary Statistics

Circuit Name:	Router 1 to Router 2	Reset Time:	
Logical Port(A):	Router 1 LPort A	Current Time:	Thu May 7 14:20:38
Logical Port(B):	Router 2 LPort B	Poll Interval(sec):	5

	->	<-
CIR (Kbps):	3.0	3.0
Burst Size(Kbits):	3.0	3.0
Excess Burst(Kbits):	0.0	0.0
Graceful Discard:	On	On

Cumulative Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Total Frames	35973	0	Total Frames	18412	46413
Green Frames	35973	0	Green Frames	18412	35901
Amber Frames	0	0	Amber Frames	0	0
Red Frames	0	0	Red Frames	0	10512
Frames Discarded	0	0	Frames Discarded	0	0
Total Octets	3525354	0	Total Octets	1804376	4620268
Green Octets	3525354	0	Green Octets	1804376	3590092
Amber Octets	0	0	Amber Octets	0	0
Red Octets	0	0	Red Octets	0	1030176

Throughput:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Bits per second	283.0	0	Bits per second	1049.2	2686.5
Packets per second	0.4	0	Packets per second	1.3	3.4

Congestion Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
FECN Frames	0	0	FECN Frames	0	0
BECN Frames	0	0	BECN Frames	0	0

Circuit Utilization 'A' (%):	9.4	0	Circuit Utilization 'B' (%):	35.0	89.6

PPort Stats | LPort Stats | Save | Restore | Reset | Close

Figure 14-23. Statistics for A Set to Remote and B Set to None

Figure 14-24 illustrates a PVC loopback that has Endpoint A set to None and Endpoint B set to Remote.

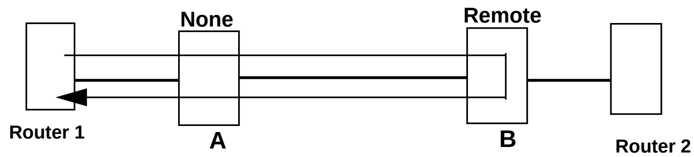


Figure 14-24. PVC Endpoint A Set to None, Endpoint B Set to Remote

Figure 14-25 illustrates the circuit summary statistics generated if Endpoint A is set at None and Endpoint B is set at Remote.

NavisCore - Circuit Summary Statistics

Circuit Name:	Router 1 to Router 2	Reset Time:	
Logical Port(A):	Router 1 LPort A	Current Time:	Thu May 7 14:20:38
Logical Port(B):	Router 2 LPort B	Poll Interval(sec):	5

	->	<-
CIR (Kbps):	3.0	3.0
Burst Size(Kbits):	3.0	3.0
Excess Burst(Kbits):	0.0	0.0
Graceful Discard:	On	On

Cumulative Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Total Frames	35973	35859	Total Frames	18412	0
Green Frames	35973	35859	Green Frames	18412	0
Amber Frames	0	0	Amber Frames	0	0
Red Frames	0	0	Red Frames	0	0
Frames Discarded	0	0	Frames Discarded	0	0
Total Octets	3525354	3585900	Total Octets	1804376	0
Green Octets	3525354	3585900	Green Octets	1804376	0
Amber Octets	0	0	Amber Octets	0	0
Red Octets	0	0	Red Octets	0	0

Throughput:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Bits per second	283.0	287.9	Bits per second	1049.2	0
Packets per second	0.4	0.4	Packets per second	1.3	0

Congestion Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
FECN Frames	0	0	FECN Frames	0	0
BECN Frames	0	0	BECN Frames	0	0

Circuit Utilization 'A' (%):	9.4	9.6	Circuit Utilization 'B' (%):	35.0	0

PPort Stats | LPort Stats | Save | Restore | Reset | Close

Figure 14-25. Statistics for A Set to None and B Set to Remote

When to Use PVC Loopback

The PVC loopback option can be used with active PVCs only. You should use the PVC loopback option if any of the following problems exist:

- Data is not successfully transmitting from one endpoint to the other endpoint of a defined circuit
- There is slow response across a circuit path
- Frames are being lost across a circuit path

Problems PVC Loopback Can Detect

PVC loopback enables you to determine the following circuit problems:

- If the logical level of a circuit path is functioning properly
- Where a fault may exist in the circuit path
- If a congestion problem exists on the circuit path

See the section that follows for information about how to set a PVC loopback. See "Monitoring a PVC Loopback" on page 14-63 for information about how to view PVC loopback status.

Setting a PVC Loopback

When you add a PVC, the system automatically assigns a PVC state of None to each endpoint. Use the following steps to set the state of each endpoint PVC:

> You must be logged on to perform this task.

1. From the Administer menu, select Ascend Parameters ⇒ Set All Circuits ⇒ Point-to-Point. The Set All PVCs On Map dialog box appears (see Figure 14-26).

> If the circuit names do not appear immediately in the Defined Circuit Name list box, insert the cursor in the blank Search by Name field and press Return. This action will display a list of configured circuits.

2. Select the PVC you want to test. Use the Search by Name or Search by Alias fields to enter wild-card characters, as follows:
   - Use an * to match any number of characters
   - Use a ? to match a single character
   - Type ***** to match the * character
   - Type **\?** to match the ? character
   - Type \\ to match the \ character
3. Select Show Frame User Preference Attributes to check the current loopback status of the selected PVC (see Figure 14-26). The current PVC loopback status appears in the bottom half of the dialog box.

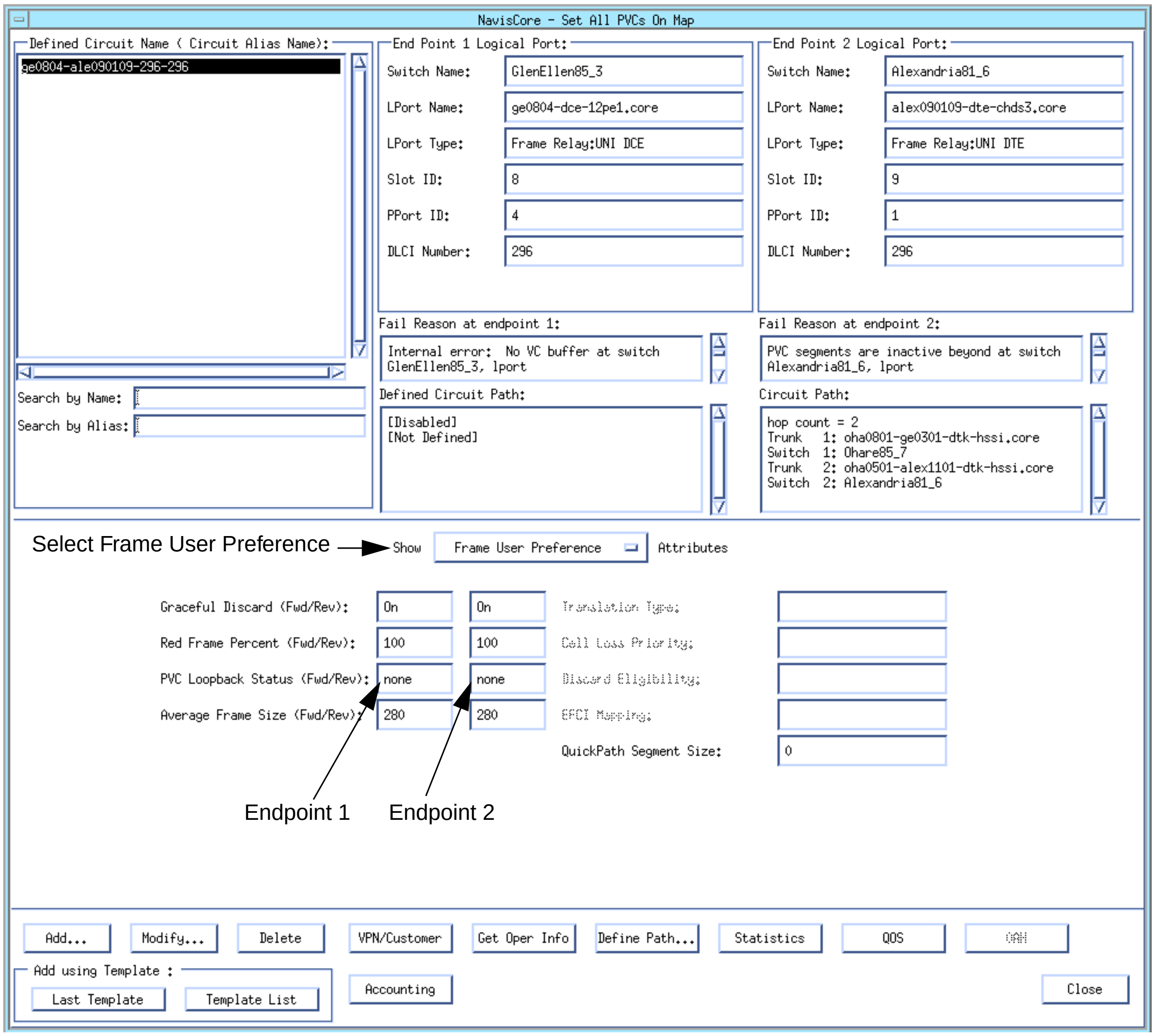


Figure 14-26. Set All PVCs on Map Dialog Box

4. Choose Modify from the Set All PVCs on Map dialog box. The Modify Circuit dialog box appears.
5. Select the Set User Preference Attributes option. The system then displays the user preference attributes at the bottom of the Modify PVC dialog box (see Figure 14-27). In Figure 14-27, the administrator has set one endpoint to None and the other endpoint to Remote.

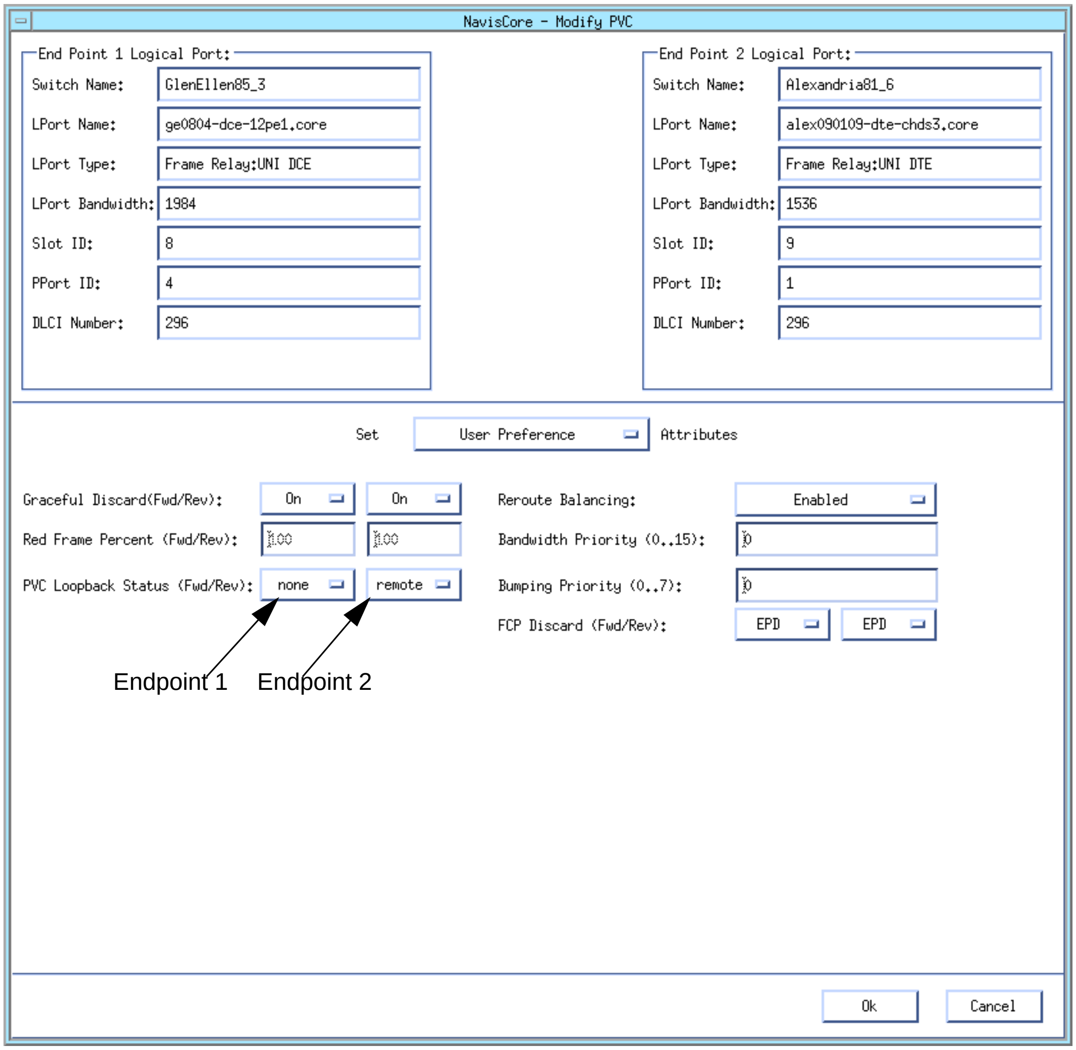


Figure 14-27. Setting a PVC Loopback

6. Set the PVC loopback status for each endpoint and choose OK.

   For each endpoint you can use one of the following PVC loopback state options: *None*, *Local*, *Remote*, *or Both*. See “PVC Loopback Settings” on page 14-54 for a complete description of the PVC loopback settings.

   Use the circuit summary statistics window to monitor a PVC loopback. See “Monitoring a PVC Loopback” on page 14-63 for instructions about accessing this window.

> It is not possible to set the loopback status to Remote at both endpoints of a PVC at the same time. In addition, the Remote loopback setting does not apply to circuits that originate and terminate in the same switch.
>
> If both ends of a PVC terminate to user ports on the same node, use only those combinations marked with an asterisk (*) in Table 14-23.

Table 14-23 lists the valid PVC loopback combinations for the endpoint loopback specifications.

Table 14-23. Valid PVC Loopback Combinations

Loopback Status for Logical Port 1	Loopback Status for Logical Port 2
None	None*
Local	None*
None	Local*
Remote	None
None	Remote
Both	None
None	Both
Local	Local*

Monitoring a PVC Loopback

The Show All PVCs dialog box specifies whether or not a PVC loopback status is in effect. When you view this dialog box, select Show Frame User Preference Attributes to view the PVC loopback status. See "Viewing Frame Relay PVC Status" on page 14-1 for detailed information about accessing the Show All PVCs dialog box.

The sample frame user preference attributes in Figure 14-28 show that a PVC loopback is in effect for the selected circuit. One endpoint has been set to None while the other endpoint has been set to Remote.

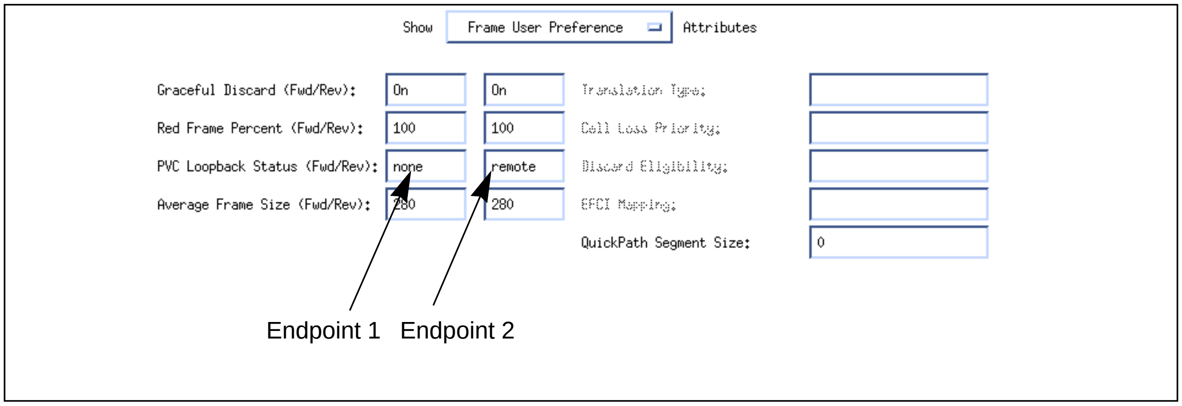


Figure 14-28. Frame User Preference Attributes (with PVC Loopback Set)

To view the statistics for a PVC loopback, choose the Statistics button from the Show All PVCs dialog box. The system then displays the Circuit Summary Statistics dialog box. See "Viewing Frame Relay PVC Summary Statistics" on page 14-20 for more information about viewing circuit summary statistics.

15

Managing Traps

Traps notify the network operator about events that occur on switches configured to report trap information to the NMS. You can view a list of logged traps through the Ascend Events option in the Event Categories window in NavisCore.

This chapter describes how to:

- Manage Ascend events through the Ascend Events Browser dialog box
- Add event categories
- Move events from one category to another
- Filter traps
- Manage the trap configuration for a switch, which includes modifying alarm relay status and trap transmission rate
- Optimize trap processing performance

Appendix A describes the trap messages reported and displayed in the Ascend Events browser.

Using the Ascend Events Browser Dialog Box

Through the Ascend Events browser dialog box, you can view and manage Ascend events. You access the Ascend Events Browser dialog box from the Event Categories window (see Figure 15-1), which appears each time you run NavisCore and notifies you of any significant trap alarm conditions.

Figure 15-1. Event Categories Window

> If the Event Categories window does not appear automatically when you run NavisCore, you can view this window manually by selecting Fault ⇒ Events from the HP OpenView menu bar.

The Event Categories window has a button for each event category, including Ascend Events. To access the Ascend Events Browser dialog box, double-click on Ascend Events from the Event Categories window. The Ascend Events Browser dialog box appears (see Figure 15-2).

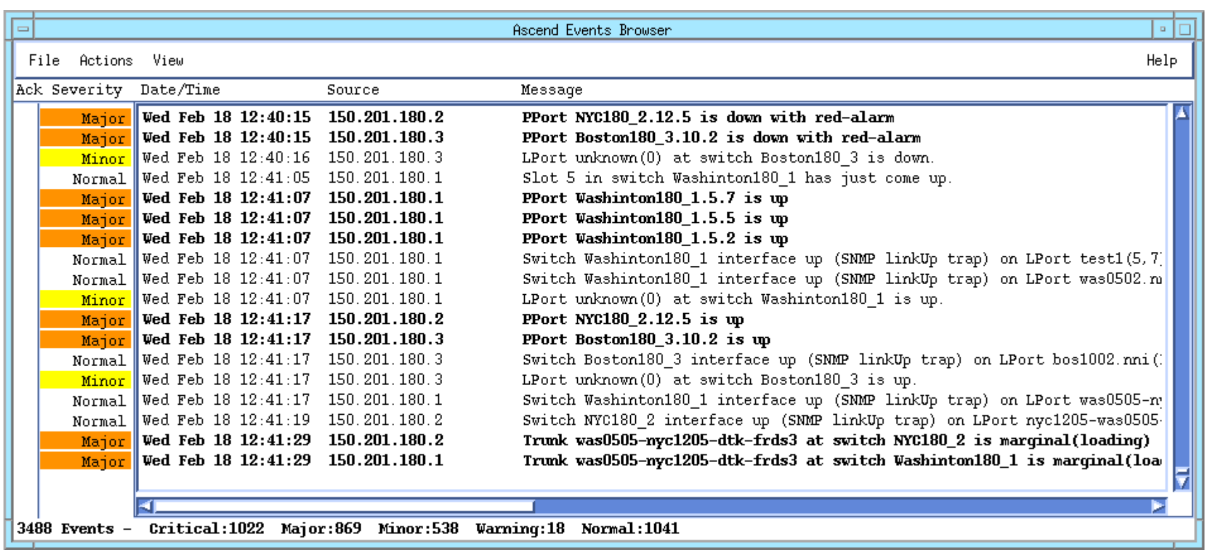


Figure 15-2. Ascend Events Browser Dialog Box

The Ascend Events Browser dialog box lists the following information about each trap alarm:

Severity — Displays the severity level. Possible values include: Critical, Major, Minor, Warning, or Normal.

Date/Time — Displays the date and time the trap alarm occurred.

Source — Displays the name of the system on which the trap alarm occurred.

Message — Displays a message that describes the trap alarm.

See Appendix A, "Trap Alarm Condition Messages" for a list and description of the trap alarm messages reported and displayed in the All Events Browser dialog box.

Viewing a Switch from the Ascend Events Browser

To view the switch that generated an event:

1. Access the Ascend Events Browser dialog box (Figure 15-2 on page 15-2).
2. Select the event from the list.
3. From the Actions menu, select Highlight Source on Map. The network map appears and the switch that generated the event appears highlighted.

For more information about the Events Browser, see the *HP OpenView Network Node Manager User's Guide* or choose Help from HP OpenView.

Acknowledging Events from the Ascend Events Browser

The Ascend Events Browser enables you to acknowledge events. When you acknowledge an event, a check mark appears next to the event. As an additional visual cue, the color of the event becomes faded.

You can acknowledge the following types of events:

- Events you select from the Ascend Events Browser dialog box
- All filtered events
- All events in the Ascend Events category

After you acknowledge events, you can perform additional actions, such as deleting them or moving them to another category.

Acknowledging Selected Events

To acknowledge selected events:

1. Access the Ascend Events Browser dialog box (Figure 15-2 on page 15-2).
2. Select the event(s) from the list.
3. From the Actions menu, select Acknowledge ⇒ Selected Events.

Acknowledging Filtered Events

To acknowledge filtered events:

1. Access the Ascend Events Browser dialog box (Figure 15-2 on page 15-2).
2. From the Actions menu, select Acknowledge ⇒ Filtered Events.

Acknowledging All Events

To acknowledge all events in the Ascend category:

1. Access the Ascend Events Browser dialog box (Figure 15-2 on page 15-2).
2. From the Actions menu, select Acknowledge ⇒ All Events in Category.

You follow similar procedures to unacknowledge selected events, filtered events, and all events in the Ascend Events category. Select Unacknowledge from the Action menu instead of Acknowledge.

Deleting Events from the Ascend Events Browser

You can delete the following types of events from the Ascend Events browser:

- Selected events
- Filtered events
- Acknowledged events
- All events in the Ascend Events category

Deleting Selected Events

To delete selected events in the Ascend Events category:

1. Access the Ascend Events Browser dialog box (Figure 15-2 on page 15-2).
2. Select one or more events from the list.
3. From the Action menu, select Delete ⇒ Selected Events.

Deleting Filtered, Acknowledged, and All Events

To delete filtered events, acknowledged events, or all events in the Ascend Events category:

1. Access the Ascend Events Browser dialog box (see Figure 15-2).
2. Select one of the following options from the Actions menu:
   - Select Delete ⇒ Filtered Events
   - Select Delete ⇒ Acknowledged Events
   - Select Delete ⇒ All Events in Category

   Even though you can delete an event(s) from the Event Browser, HP OpenView continues to store the information in the */usr/OV/log/trapd.log* file. Once this log is full, events are moved automatically to the */usr/OV/log/trapd.log.old* files.

Using Additional Ascend Event Browser Management Functions

In addition to the event management functions described in the previous sections, you can perform the following functions from the Actions menu of the Ascend Events Browser dialog box:

Configure Events — Enables you to perform several event configuration tasks, such as customizing events to make them more meaningful or defining the actions HP OpenView should take when the events are received.

Assign Severity — Enables you to assign a severity level to selected events. For example, you can select events that currently have a Normal severity level and assign them a Minor severity level.

Additional Actions — Enables you to configure actions that you can take from the event browser dialog box whenever selected events occur. These actions do not happen automatically — they are actions you can perform manually through the event browser dialog box.

These functions are standard HP OpenView event management functions. See your HP OpenView documentation or online Help for details.

Managing Event Categories

HP OpenView enables you to organize events by “categories.” Some categories are defined for you, such as the Ascend events category. You can also define your own categories and specify which events that go in those categories.

Using the Event Categories Window

In the Event Categories window (Figure 15-1), when a button changes color, an event in that category has occurred on the network. The color of the button indicates the level of severity of the event. Through the Network Node Manager (NNM) internal processes, the event is sent to a predefined category in the Events browser. You can view these events through the All Events browser function or the browser functions for the various categories (such as Ascend Events).

You can customize the Event Categories window by adding categories. For example, you may want to add a category that holds all acknowledged events or one that holds all cancelled events. See “Adding Event Categories” on page 15-6 for instructions about adding event categories.

For more information about operational states and status colors, select Display Legend from the HP OpenView Help menu.

Adding Event Categories

To add one or more categories to the Event Categories window:

1. From the HP OpenView Options menu, select Event Configuration. The Event Configuration dialog box appears (see Figure 15-3).

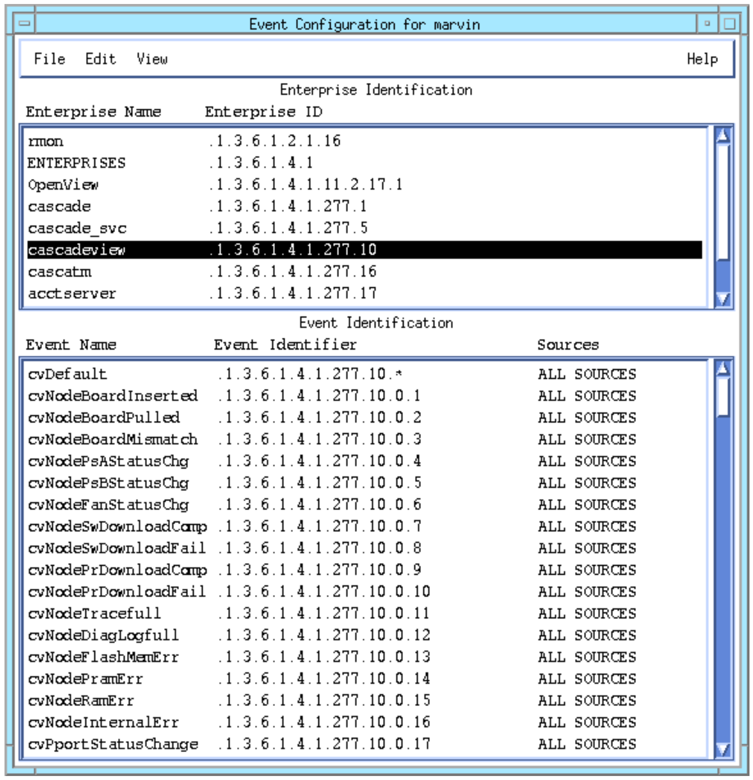


Figure 15-3. Event Configuration Dialog Box

2. Select Edit ⇒ Configure ⇒ Event Categories. The Event Configuration / Event Categories dialog box appears (see Figure 15-4).

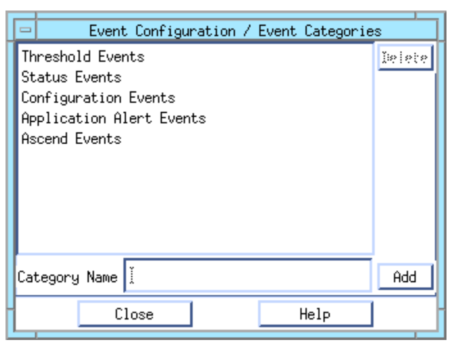


Figure 15-4. Event Configuration / Event Categories Dialog Box

3. Specify the category name and choose Add. The system then adds the new event category to the list.

Moving Events from One Category to Another

To move an event from one category to another:

1. From the Event Categories window (Figure 15-1 on page 15-2), double-click on the button next to the category from which you want to move events. The browser dialog box for that category appears. For example, if you double-click on the Ascend Events category button, the Ascend Events browser dialog box appears (see Figure 15-2).
2. Click on each event you want to move.
3. From the Actions menu, select Assign Category. The Assign Category dialog box appears for the selected category (see Figure 15-5).

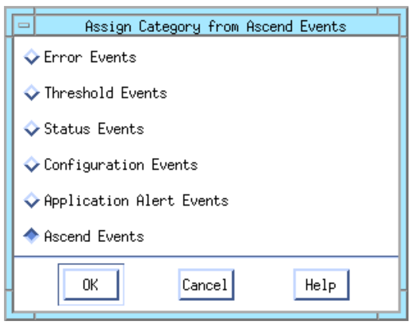


Figure 15-5. Assign Category Dialog Box (Ascend Events)

4. Select the category to which you want to move the selected event(s).
5. Choose OK.

Filtering Traps

The trap filtering feature enables you to filter traps that you do not want the switch to send to the Events browser. The switch forwards *only* unfiltered traps to the NMS. You can filter specific traps or traps based on severity level. For example, if you filter all traps that have a non-alarm severity level, none of these traps will be sent to the Events Browser.

Setting Trap-Filtering Parameters

> You must log on to set trap-filtering parameters.

To filter traps that you do not want the switch to report to the Events browser:

1. From the Administer menu, select Ascend Parameters ⇒ Set All Trap Mask Parameters. The Modify Trap Masks dialog box appears (see Figure 15-6).

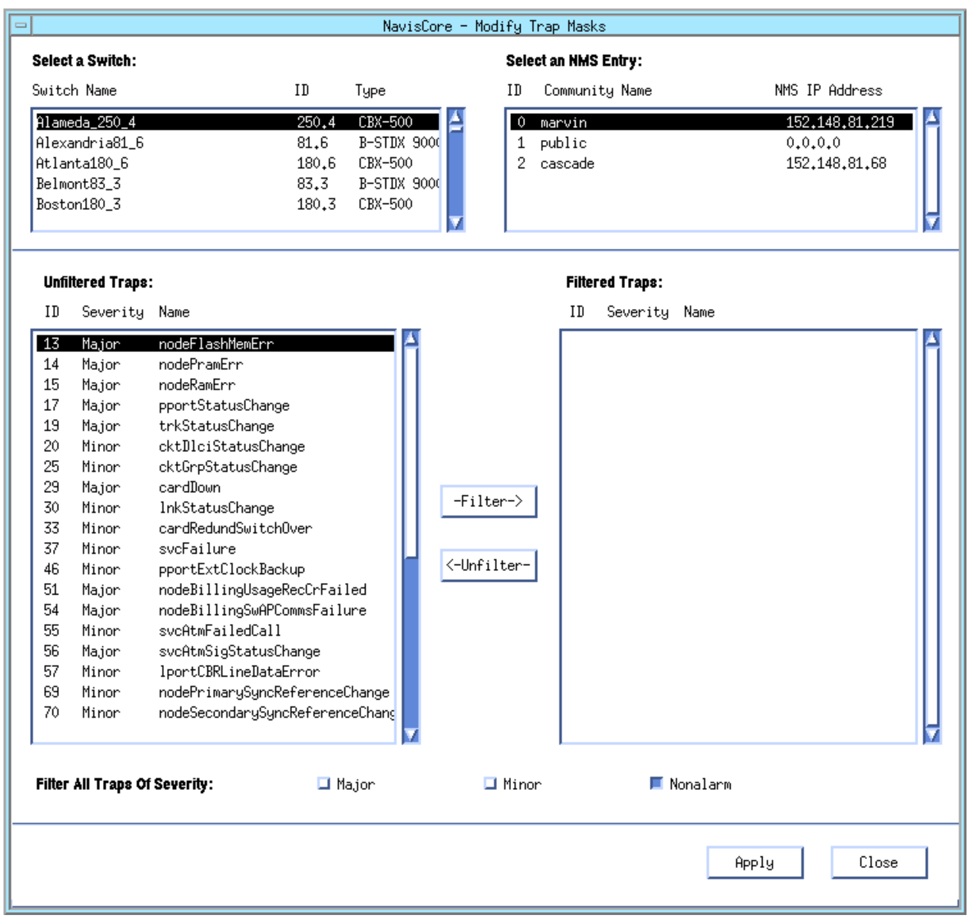


Figure 15-6. Modify Trap Masks Dialog Box

The Modify Trap Masks dialog box displays the switch name, community name, and NMS IP address. Traps are displayed by their corresponding MIB ID.

2. Select the switch from the list box on the left. The corresponding community name and IP address for the selected switch appear in the list box on the right.
3. Select an NMS entry. The default is the community name of your NMS.
4. From the Unfiltered Traps list box on the left, select the trap(s) that you want to filter. You can select multiple traps at the same time. To select non-sequential traps, hold down the control key and select each trap ID.
5. Choose Filter. The system moves the trap(s) to the Filtered Traps list box on the right as shown in Figure 15-7.

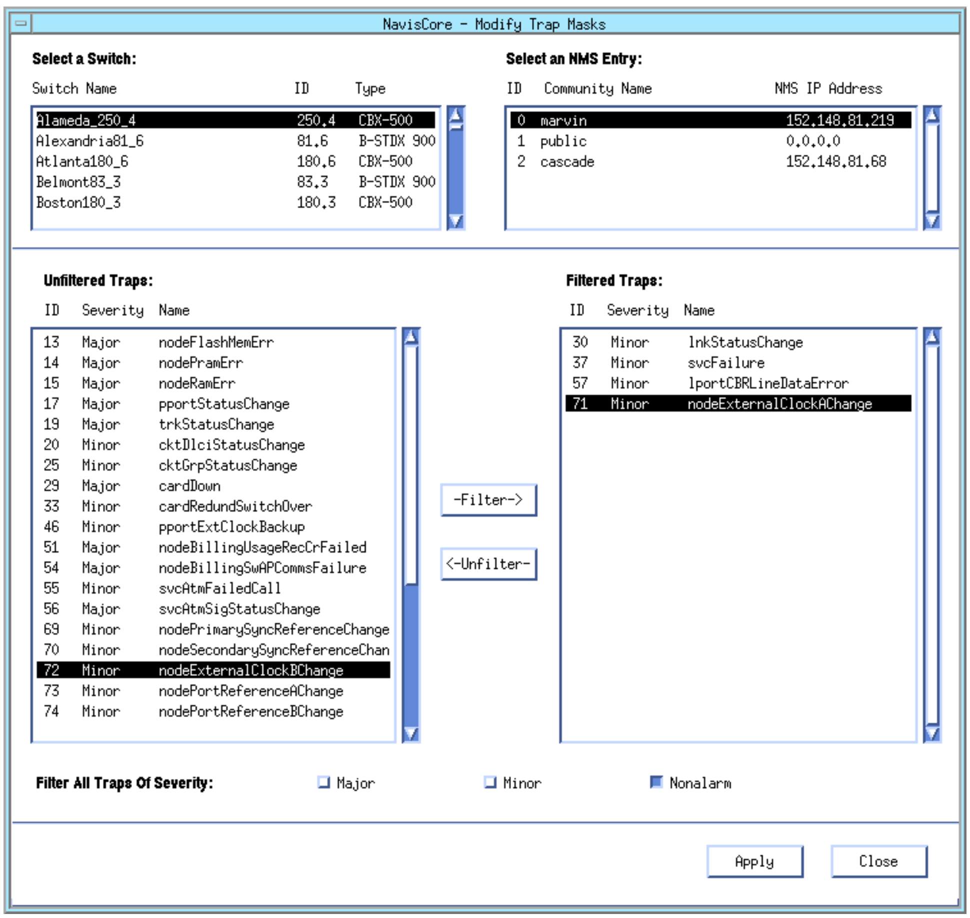


Figure 15-7. Modify Trap Mask Dialog Box (Filtered Traps)

6. (*Optional*) Select a severity level (*major, minor, or non-alarm*) to filter traps based on trap severity.

▶ You cannot filter critical traps. All critical traps are sent to the NMS.

7. Choose Apply to confirm the changes.
8. Choose Close to exit the dialog box and return to the network map.

Removing Trap-Filtering Parameters

> You must log on to remove trap-filtering parameters.

To remove the filtering parameters and add traps to the unfiltered list:

1. From the Administer menu, select Ascend Parameters ⇒ Set All Trap Mask Parameters. The Modify Trap Masks dialog box appears (Figure 15-6 on page 15-9).
2. Select the switch from the list box on the left. The corresponding community name and IP address for the selected switch appear in the list box on the right.
3. Select an NMS entry. The default is the community name of your NMS.

   The filtered traps appear in the Filtered Traps list box on the right (Figure 15-7 on page 15-10).
4. Select the trap(s) from the Filtered list box and choose Unfilter. The system moves the trap(s) to the Unfiltered Traps list box on the left.
5. To remove the filtering parameters on severity traps, deselect major, minor, or non-alarm. This unfilters the *deselected* severity-level traps.
6. Choose Apply to confirm the changes.
7. Choose Close to exit the dialog box and return to the network map.

Managing the Trap Configuration for a Switch

For selected switches in an Ascend network, you can configure alarm relay status and trap transmit rate.

> You must log on to configure alarm relay status and trap transmit rate.

The CBX 500 switch processor adapter (SPA) module and the GX 550 node processor adapter (NPA) module contain an 8-position terminal strip that enables you to connect remote audio and visual alarms. These relay contacts alert you to critical, major, and minor alarm conditions in the switch and power supply. See the *CBX 500 Hardware Installation Guide* and the *GX 550 Hardware Installation Guide* for information on connecting these alarms. If necessary, you can disable the contact alarm relay feature through NavisCore (see "Alarm Relay Status" on page 15-16).

> B-STDX switches do not support the contact alarm relay feature. They support the trap transmit rate feature only.

The trap transmit rate determines the maximum number of traps per second that the switch sends to the NMS. For example, if you enter 5 (default), the switch sends a maximum of five traps to the NMS every second and queues any remaining traps.

To use the alarm relay feature or adjust the trap transmit rate:

1. Select the switch object and from the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears. Figure 15-8 shows a sample Switch Back Panel dialog box for a CBX 500.

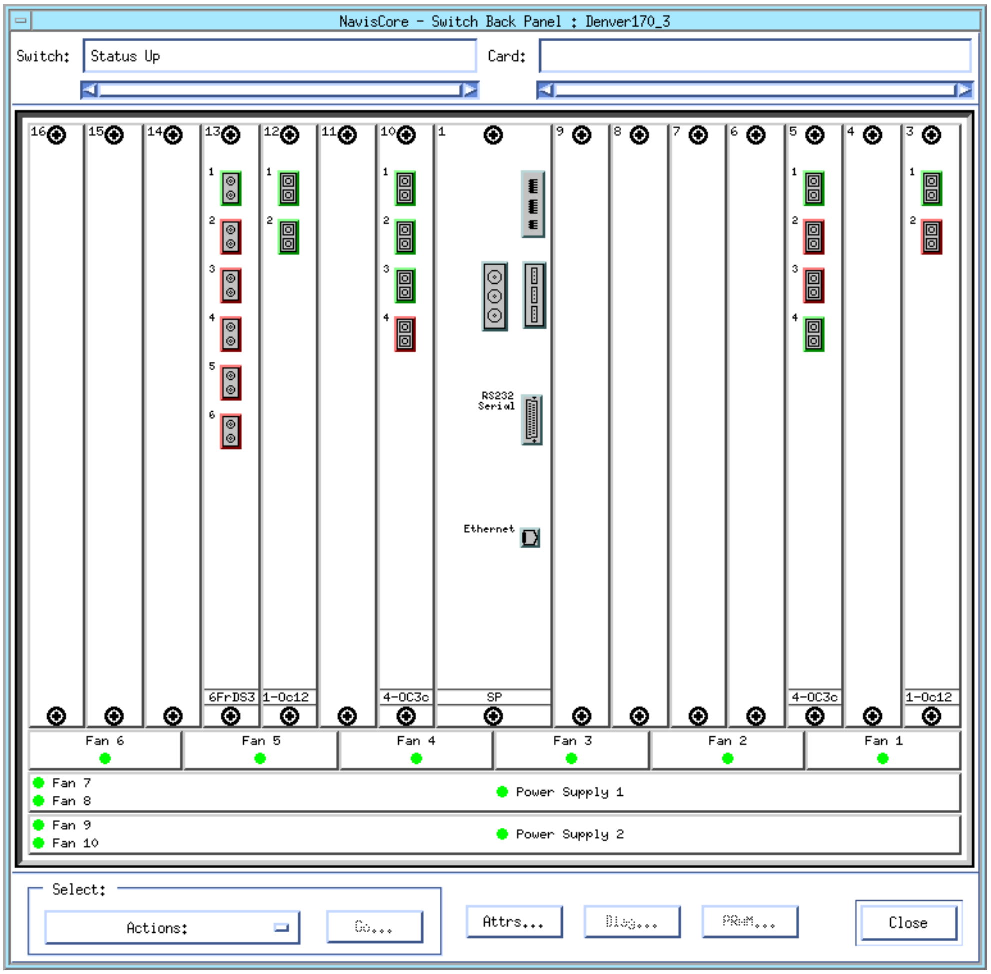


Figure 15-8. Switch Back Panel Dialog Box (CBX 500)

2. Select Actions ⇒ Set Switch Attributes.

3. Choose Go. The Set Switch Attributes dialog box appears (see Figure 15-9).

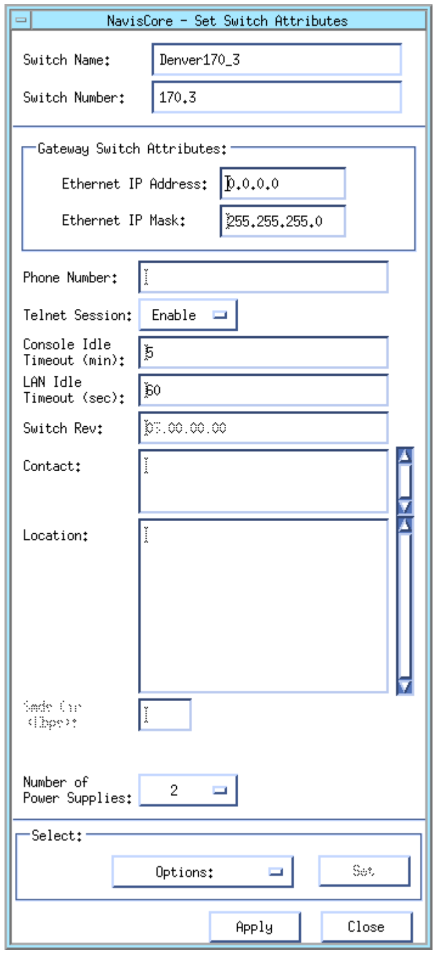


Figure 15-9. Set Switch Attributes Dialog Box

4. Select Options ⇒ Trap Config.

5. Choose Set. The Modify Trap Configuration dialog box appears (see Figure 15-10).

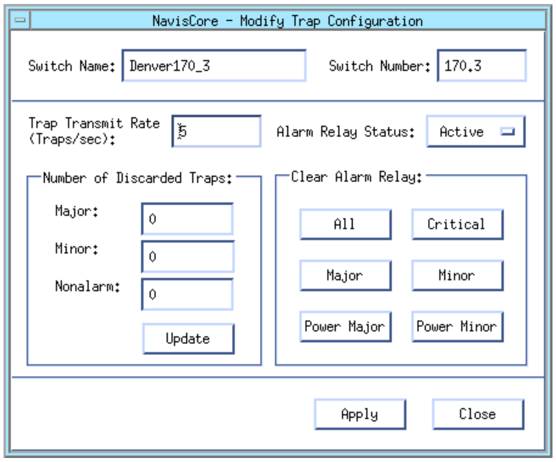


Figure 15-10. Modify Trap Configuration Dialog Box

6. Complete the fields described in Table 15-1.

7. Choose Apply to send the change to the switch.

Table 15-1. Modify Trap Configuration Fields

Field	Action/Description
Trap Transmit Rate (Traps/sec)	Use the Update function to view the number of discarded traps according to their severity (*major, minor, non-alarm*). ***Note:** The switch discards traps under peak problem conditions when the trap transmit queues overflow.* If the switch discards traps, increase the trap transmit rate. Valid values range from 1 to 10.
Clear Alarm Relay	Select one of the following options to clear an alarm relay (that is, turn off an audible/visual contact alarm) immediately: *All* – Clears all alarm relays. ***Note:** This function does not clear the alarm condition, only the audible/visual alarm contact relay.* *Critical* – Clears a Critical alarm relay. These alarms indicate severe, service-affecting conditions that require immediate corrective action, for example, a power supply failure. *Major* – Clears a Major alarm relay. These alarms indicate a hardware or software condition that can cause a serious disruption of service or circuit failure. An example would be an IOM or physical port down. *Minor* – Clears a Minor alarm relay. These alarms indicate non-service-affecting conditions, for example, an exceeded performance monitoring threshold. *Power Major* – Clears a major power alarm relay, for example, the second power supply is out of service. For example, on the CBX 500's N+1 chassis, this alarm is generated if two out of three power supplies fail. *Power Minor* – Clears a minor power alarm relay. With an N+1 chassis, this alarm is generated if one of the three power supplies fails.

Table 15-1. Modify Trap Configuration Fields (Continued)

Field	Action/Description
Alarm Relay Status	Set to *Inactive* to disable the alarm relay function.

Optimizing Trap Processing Performance

The file */opt/cvux/CascadeView/etc/cvtraplogd.cfg* contains five timers that determine how long the name of a network object (switch, trunk, logical port, card, or circuit) is stored in the NMS cache for insertion into trap messages. These names are stored in NMS cache in order to reduce the number of database lookups that the NMS must perform. You can adjust these timers to optimize trap processing performance.

How the NMS Stores Network Object Names in Cache

In order to understand these timers, it is helpful to understand how the NMS stores names of network objects in cache:

1. A trap arrives at the NMS with an ID that describes the switch, trunk, logical port, card, or circuit that is associated with the trap. Keep in mind that a trap may have multiple IDs. For example, a trap may arrive that has two IDs: one that identifies a logical port and one that identifies the switch where the logical port resides.
2. Using the ID(s), the NMS issues a Sybase database query to get the name of the associated switch, trunk, logical port, card, or circuit.
3. To avoid repetitive (and expensive) database lookups, the NMS caches the name that Sybase returns and inserts the name into the trap message that appears in the Ascend Events browser. The name is kept in cache for as long as the appropriate timer specifies. The timers include:

   CV_SWITCH_CACHE_TIME — The amount of time that a switch name is allowed to remain in the cache.

   CV_CARD_CACHE_TIME — The amount of time that a card name is allowed to remain in the cache.

   CV_TRUNK_CACHE_TIME — The amount of time that a trunk name is allowed to remain in the cache.

   CV_LPORT_CACHE_TIME — The amount of time that a logical port name is allowed to remain in the cache.

   CV_CIRCUIT_CACHE_TIME — The amount of time that a circuit name is allowed to remain in the cache.
4. The NMS removes the name from cache when the timer expires. Following expiration, the NMS resets the timer upon arrival of the next trap that contains an ID associated with the same name.

The following example illustrates the use of the timers:

1. A switch issues a trap that contains a logical port ID.
2. The NMS receives the trap and, using the logical port ID, performs a Sybase database lookup to find the name “LPort1.”
3. The NMS caches the “LPort1” name. The NMS does not have to perform another database lookup until the timer expires.
4. The CV_LPORT_CACHE_TIME timer expires, and the NMS removes the name “LPort1” from the cache.
5. The NMS caches the name “LPort1” again the next time the NMS receives a trap with the associated “LPort1” ID.

Guidelines for Setting Name Cache Timers

If you decrease the timers, NMS performance may degrade due to an increase in database lookups.

If you increase the timers, you may improve NMS performance by decreasing the number of database lookups. However, if you increase the timers, you could encounter problems like the one described below:

1. You increase the CV_CIRCUIT_CACHE_TIME timer.
2. You delete a circuit, then add a new circuit using exactly the same attributes that were configured for the deleted circuit except for the circuit name. Thus, the only difference between the old circuit and the new circuit is the circuit name, and the old circuit name remains in the cache due to the increased timer.
3. Traps that describe events on the newly add circuit arrive at the NMS, but the old circuit name continues to appear in these traps.

Setting Name Cache Timers

To set the timers, edit the file */opt/cvux/CascadeView/etc/cvtraplogd.cfg*. The timers (and their default values) appear in the file as follows:

```
CV_SWITCH_CACHE_TIME=36000
CV_CARD_CACHE_TIME=18000
CV_TRUNK_CACHE_TIME=18000
CV_LPORT_CACHE_TIME=18000
CV_CIRCUIT_CACHE_TIME=7200
```

Specify timer values in seconds. Ignore the CVDB_TRACE_FILE_NAME parameter.

After you edit the file, stop and restart the trap log daemon (cvtraplogd) to put the changes into effect:

1. Log on to the NMS workstation as superuser.
2. Stop the cvtraplogd daemon by issuing the following command at the UNIX prompt:

   ```
   /opt/OV/bin/ovstop cvtraplogd
   ```

3. Restart the cvtraplogd daemon by issuing the following command at the UNIX prompt:

   ```
   /opt/OV/bin/ovstart cvtraplod
   ```

16

Monitoring MIB Values

This chapter introduces the Management Information Base (MIB) and describes how to use the HP OpenView MIB browser to navigate through the Ascend MIB. For more information, see the *NavisCore Enterprise MIB Definitions*.

MIB Overview

The MIB is a collection of objects that represent network devices and their internal components. Common MIB objects include:

- Counters of packets sent
- Connections used
- Connections attempted

SNMP Structure of Management Information

The Ascend MIB uses the SNMP Structure of Management Information (SMI) as the set of rules that define the MIB structure. These rules specify the structure of each object in the MIB:

Object Type — Specifies the type of MIB object.

Syntax — Identifies the data type for the object as integer, string, counter, IP address, or pointer.

Access — Specifies the possible access to the object as read-only, read-write, or non-accessible.

Status — Uses one of the following types to specify the currency of the object:

Mandatory – The object is required to configure a switch.

Current – The object is not required for configuration.

Obsolete – The object is no longer part of the MIB.

Description — A text definition that further describes the object.

Index — Lists an index value that provides instructions for identifying object instances. For example, an index value of

```
::={lportEntry 68}
```

indicates the 68th instance of lportEntry.

MIB Information Example

The following example illustrates the MIB object for the source logical address of a circuit:

```
cktSrcLaddr  OBJECT-TYPE
      SYNTAX  INTEGER
      ACCESS  read-write
      STATUS  mandatory
      DESCRIPTION
            “The source logical address of the circuit.”
: : = {  cktEntry 82  }
```

For a list of Ascend MIB definitions, see the *NavisCore Enterprise MIB Definitions.*

MIB Structure

The MIB structure has a tree hierarchy. This hierarchy starts at the root of the tree (which is unnamed) and splits into the following three main branches:

ccitt(0) — Administered by the International Telecommunication Union (formerly known as the International Telegraph and Telephone Consultative Committee).

iso (1) — Administered by the International Organization for Standardization and the International Electrotechnical Committee.

joint-iso-ccitt(2) — Jointly administered by ISO/IEC and ITU.

> Each administrator of a branch is free to assign further subordinate branches (nodes).

Object Identifier

Each branch of the MIB is identified by a short text string (for example iso) and a non-negative integer (for example 1). The integer is used as part of an *object identifier* for each object in the MIB.

The object identifier (OID) provides a way to identify a specific object within a MIB. It contains a sequence of non-negative integers that denote a path from the root of the path to the object. The string of integers is separated by periods.

For example, the following string specifies the path to the Ascend MIB:

```
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1)
.cascade(277)
```

The object identifier for each branch of this path is indicated in parentheses. The following string specifies the object identifier for the path to the Ascend MIB.

```
1.3.6.1.4.1.277
```

See the *NavisCore Enterprise MIB Definitions* for specific information about the OID values for each cascade variable. The OID string for each variable is shown in brackets ({ }) as shown in the following example:

```
: : = {  cktEntry 82  }
```

In this example, the OID string for the circuit is specified in the brackets as 82.

Ascend MIB

The Ascend MIB is identified by the group name *cascade*. Cascade (which has an object ID of 277) has the following groups:

Group	Object ID
cascade_OV_v1traps_	0
cascfr	1
cascsmds	2
namdbinding	3
isdnaddr	4
cascsvc	5
software	6
mpt	7
protconnect	8
provserver	9
cascview	10
casccnm	11
cascdvc	14
cascadepm	15
cascatm	16
acctserver	17
cascsna	18
ipswitch	19
cascfltsrv	20

Figure 16-1 illustrates the SNMP MIB tree hierarchy, which shows the branches through the hierarchy that you use to access the Ascend MIB.

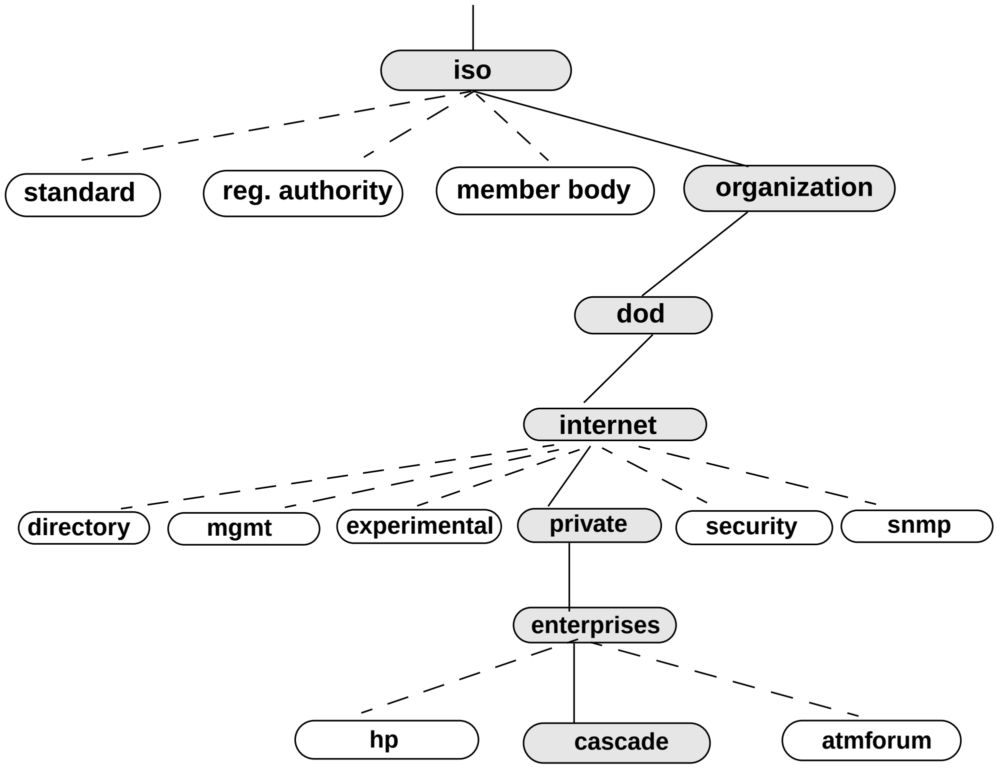


Figure 16-1. SNMP MIB Tree Hierarchy

cascfr Group

The cascfr group contains groups that are common to all protocols (including Frame Relay, SMDS, ATM, and ISDN). The cascfr group contains the following groups:

Group	Description
cascfr_OV_v1traps_	Ascend traps.
net	Variables that are relevant to an Ascend network.
ase	The OSPF Autonomous System External device and host table for NMS paths.
node	Variables that configure a switch.
card	Variables that configure an intelligent card.
pport	Variables that configure a physical port.
lport	Variables that configure a logical port.
ckt	*(Frame Relay only)* Variables that configure permanent virtual circuits (PVCs) on a port.
cascds1	Variables that specify DS1 channel information.
chan	Additional variables that relate to channel information.
fracct	Variables that relate to Frame Relay accounting.

Using the HP OpenView MIB Browser

The Management Information Base (MIB) browser enables you to:

- Navigate through the Ascend MIB and locate a specific object
- Display a description of the selected MIB object
- Retrieve a list of all possible instances of an object
- Run a query for a specified object
- Save data collected through the browser

Accessing Information in the Ascend MIB

The first step in using the MIB is to determine what type of information you need. Then you must identify the group that contains the information.

For example, to use the MIB to check a module's admin status, you would look in the card group. After you determine the group, the next step is to find the variable you need. The MIB browser enables you to navigate through the MIB tree to find the required variable.

Accessing the MIB Browser

To access the MIB browser:

1. From the Misc menu, select SNMP MIB Browser. The system displays the Browse MIB dialog box (see Figure 16-2).

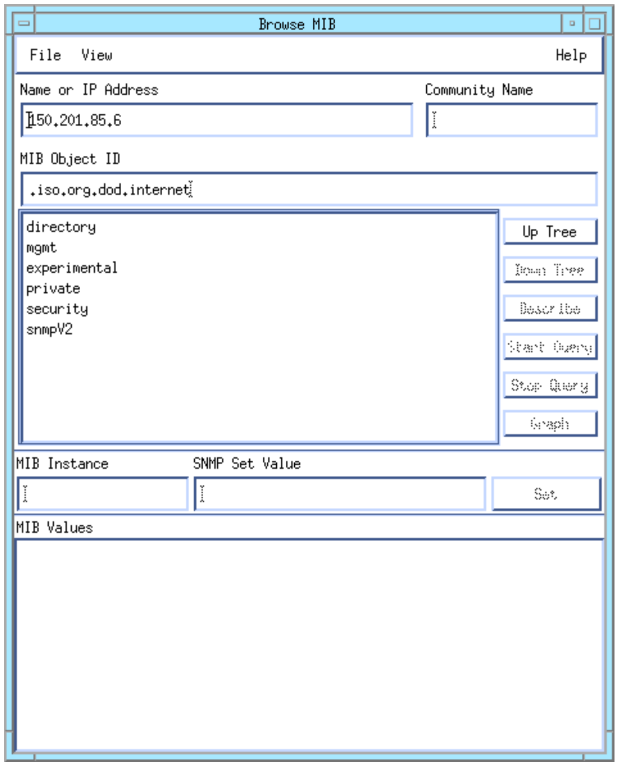


Figure 16-2. Browse MIB Dialog Box

Table 16-1 describes the buttons on the Browse MIB dialog box. Table 16-2 describes the Browse MIB dialog box fields.

Table 16-1. Browse MIB Buttons

Button	Function
Up Tree	Moves up the MIB tree to the previous MIB group.
Down Tree	Moves down the MIB tree to the selected MIB group.
Describe	Displays descriptive information about the selected object.
Start Query	Starts a query on a specified object ID string.
Stop Query	Stops a query on a specified object ID string.
Graph	Not supported.
Set	Sets a writable MIB object to the value in the SNMP Set Value field.

Table 16-2. Browse MIB Fields

Field	Displays...
Name or IP Address	The name or IP address that identifies the switch.
MIB Object ID	An object ID string that identifies the specified MIB object. See the *NavisCore Enterprise MIB Definitions* for more information.
MIB Instance	Specific MIB instance of a selected category.
SNMP Set Value	The current SNMP set value for writable MIB objects. Reset this value by entering a new value in this field and choosing Set. Use the Describe option to verify the numeric SNMP Set values. (You must enter a numeric value; for example, 1 represents Enable, and 2 represents Disable.)
MIB Values	Values that result from a query on an object.
Messages	Any resulting error or informational messages.

2. Select private as the MIB object ID and choose the Down Tree button.
3. Select enterprises as the MIB object ID and choose the Down Tree button.
4. Select cascade as the MIB object ID and choose the Down Tree button. The system displays all of the possible cascade groups in the Browse MIB dialog box (see Figure 16-3).

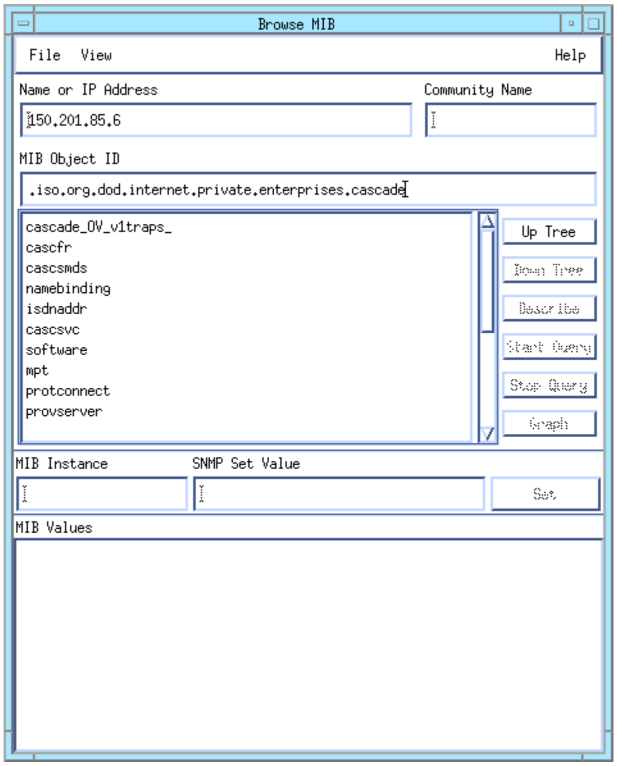


Figure 16-3. Displaying Groups in the Browse MIB Dialog Box

5. Select the group that you want to access and continue to choose Down Tree to access a specific object within a group.

6. Choose Describe at any point in the tree to display a description for a selected MIB variable (see Figure 16-4).

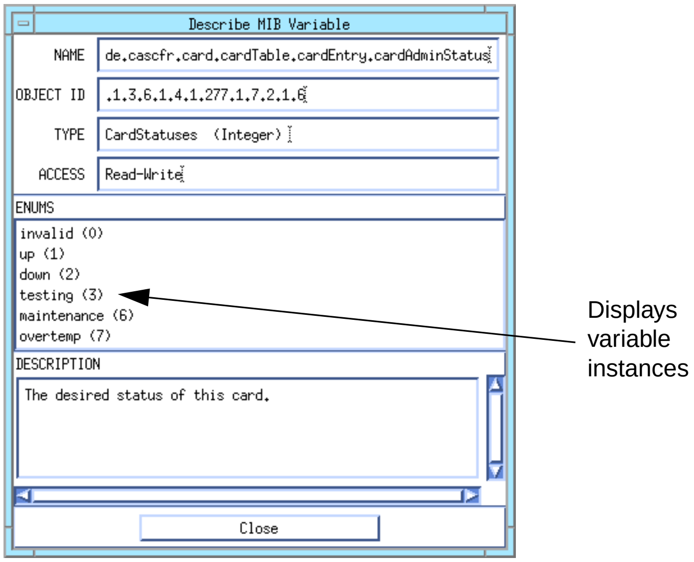


Figure 16-4. Describe MIB Variable Dialog Box

17

Resolving NMS Problems

This chapter provides general troubleshooting solutions for resolving problems with the NMS software applications. Unless otherwise noted, this chapter only addresses NMS software problems and solutions.

Basic Troubleshooting

In diagnosing and troubleshooting software, proceed from simple tasks to complex tasks, following a systematic procedure. As a point of reference, keep in mind the directory structures listed in Table 17-1.

Table 17-1. NMS Directories

Directory Name	Contents
/opt/sybase	Home directory for Sybase.
/opt/sybase/bin	Database binaries.
/opt/sybase/install	Sybase database startup script, startserver, and showserver scripts.
/opt/CascadeView/bin	NavisCore scripts.
/opt/CascadeView/conf	Trap daemon configurations.
/opt/CascadeView/etc	NavisCore configurations.
/opt/CascadeView/sqr	Network report binaries.
/usr/OV/bin	OpenView binaries.
/opt/cde	Common Desktop Environment (CDE) files.
/opt/cv_scripts	Installation scripts.

SPARCstation Problems

If you are having problems with your SPARCstation, complete the following steps to isolate the cause:

1. List the configuration of all hardware and software items currently installed on the SPARCstation. Include all related external devices, software configuration settings, and vendor types.
2. Restart the OV processes using **ovstop** and **ovstart**.

NMS Problems

To isolate the cause of new problems on an NMS:

☑ *Check the hardware.*

- Verify any new hardware installations on the SPARCstation. If you recently added a new device or card to the SPARCstation, it may have conflicts with existing devices for system resources. Verify the SCSI device target addresses are as follows:
  - CD-ROM drive is 6
  - Tape drive is 4
  - First hard disk is 0
  - Second hard disk is 1

☑ *Check the software.*

- If you install or run new software on the SPARCstation, it may have conflicts with existing software for control of peripheral devices or use of memory. Deactivate the new software to verify a potential conflict. If existing applications run without the new software, you must then determine the cause of the conflict and correct the problem.
- If you changed any settings in your configuration files, return the files to their previous configurations.

Common Installation Problems

This section describes some common problems and questions related to new NMS software installations.

I'm having problems seeing my external tape/cdrom drive.

1. Verify that the SCSI target addresses on the back of each device are as follows:

- CD-ROM drive is 6
- Tape drive is 4
- First hard disk is 0
- Second hard disk is 1

> Every device must have a unique SCSI address.

2. The SCSI devices need to be terminated. Install a terminator on the last device on the SCSI chain.

3. Turn on the external SCSI devices, then power up the system. This gives the devices time to boot up and be recognized by the system.

4. While holding down the stop key, type **a** to stop the boot process.

- At the OK prompt, type **probe-scsi**

This searches the system for SCSI devices and lists what is installed and the corresponding SCSI IDs. Make a note of the SCSI addresses for all the devices.

5. Type **boot -r** when the system recognizes the devices.

How much physical memory do I have?

When you first boot up the system, the system tests the memory and displays the amount of memory (MB) available.

1. Log in as the root user and enter the root password.

2. Enter the following command:

```
/usr/bin/dmesg
```

- This command provides system boot-up information and displays the installed physical memory in (MB).
- If the system has been running, the information that you need is not displayed properly. Shut down and restart the system. Repeat Steps 1 and 2 to display the amount of available memory.

I'm having trouble installing Solaris 2.5.

Verify that you have identified your hardware correctly and partitioned your disks properly.

1. To restart the Solaris 2.5 installation, hold down the stop key and type **a** to interrupt the machine.
2. Verify that the Solaris 2.5 installation CD is installed in the CD-ROM drive.
3. Enter **boot cdrom**.
4. See the *Network Management Station Installation Guide* for installation instructions.

How do I copy Ascend switch software from a floppy to my NMS?

1. Insert the floppy into the drive.
2. To initiate the File Manager from the command window, enter:

   ```
   /usr/openwin/bin/filemgr &
   ```

3. From the File menu, select Check for Floppy. A file manager window appears and displays the contents of the floppy. The switch software files are listed in the window.
4. Make sure the system File Manager is set to the following directory:

   ```
   /opt/CascadeView.var/switchSoftware
   ```

5. Select the switch software window. Select a file and drag it to the system file manager window.

   Continue this procedure for each additional file that you want to copy. This process takes a few minutes to complete.

   When the copy is complete, the icon appears.

6. Select the **eject disk** button located in the floppy File Manager box.
7. To download the switch software from the NMS to the switch, see the software release notice that comes with your software release.

How do I start NavisCore?

1. Verify you are logged in as the NMS user by entering the following command:

   ```
   whoami
   ```

2. Verify that you are in the **/opt/nms** directory by entering the following command:

   ```
   pwd
   ```

3. Execute NavisCore by typing:

   ```
   /usr/OV/bin/ovw &
   ```

What is my password?

Ascend does not know your root or nms user password. Ascend does not have default passwords.

How do I shut down the NMS?

You must shut down all processes before you can power off the NMS.

Where do I get an HP OpenView key?

A key is associated with each copy of HP OpenView. The key matches the IP address of the UNIX workstation for which it was purchased. Register the key with Hewlett Packard by sending the completed software certificate included with your HP OpenView package to Hewlett Packard.

I get the error “Cannot connect to database”.

If you receive the error “cannot connect to database” when you try to start NavisCore, do the following:

1. Log in as the root user and enter the appropriate password.

2. To verify that all OV daemons are RUNNING and their behavior is OVs_WELL_BEHAVED, enter the following command:

```
/usr/OV/bin/ovstatus
```

3. If all OV daemons are not running, restart the OV daemons by entering:

```
/usr/OV/bin/ovstart ovwdb
```

4. To start all daemons, enter the following command:

```
/usr/OV/bin/ovstart
```

5. To confirm that all daemons are running, enter:

```
/usr/OV/bin/ovstatus
```

What kind of hardware do I need?

See the *Network Management Station Installation Guide*.

What software versions do I need?

See the *Network Management Station Installation Guide*.

What is a raw partition?

A raw partition is not part of the operating system. It is treated as a separate device and is assigned to one of the three database devices used by Sybase. A file device is part of the UNIX file system and runs on a cooked partition. A file-system partition is a file that grows bigger and bigger, as the database size increases.

I can't start Sybase!

To start Sybase, you must be in the $SYBASE directory and logged in as the sybase user.

1. Enter **cd $SYBASE**
2. Enter **whoami** to verify that you are logged in as the sybase user.
3. Enter **ls -l** to list the files in long format.
4. Verify that the correct read and execute permissions are set.
5. Enter **cd install**.
6. Enter **ls -al RUN_CASCADE**.
7. Verify that the file has the correct group and ownership, and that sybase and dba appear in the third and fourth columns.
8. Verify that the line begins with -r-xr--r--.

I get a "cannot allocate shared memory" error when I start Sybase.

1. Make sure that the shared-memory allocation was added to the */etc/system* file and the system was rebooted after the file was edited.
2. Move the files *CASCADE.krg* and *CASCADE.srg0* in the */opt/sybase* directory to *CASCADE.krg.old* and *CASCADE.srg0.old* by entering the following commands:

   ```
   mv CASCADE.krg CASCADE.krg.old
   ```

   ```
   mv CASCADE.srg0 CASCADE.srg0.old
   ```

3. Restart the Sybase server again.

► Corrupt files are caused by improperly shutting down the Sybase server. These files are shared-memory files that Sybase uses. If these files become corrupt, you cannot start the server.

How do I know if NavisCore is running?

The NavisCore icon appears at the bottom of the screen. Never close this box, unless one of the supporting programs (such as HP OpenView) stops processing.

I keep getting the message “access denied.”

You are not logged on.

1. From the Misc menu, select NavisCore ⇒ Logon.
2. Enter your operator password.

I get error “1997” in the same window I started Open Windows.

1. The Sybase server cannot be accessed by NavisCore.
2. Check to see if the Sybase server is running.
3. Log in as the sybase user and change directories to ***/opt/sybase/install***.
4. Enter **showserver**.

How do I know the Sybase server is running?

1. Log in as the sybase user.
2. Change to the following directory:

   `/opt/sybase/install`

3. Enter **showserver**.

How do I start the Sybase server?

1. Log in as the sybase user.
2. Change to the following directory:

   /sybase/install

3. Enter **startserver -f RUN_CASCADE**.

How do I shut down the Sybase server?

1. Log in as the sybase user as follows:

   ```
   su - sybase
   ```

2. Shut down the Sybase server as follows:

   ```
   isql -U sa -P superbase
   ```

3. Enter the following commands:

   ```
   1> shutdown
   2> go
   ```

My mouse does not seem to be working.

The SPARCstation uses an optical mouse. Make sure you have the shiny mousepad.

After upgrading Solaris, I cannot pram sync. The tftp server is not running.

When you upgrade Solaris, Solaris loads a new version of the **/etc/inittab** file and renames the existing **/etc/inittab file**. As part of the NavisCore installation process, you added a line to the **inittab** file so that the system would invoke the Ascend tftp daemon to listen to the default tftp port for requests rather than using inetd. You must edit the new version of the inittab file to include the line that invokes the Ascend tftp daemon.

Use the following steps to add the line to inittab:

1. Enter the following command:

   ```
   vi /etc/inittab
   ```

2. While holding down the Shift key, enter **$G** to go to the end of the file.
3. While holding down the Shift key, enter **A** and press the Return key to append a line onto the file.
4. Add the following line to the end of the file:

   ```
   tf:3:respawn:/opt/CascadeView/bin/tftpserv > /dev/null
   ```

   These commands invoke the Ascend tftp daemon to listen to the default tftp port for requests, rather than using inetd. No tracing is enabled.

5. Press the Escape key.
6. Enter **:wq!**
7. At the # prompt, enter the following command:

   ```
   init Q
   ```

This command forces the system to read the inittab file. The system then starts the Ascend tftp daemon.

> You cannot retrieve and display trace and status information if you use Sun Microsystem's tftp daemon. If you use Sun Microsystem's tftp daemon, configure it to run with the command: `in.tfpd/tfpboot`. Do not run TFTP in secure mode (with the -s option) or switch download and configuration sync operations will fail.

Are any other files affected by upgrading to Solaris 2.5?

When you upgrade to Solaris 2.5, Solaris creates the file */var/sadm/install_data/upgrade_cleanup* to identify any files that may need to be modified after the update. Information about any files that you may need to modify is included at the end of the file. The following list outlines the types of entries that the *upgrade_cleanup* file includes. For more information, see the *Network Management Station Installation Guide*.

Entry

[*file1*]: existing file renamed to [*file2*]

Description

The file with the name [*file1*] was present on the system at the time of the upgrade. The file changed after the installation of Solaris 2.3. For this reason, the Solaris upgrade process renamed [*file1*] to [*file2*] before loading the new version of the file.

Action

Examine the contents of [*file2*] and compare it to the new version of the file. If there are differences, you may need to edit [*file1*] to reflect the differences.

Entry

[*file1*]: existing file preserved, the new version was installed as [*file2*]

Description

The file with the name [*file1*] was present on the system at the time of the upgrade. The file was preserved. The Solaris upgrade process loaded the new version of the file as [*file2*].

Action

Examine the contents of [*file2*] and compare it to the old version of the file. If there are differences you may need to edit [*file1*] to reflect the differences.

Entry

[*file*]: had been deleted and has now been restored

Description

The file with the name [*file1*] was deleted from the system since its original installation. The Solaris upgrade installed the new version of the file.

Action

Examine [*file1*] to determine whether or not to delete the file.

Entry

[*file*]: file type was changed from [*type1*] to [*type2*]

Description

At its original installation, the file with the name [*file*] was of type [*type1*]. The file was later replaced by a file of [*type2*]. (For example, a symbolic link may have been replaced by a regular file.) In most cases the Solaris upgrade restores the file to its original type.

Action

Examine [*file*] to determine whether or not to replace [*file*] with a file of [*type2*].

Entry

[*file*]: target of symbolic link was changed from [*target1*] to [*target2*]

Description

At its original installation, the file with the name [*file*] was a symbolic link to [*target1*]. The file was later changed to be a symbolic link to [*target2*]. (For example, a symbolic link may have been replaced by a regular file.) The Solaris upgrade process changed the link to point to its original target.

Action

Examine [*file*] to determine whether or not to change the symbolic link to point to the original target before the upgrade.

Entry

[*file1*]: target of hard link was changed from [*file2*]

Description

At its original installation, the file with the name [*file1*] was a hard link to [*file2*]. The file was later changed to be a hard link to [*file2*]. The Solaris upgrade changed the link to point to its original target.

Action

Examine the file to determine whether or not to change the hard link to point to the original target before the upgrade.

Common Operating Problems

My switch will not turn green.

1. Make sure you can ping the switch.
2. Make sure the initial configuration (performed through script download, PRAM Kermit, or console install) was successful.
3. Check the cable connections.
4. Review the configuration.

I can't ping my switch

1. Check the route to the switch. To do this, log on as the root user and enter **netstat -r**. This command causes the system to list the destination networks and gateways. Make sure the appropriate route is listed. You can also look at the Use column which lists the route to the switch.

   An H in the flag field of this route indicates you added a host route instead of a net route. (A UG in the flag field indicates a net route.) Make sure you use the keyword net in the route add statement. Note that Solaris follows traditional subnetting. For this reason the lowest route in a subnet always reverts to its IP class (for example, 152.148.50.0 becomes 152.148.0.0).
2. If you cannot find the ping utility, it is in the ***/usr/sbin*** directory.

I am locked out of a node that no one else is using.

This problem occurs if you improperly exit from HP OpenView, or if HP OpenView windows is hung and the user kills the process.

To correct this problem:

1. Change directories to */opt/CascadeView/bin* and execute the *cv-release-locks.sh* shell script. This lists the currently locked nodes, and the user name who has locked each node.

   The following example illustrates the type of output that the *cv-release-locks.sh* script displays.

   ```
   Net0x00000005.Sw0x00000011.Card0x00000019.Ppt0x00000025.Lpt0x0000003c
   by userone              with UserPid                  703
   ```

2. To release the lock, enter **sh cv-release-locks.sh [*first line of display*]**

   Using the example shown in Step 1, you would release the lock by typing the following:

   ```
   sh cv-release-locks.sh Net0x00000005.Sw0x00000011.
   Card0x00000019.Ppt0x00000025.Lpt0x0000003c
   ```

Performance is being degraded.

1. Find out how many X-terms you have logged in on the main screen.

   Do not run more than three event logs at the same time.

2. Check the Ascend Event Browser dialog box and see how often events come in (See “Using the Ascend Events Browser Dialog Box” on page 15-2.)
3. Check the CPU utilization with ***/usr/openwin/bin/perfmeter***. Do not leave this running, however, since it takes over CPU resources.
4. Make sure that the IP network icon is unmanaged (and has been from the start) and that it is currently hidden. The IP network icon should be disabled.

I cannot access a switch (red nodes)

If you attempt to configure the switch and the NMS with multiple community names and swap NMS entry one with NMS entry two, the switch may interchange the IP addresses (but not the community names), resulting in unreachable nodes. Check your NMS and switch configurations. See the *NavisCore NMS Getting Started Guide* for details.

I cannot delete a switch configuration from the database

You cannot delete a switch until you delete all of its associated configurations (trunks, circuits, etc.). See the *NavisCore NMS Getting Started Guide* for details.

What is the Event Monitor and what does it do for me?

In the NavisCore Network Management Station (NMS), the trap daemon is a separate process. The Event Monitor is the display for this process. Therefore, if you do not use Event Monitor you can close this process without affecting the rest of the NMS. See "Using the Ascend Events Browser Dialog Box" on page 15-2 of this guide for more information.

I keep getting the error / or /var is full.

1. The wtmp and wtmpx files may be too large. Enter the following to check the size of the */var/adm/wtmp* and */var/adm/wtmpx* files.

```
ls -al
```

2. The file may have tftpserv errors. Use the following command to check for tftpserv errors.

```
tail wtmp
```

> If the wtmp and wtmpx files are not very large, or if the wtmp file is filled with errors other than tftpserv errors, you should consult with your System Administrator.

3. Check to see if tftpserv is actually running. To do this, enter the following:

```
ps -ef|grep tftp
```

Null results indicate that tftpserv is not running. Contact the Ascend Core Switching Technical Assistance Center to determine why this condition exists.

If tftpserv is running, proceed to Step 4.

4. Clean the error logs in the */var/adm* directory. To do this you must delete the files and replace them with empty files that have the same characteristics. Use the following steps:

a. Log on as the root user.

b. Enter the following commands:

```
rm wtmp
touch wtmp
chown adm wtmp
chgrp adm wtmp
chmod 664 wtmp
rm wtmpx
touch wtmpx
chown adm wtmpx
chgrp adm wtmpx
chmod 664 wtmpx
```

c. Enter the following commands to move to the *tmp* directory and check to see if there are more than two tftpserv error logs.

```
cd /tmp
ls tftp.error.log.*
```

d. If there are a large number of error logs, enter the following to remove all of the error logs:

```
rm tftp.error.log.*
```

e. Periodically check the */opt/CascadeView.var/initFiles* and */opt/CascadeView.var/cfgSyncFiles* directories. The system creates these files each time you create a text file or PRAM sync a card or switch. Delete these files if you no longer have a need for them.

How do I change a logical port name?

You cannot use the NavisCore NMS to make this change. Use the following steps to make this change:

1. Change directories to */opt/CascadeView/bin*.

2. Run the *renamelp.sh* shell script.

In addition, if your installation has access to the NavisCore Toolbox product, you can use a utility called *cvtool_rename_lport* to rename logical ports.

What is a core file?

A core file is a UNIX process that dumps the entire system contents when it crashes. UNIX programmers can interpret this core file to determine what caused the system crash. If the NavisCore NMS crashes, you should copy the core file. The core file is usually from one to ten Mbytes or larger. After you make a copy of the core file you can delete it.

I'm in the correct directory and I can see the file, why can't I execute it?

Enter **./filename** instead of **filename**.

How do I change the IP address of my machine?

The following steps cannot be used in an NIS domain.

1. Change the IP address in the */etc/hosts* table for the entry corresponding to the machine. If it is part of an NIS domain, consult with your network administrator.
2. Change the Sybase map.
3. Enter the following command to delete the current configuration and add a new configuration.

   ```
   /opt/sybase/sybtli
   ```

What do I do if I get an error that the log device is full?

The following two procedures describe the actions you should take when the log device is full. Use *Procedure 2 only when the log is 100% full.* The log should be dumped each day to a backup device according to Sybase backup procedures.

Use *Procedure 1 to purge* the log daily when you do not want to backup the database.

Procedure 1

The following procedure safely purges the transaction log. To purge the log daily when you do not want to backup the database:

1. Log in to ISQL.
2. Enter the following commands:

   ```
   1> dump transaction cascview with truncate_only
   2> go
   ```

Procedure 2

The following steps leave the database in an inconsistent state. You must back up the database immediately after completing this procedure.

1. Log in to ISQL and enter the following commands.

```
1> dump transaction cascview with no_log
2> go
```

2. Enter the following command to leave ISQL.

```
1> quit
```

NMS to Network Connectivity Problems

Table 17-2 provides basic troubleshooting solutions for resolving connectivity problems between the NavisCore NMS software applications and the network.

Table 17-2. Connectivity Troubleshooting Solutions

Problem	Possible Causes	Solutions
Changes that you entered to the IP routing table have not taken affect.	Routing table entry was added in the wrong order.	Use the **netstat -nr** command to check the routing table. Make sure the entry is placed before the default route.
You are unable to access a Serial Port on the SPARCstation.	You may be using the wrong end of the split cable.	Connect the other end.
SPARC Network Interface Card fails.	The Network Interface card may be defective.	Run the diagnostic software supplied by the network card manufacturer. If the diagnostic program fails, remove and replace the card. Attempt to ping another host on the LAN to verify connectivity.
Ping failed: Network unreachable.	The gateway device could not forward the ping packet. Either the destination address is non-existent or the route in the netstat table does not match the Ethernet IP address in the switch.	Use NavisCore to change the current Ethernet IP Address. Then, regenerate the text file and repeat the text file transfer to the switch. Or, change the netstat route to reflect the Ethernet IP Address that is already configured in the switch.
Ping failed: timeout.	Either the IP address machine is down or the network path to the target IP address failed.	The other end of the connection did not respond to the ping command. Use the **ping -s** command to reach the IP address multiple times to determine if the problem persists.

Table 17-2. Connectivity Troubleshooting Solutions (Continued)

Problem	Possible Causes	Solutions
A switch or SPARC that was previously accessible is now unreachable.	Possible problem with the network routing, or a device(s) on the network is down.	Use the **ping -s** command to test the connectivity.
The switch icons in the network map remain Red, even after checking all of the following configurations: Ethernet or SLIP physical connections (cabling, transceiver connections, Ethernet drivers, Ethernet network interface cards), communications settings, software configurations, and all error messages.	The NMS is not communicating with the switch. There are many possible reasons for this problem: • The NMS may be sending the wrong ARP and ICMP requests. • You may have a faulty network interface card installed on the SPARC. • There may be an error in the network media. • The SPARC IP Address may be wrong. • The NMS Path is incorrect. • The Ethernet IP address for the switch is missing or incorrect	Use the **ping** command to test connectivity. Make sure that other active IP devices on the local network can respond to ICMP echo requests. You should also verify that the SPARC is sending proper ARP and ICMP echo requests by trying to ping a UNIX host or any other machine that supports TCP/IP protocol stack. If you get intermittent results, your problem may be hardware related. Run diagnostics on the network interface card and diagnose possible faults in the LAN or inter-network media. If the current IP Address of your SPARC is different from your SPARC’s IP address when you configured the switch, do one of the following: • Use a text editor to change your SPARC’s IP Address to reflect the IP Address that was downloaded to the switch. Then change the NMS Path IP address in NavisCore to reflect the NMS SPARC’s current IP address and regenerate the text file. Next, repeat the text file transfer to the switch. • Change the SPARC’s entry in the */etc/hosts* file to the new IP address and reboot the SPARC.

Technical Support Checklist

Before calling the Ascend Core Switching (CS) Technical Assistance Center (TAC) for assistance, make sure you have the following information:

☑ If you are experiencing NMS SPARCstation problems, check the SPARC and make note of the following:

- Model type
- Amount of available memory
- Operating system and version number
- Network interface card type
- NMS IP address
- Subnet mask

Also, display, print, and note any changes to the configuration files: *netstat -r*, *ifconfig -a*, *ovstatus*, and *showserver*. Pipe the results to a separate file to review later.

☑ If you cannot make a connection from the NMS to the switch, check and note the following:

- Connection method used, (Ethernet, Indirect Ethernet, SLIP, Management VPI/VCI, Management DLCI, Management SPVC, etc.)
- Type of modem used (if any)
- Cable and connection types (if applicable)
- All IP addresses for the NMS path, Primary NMS, second and third NMS (if any), and Ethernet IP address (if any) configured on the switch.
- If using the Indirect Ethernet, Management VPI/VCI, Management DLCI, or Management SPVC connection method, note the IP addresses of the associated routers.
- Static route has been added.

Please have access to your NMS SPARCstation when calling the Ascend Core Switching Technical Assistance Center.

☑ If you are trying to diagnose physical port problems, check and note the following:

- Physical attributes configured on the ports
- Cables, pinouts, and DSU/CSU equipment and related configurations
- Admin status

Contacting the Ascend CS TAC

Ascend provides a full range of support services to ensure that maximum network uptime is achieved with low equipment cost. The staff at the Ascend CS TAC is also available to assist with any problems you encounter while using the NMS software. You can contact the Ascend CS TAC by phone, email, or fax.

Calling by Phone

Ascend provides customer support 24 hours a day, 7 days a week. To contact the Ascend CS TAC by phone, call the following number:

1-800-DIAL-WAN (1-800-342-5926) or direct, 1-978-692-2600 (U.S and Canada)

1-978-952-7299 (outside the U.S., Canada, and United Kingdom)

0-800-96-2229 (in the United Kingdom)

Sending Electronic Messages or Faxes

To contact the Ascend CS TAC by email, address your requests to:

cs@casc.com

To fax the Ascend CS TAC, call:

1-978-392-9768

Include the following information when requesting support through electronic mail or a fax message:

- Your name and telephone number
- Name of contact person and telephone number (if different from above)
- Brief description of the problem
- List of symptoms
- Information identified in the Technical Support Checklist

A

Trap Alarm Condition Messages

This appendix describes, in alphabetical order, each of the trap alarm condition messages that the system reports in the Events Browser. Some events are informational, while others indicate a problem or potential problem within the network configuration.

The list indicates each trap alarm condition message along with a description of the trap and, where possible, a resolution for the condition. Italicized words indicate variable values. For example, *switch name* specifies the name of the switch.

A *card type* card has been inserted at *switch name*, Slot *slot number*

This trap indicates that an IOM has been installed in the specified slot.

A *card type* card has been removed from *switch name*, Slot *slot number*

This trap indicates that an IOM has been removed from the specified slot.

A Frame Relay usage record could not be created for Switch *switch name* *Number of records* usage records could not be created during day

This trap indicates that a Frame Relay usage record could not be created.

A mismatched card has been detected at *switch name*, Slot *slot number* (actual: *card type*, config: *port type*)

This trap indicates that the IOM installed in the slot does not match the NMS configuration for this slot. Use the switch console command “show system” to verify what is actually installed in the switch slot.

A usage record could not be created for *billing service type*

A Usage Data counter record could not be created for the specified node billing service type.

A usage record could not be created for service *billing service type*

The system could not create a usage data record because the Aggregated Usage Data store was at full capacity. This trap does not occur when the system is in a normal state. To resolve this condition, check the Adjunct Processor (AP) to see if it is on-line; if it is, check to see if the AP is connected to and communicating with the switching system.

A usage record counter-value overflow condition has occurred for *billing service type*

A Usage Data counter value overflow condition occurred while aggregating usage data recently collected from one or more IOPs. An overflow condition occurs when the system attempts to update a Usage Data counter, and the update would overflow the counter. Instead of updating the record, the system closes the filled Usage Data record and opens a new one. This can only be done if there is sufficient space in the service's aggregated usage data store.

The system generates only one of these traps for each collection period. For example, if your collection period is set to 30 seconds, and there are more than one Usage Record Creation Failures, only one Usage Record Overflow trap is generated. If the condition still exists when the next Collection Period starts, another Usage Record Overflow trap is generated at that time.

To resolve this condition, check the Adjunct Processor (AP) to see if it is on-line; if it is, check to see if the AP is connected to and communicating with the switching system.

Accounting Server *accounting server IP address* disk space for *disk directory* has been reduced to *disk percentage used* percent of capacity (Severity: *disk severity*)

This trap indicates that the disk space percentage used on the specified disk no longer exceeds the threshold value. The severity level that the trap reports corresponds to the exceeded threshold level.

Accounting Server *accounting server IP address* disk space for *disk directory* has exceeded *threshold value* percent of capacity (Severity: *threshold severity*). The disk percentage used on this file system is *disk percentage used*.

This trap indicates that the disk space threshold of the specified file system has been exceeded.

An ATM usage record could not be created for Switch *switch name*. *Number of records* usage records could not be created during day.

This trap indicates that an ATM usage record could not be created.

An authentication has failed on login *login user* due to *authentication failure reason*

This trap login fail reason indicates a user console authentication login failure.

An authentication assignment on Logical port *lport name* has failed due to *authentication fail reason*

Indicates a user authentication failure on a specified logical port.

An ISDN call has been rejected on Lport *port name* due to *reason*

An ISDN call was rejected due to one of the following reasons:

- Lack of B-channel pool resources.
- The system could not authenticate the call.

An ISDN IP address assignment failed on Lport *port name* due to *reason*

An ISDN IP address assignment failed call was rejected. The following list indicates the possible *reasons* for the call rejection:

- A user sent a configuration request without an IP address option.
- The assigned logical port IP address does not match the one in the configuration option.
- There are IP address conflicts with the one in the address pool that is already assigned.
- A client request for an IP address failed.

An ISDN authentication assignment on Logical port *lport name* has failed due to *authentication fail reason* (source: *E.164 source address*, destination: *E.164 destination address*)

This trap indicates a user ISDN authentication failure. The message indicates both the source and destination E.164 address for the ISDN connection.

An ISDN/PPP MP bundle modification on Logical port *lport name* has failed due to *multilink protocol fail reason* (source: *E.164 source address*, destination: *E.164 destination address*)

This trap indicates a failure to create an ISDN/PPP MP bundle or add a link to an MP Bundle. The message indicates both the source and destination E.164 address for the ISDN connection.

An MP bundle modification on Logical port *lport name* has failed due to *multilink protocol fail reason*

Indicates a failure to create an MP bundle or add a link to an MP Bundle.

A PPP negotiation has failed on logical port *lport name* due to *fail reason*

A Point-to-Point (PPP) negotiation has failed on the specified switch and logical port due to the specified PPP negotiation failure reason.

A PM Threshold Crossing has occurred in switch *switch name* at Slot *slot number* Port *port number*

This trap indicates that a threshold crossing was detected on the specified physical port on the specified slot on the specified switch for the performance parameter identified by the PM threshold object. This may indicate a physical layer problem with the port or the transmission media carrying the signal.

At Slot *slot number* Port *port number* in Switch *switch name* the protection line is now *state*

This trap indicates that a protection switching (APS) event has just taken place on the specified port on the specified slot on the specified switch.

At Slot *slot number* Port *port number* in Switch *switch name* attempting to receive traffic from working line

This trap indicates that the specified working line physical port (APS related) on the specified slot on the specified switch has resumed carrying user traffic. This may be due to either an auto switch condition that has cleared or a problem detected on the protection line.

At Slot *slot number* Port *port number* in Switch *switch name* a mode mismatch has been detected

This trap indicates that a mode mismatch has been detected based on this pport's APS configuration and the received K2 byte. This happens when one LTE is configured for 1+1 APS and the other for 1:n APS. The LTE configured for 1:n will fall back to 1+1 mode.

At Slot *slot number* Port *port number* in Switch *switch name* the protection line is now in a failed state

This trap indicates that the protection line is now in a failed state. APS switchover to protection is now inhibited. If the protection line was carrying user traffic, it is switched back to the working line.

At Slot *slot number* Port *port number* in Switch *switch name* the protection line is now in an operational state

This trap indicates that the protection line is now in an operational state. APS switchover to protection is now possible.

At Slot *slot number* Port *port number* in Switch *switch name* the protection line has declared a protection byte failure

This trap indicates that the protection line has declared a protection byte failure. This happens when a protection byte defect or inconsistent K1 byte is received and the condition persists for 2.5 seconds. APS switchover to protection is inhibited. If the protection line was carrying user traffic, it is switched back to the working line.

At Slot *slot number* Port *port number* in Switch *switch name* a far end protection line failure has been declared

This trap indicates that a far end protection line failure has been declared. This happens when the received K1 byte indicates SF on the protection line and the condition persists for 2.5 seconds.

At Slot *slot number* Port *port number* in Switch *switch name* the far end protection line failure has cleared

This trap indicates that the far-end protection line failure has cleared. This happens after 10 seconds without an indication of SF on the protection line in the received K1 byte.

At Slot *slot number* Port *port number* in Switch *switch name* a channel mismatch has been detected

This trap indicates that a channel mismatch has been detected. When the pportAPSconfigStatus is indicated as invalid, the user should check pportAPSadminDir, pportAPSlineType, pportAPSrevertiveMode, and pportAPSwtrPeriod for a mismatched configuration between the two physical ports.

At Slot *slot number* Port *port number* in Switch *switch name* the APS configuration status has changed to *new status*, the paired-with APS pport at Slot *slot number* Port *port number*

This trap indicates that the APS configuration status has changed. When the pportAPSconfigStatus is indicated as invalid, the user should check pportAPSadminDir, pportAPSlineType, pportAPSrevertiveMode, and pportAPSwtrPeriod for a mismatched configuration between the two pports.

At Slot *slot number* Port *port number* in Switch *switch name* a direction mode mismatch has been detected

This trap indicates that a direction mode mismatch has been detected on the indicated pport (the indicated pport is an APS protection line pport). This happens when one LTE is configured for Unidirectional and the other for Bidirectional mode.

ATM Accounting Server *ATM accounting server address* has had a switchover

This trap indicates that an ATM Accounting Server switchover has occurred.

Billing communications failure to adjunct processor *adjunct processor address*

The switch to the specified *adjunct processor address* has failed. For this reason, the system could not complete a Usage Data file transfer. As with the Usage Record Overflow trap, the generation rate of this message is controlled such that only one of these traps is generated for each collection period.

To resolve this condition, check the Adjunct Processor (AP) to see if it is on-line; if it is, check to see if the AP is connected to and communicating with the switching system.

Billing has been (*enabled/disabled*) for service *billing service type*

The billing system state was enabled or disabled at the specified *billing service type*. The billing system state is changed when a switch boots (billing becomes enabled), or when the state is changed manually via NavisCore.

Billing has been *billing service type* for service (*enabled/disabled*) on Lport *port name*

The billing system state was enabled or disabled at the specified *billing service type* and logical *port name*. The billing system state is changed on a logical port when a switch boots (billing becomes enabled), or when the state is changed manually via NavisCore.

Billing Sys Mgr on Active CP+ failed to recover the contents of the use data store on boot for switch *switch name* and for service *node billing service type*

Indicates a warning that the billing system manager on the active CP+ failed to recover the contents on boot.

Billing Sys Mgr on the Active CP+ discarded the data recovered on boot because they are too old for switch *switch name* and for service *node billing service type*

Indicates that the billing system manager on the active CP+ discarded the usage data recovered on boot because the data was outdated. Currently, any recovered data that is older than 30 days is discarded.

Billing usage data store on the redundant CP+ has failed for switch *switch name* and for service *node billing service type*

Indicates a warning that the billing system manager on the active CP+ failed to write the contents of the usage data store on the redundant CP+.

CBR Lport *lport name* at switch *switch name* error states: *starvation condition, receive overflow condition, loss of cell sequence, loss of structure pointer*

This trap indicates the error state of the CBR logical port. Error states are as follows:

Starvation Condition — ok (1), error (2)

Receive Overflow Condition — ok (1), error (2)

Loss of Cell Sequence — ok (1), error (2)

Loss of Structure Pointer — ok (1), error (2)

CBR PPort *switch name.slot number.port number* runs *clock mode* clock mode

This trap indicates that the CBR physical port switched its clock mode. Possible clock modes are as follows:

1 — Synchronous

2 — SRTS

3 — ACM

Circuit *circuit name* at switch *switch name* is *state* with *fail reason* (FailNode: *node ID*, FailPort: *lport IF index*)

This trap indicates the specified point-to-point ATM PVC or Frame Relay PVC on the specified switch has changed state. The possible states for the circuit include active (0), inactive (1), and invalid (2). When the circuit is inactive, an explanation is provided in the fail reason portion of the message. The node where the failure occurred is also indicated (the last 2 octets of the internal node ID is provided) along with the interface (IF) index of the logical port where the failure occurred. Use the Show All Logical Ports dialog box to determine the mapping between logical port names and IF indexes.

Possible fail reason variables for point-to-point and point-to-multipoint PVCs are described in Table A-1.

Table A-1. PVC Fail Reason Variable Values

Reason Variable	Condition
admindown (1)	Admin status of the PVC is down.
novcbuff (2)	No virtual circuit buffer.
nobw (3)	No bandwidth.
noroute (4)	No circuit route.
timeout (5)	A timeout has occurred.
nopdubuff (6)	No PDU buffer.
nodest (7)	No destination.
trknr (8)	Trunk route not received.
trkdown (9)	Trunk down.
balancereroute (10)	Balance reroute.
dead (11)	Circuit is dead.
defpathreroute (12)	Define a new path.
nidown (13)	Network interface is down; PVC is not transmitting.
otherpvcsegdown (14)	Other PVC segment is down.
otherpvcsegrnr (15)	Other PVC segment route not received.
usingaltpathwarning (16)	Using an alternate path.
iopdown (17)	An IOP used by the circuit is down.
numsgbuffer (18)	The PVC manager has no user message buffer for the PDU.
noport (19)	No logical port is configured for use by the PVC.
misconfig (20)	Configuration error.
svcsetupfail (21)	Soft PVC setup failed.
srcbackedup (22)	Source is in a backup condition.
srcunknown (23)	Source is unknown.
dstunknown (24)	Destination is unknown.
bkpdlcicollision (25)	DLCI collision occurred during backup.

Table A-1. PVC Fail Reason Variable Values (Continued)

Reason Variable	Condition
oldrevinpath (26)	A switch that is running an incompatible version of software is in the circuit path.
smdsmgmttrunk (27)	The PVC attempted to traverse an SMDS management trunk.
nevercalled (28)	The PVC endpoint was never called.
bothendptbackup (29)	Both endpoints are backups.
pvcroutemgmttrunk (30)	The PVC attempted to traverse a management trunk.
nomultipointparent (31)	No multipoint circuit parent was found.
pvcroutefail (32)	PVC route failed because it changed during setup.
novpivci (33)	No VPI/VCI is available.
svcuserclear (34)	User cleared the SVC. This error appears for SPVCs only.
pathregfailed (35)	Circuit path registration failed.
noatmchan (36)	The ATM channel selected by the PVC cannot be allocated.
norevbw (37)	No bandwidth in the reverse direction is available.
internalreset (38)	The PVC reset internally.
highprivcinpath (39)	High priority VCI is in the PVC's path. The PVC is disrupted due to priority routing.
nopribw (40)	No negative priority bandwidth could be allocated.

***Circuit name* at *switch name* has been rerouted**

This trap indicates that an ATM or Frame Relay PVC has been rerouted.

Circuit *circuit name* at switch *switch name* is setup or cleared: calling number: *calling party number,* called number: *called number*

This trap is generated by the ingress switch whenever an SVC is setup or cleared. The value of cktStatus indicates whether the circuit is initiating a setup or a clear.

Circuits on interfaces go *switch name, string*

Circuit interfaces (such as physical ports) on the switch go up or down. The data passed in *string* is 4 + n*134 bytes in length where n => 1. The first and second byte make up the interface/slot ID associated with the link that goes down or comes up. The third byte is the reason why circuits go down:

1 — A user link goes down.

2 — A trunk link goes down.

3 — An IOM goes down.

4 — A user link comes up.

The fourth byte is the count of entries in a 134-byte circuit bit map array that follows. In this array, the first two bytes represent the IOM slot associated with the circuits' DLCIs. The next two bytes represent the physical port ID associated with the DLCIs. The third pair of bytes represent the interface ID associated with the DLCIs.

The remaining 128 bytes (1024 bits) is a bit map for the DLCIs associated with the interface. The left-most bit of the first byte represents DLCI 0 and the right-most bit of the 128th byte represents DLCI 1023. If a bit is set, it means that the corresponding DLCI associated with the interface is up or down.

Clock generation unit *switch name.pport slot number.pport number* synchronized on clock source *clock source ID*

Indicates that the clock generation unit synchronized to a reference clock specified by *clock source ID*.

Clock generation unit *switch name.pport slot number.pport number* is in holdover mode

The clock generation unit switched to holdover mode.

CUG: Configuration error for *prefix name* on *switch name*

This trap indicates a run-time configuration error on the number of CUGs allowed per address.

CUG: Configuration error for *address name* on *switch name*

This trap indicates a run-time configuration error on the number of CUGs allowed per address.

CUG: Configuration error for *node prefix name* on *switch name*

This trap indicates a run-time configuration error on the number of CUGs allowed per node prefix.

DC 48V power supply input bus A at switch *switch name* is *status of input bus*

This trap indicates that the DC 48V power supply input bus A has changed state (that is, toggled between up and down states). *Status of input bus* can be one of the following values: 1 (Up) or 2 (Down).

DC 48V power supply input bus B at switch *switch name* is *status of input bus*

This trap indicates that the DC 48V power supply input bus B has changed state (that is, toggled between up and down states). *Status of input bus* can be one of the following values: 1 (Up) or 2 (Down).

DS1 at *channel number, port number, slot number, switch name* has changed loopback state to *state*

This trap indicates when the DS1 has changed its current loopback state.

The loopback state can change to one of the following:

- ds1ClearLoop (1)
- ds1PayloadLoop (2)
- ds1LineLoop (3)
- ds1DiagLoop (4)

DS1 at Channel *chan ID,* PPort *pport number,* Slot *slot number,* Switch *switch name* has changed alarm state to *alarm state*

Indicates when the DS1 changes its alarm state. The *alarm state* value can be any of the following values: none (0), red-alarm (1), yellow-alarm (2), blue-alarm (4), carrier-loss (8), looped-back (16).

DXI heartbeat poll exceeds threshold

A non-Ack count for SMDS DXI heartbeat poll exceeds the specified threshold. The non-Ack count value is reset every 15 minutes.

Establish the backup trunk associated lport *lport name* on switch *switch name*

An attempt to establish the backup trunk associated with the specified logical port is being made.

Fail to backup trunk with lport *lport name* on switch *switch name*e due to *lport backup fail reason*

This trap indicates that the primary trunk associated with the indicated logical port has not been backed up or the backup trunk associated with the indicated logical port has not been restored. The reason for the failure is either buTrkNotDef (primary trunk has not been backed up) or buTrkNotEstab (backup trunk has not been restored).

Fan *number* at *switch name* is *state*

This trap indicates that the specified fan in the specified switch has changed state to either up, down, or marginal.

Frame Relay Accounting Server *Frame Relay accounting server address* has had a switchover

This trap indicates that a Frame Relay Accounting Server switchover has occurred.

IOP in Slot *slot number* at switch *switch name* is down, following PVCs is also down: *circuit name list*

An IOP in the specified *slot number* is down; as a result the specified circuits are also down.

In switch *switch name* an alarm is opened or closed

The fault server generates this trap when an alarm is open or closed.

ISDN/PPP negotiation has failed on logical port *lport name* due to *PPP negotiation fail code* (source: *E.164 address*, destination: *E.164 address*)

This trap indicates that ISDN PPP Negotiations have failed on the specified logical port due to the specified PPP negotiation fail code.The trap also lists the E.164 address of the source of this ISDN connection and the E.164 address of the destination of this ISDN connection.

Logical port *lport name* has BAP or BACP call failure with status code *BAP call fail stat*

Indicates a failure on a BAP or BACP Call on the specified logical port. The *BAP call fail stat* variable is the BAP Call Fail Status code (Q.931 cause code).

Logical port *lport name* has ISDN/PPP BAP or BACP call failure with status code *BAP call fail status code* (*Q.931 cause code*) (source: *E.164 source address*, destination: *E.164 destination address*)

This trap indicates a failure on a ISDN/PPP BAP or BACP Call. The message indicates both the source and destination E.164 address for the ISDN connection.

Lport *port name* at switch *switch name* is *link protocol status*

The link protocol status for the specified logical port has changed states. Possible values for the *link protocol status* are up (1) or down (2). The link values can be Frame Relay, LMI, DXI heartbeat poll, PPP LCP, etc., depending on the logical port type.

Lport *port name* at switch *switch name* non-Ack count for SMDS DXI heartbeat poll exceeds threshold

A non-Ack count for the SMDS DXI heartbeat poll exceeds the threshold. The non-Ack count is reset every 15 minutes.

Lport *port name* at switch *switch name* SMDS discard packets exceed the threshold

The Total Discard packet count for an SMDS packet exceeds the specified threshold.

Lport *port name* at switch *switch name* has encountered *packet number* frame errors (exceed threshold *per minute threshold*)

The frame errors per minute on this logical port exceed the threshold. The *packet number* variable is the number of inbound packets that contained errors, which prevented them from being delivered to a higher layer protocol. When this number exceeds the specified per-minute threshold, a link error trap is sent.

Lport *name* in *switch name* is down, following PVCs are also down: *circuit name list*

The specified logical port is down; as a result, the specified circuits are also down.

Lport *name* in *switch name* is up, following PVCs are also up: *circuit name list*

The specified logical port is now active; as a result, the specified circuits are now active.

Lport *name* in *switch name* has congestion *rate %* (exceeded threshold *threshold %*)

The specified logical port is congested (threshold %). The *rate %* variable is the value of the congestion rate when the logical port entered a severely or absolutely congested state in the last minute interval. The *threshold %* variable is the alert threshold for the congestion rate. A trap is sent whenever the congestion rate exceeds this threshold value. This trap is not supported for SMDS.

> The following nine traps are based on a counter that is set from the Add Logical Port dialog box when you add an SMDS logical port. The threshold value can be set to a value from 1 to 255 (with a default value of 10). The threshold value applies to all nine traps.
>
> These trap violations occur during the transmission of an SMDS packet. The system maintains a counter for each type of violation and generates a trap each time the value in the counter exceeds the specified threshold value. After sending the trap, the system resets the counter to zero.

The number of SMDS DXI2 Invalid Mgmt Link ID violations exceeds the SMDS PDU violations threshold for the Lport *port name* in switch *switch name*

The number of invalid management link ID violations exceeds the specified SMDS PDU threshold for the logical port.

Lport *port name* in switch *switch name* the number of SMDS SIP3 Dest GA Not Found violations exceeds threshold

The number of destination group address not found violations exceeds the specified SMDS PDU threshold for the logical port.

Lport *port name* in switch *switch name* the number of SMDS SIP3 Dest GA Screen Fail violations exceeds threshold

The number of destination group address screen failures exceeds the specified SMDS PDU threshold for the logical port.

Lport *port name* in switch *switch name* the number of SMDS SIP3 Dest IA Not Found violations exceeds threshold

The number of destination individual address not found violations exceeds the specified SMDS PDU threshold for the logical port.

Lport *port name* in switch *switch name* the number of SMDS SIP3 Dest IA Screen Fail violations exceeds threshold

The number of destination individual address screen failure violations exceeds the specified SMDS PDU threshold number for the logical port.

Lport *port name* in switch *switch name* the number of SMDS SIP3 SA Not Found violations exceeds threshold

The number of source address not found violations exceeds the specified SMDS PDU threshold for the logical port.

Lport *port name* in switch *switch name* the number of SMDS SIP3 SA DA on Same Port violations exceeds threshold

The number of SA DA on Same Port violations exceeds the specified SMDS PDU threshold for the logical port.

Lport *port name* in switch *switch name* the number of SMDS SIP3 SA Not Found violations exceeds threshold

The number of source address not found violations exceeds the specified SMDS PDU threshold for the logical port.

Lport *port name* in switch *switch name* the number of SMDS SIP3 Source IA Screen Fail violations exceeds threshold

The number of source individual address screen failures exceeds the specified SMDS PDU threshold for the logical port.

ML Member Trunk *ML member lport name* at switch *switch name* bound to MLFR Trunk Bundle LPort *lport name* has changed state to *state*. The corresponding MLFR Trunk *trunk name* has total aggregate bandwidth of *aggregate BW* and operational bandwidth of *operational BW*.

This trap indicates that the ML member trunk associated with the specified logical port has changed state. Possible states include:

ndown (0) — The switches cannot establish a communication link.

nattempt (1) — A switch is attempting to contact another switch but has not yet received a response.

ninit (2) — A one-way communication exists between the switches.

n2way (3) — A bidirectional communication exists between the switches.

nexstart (4) — The switches are about to exchange information on the network topology.

nexchange (5) — The switches are exchanging network topology information.

nloading (6) — The switches are requesting the most recent link state information.

nfull (7) — The trunk is up and operational between the switches.

btdefined (9) — A backup trunk is ready.

No format in cvtrapd.conf for cascade view spec

No other NavisCore trap is configured. To configure a trap, access the HP OpenView Network Node Manager and then select Option ⇒ Event Configuration:SNMP.

OAM overload detected on circuit *circuit name* at switch *switch name* on lport *lport name*

This trap indicates that the OAM speed on this circuit has exceeded the threshold, which is 1,000 cells per second.

On switch *switch name* at Slot *slot number* the configured *card type value* type does not match the actual *card type value* type

This trap indicates that the IOA card type value specified through the NMS does not match the card type value of the installed card.

PMP ATM circuit *circuit name* endpoint index *number* at switch *switch name* is *Ckt Leaf Oper Status Ckt leaf Connection Fail Reason, Node Port*

This trap indicates that the point-to-multipoint ATM PVC state has been changed. The possible values for the *Ckt Leaf Oper Status* are the following: invalid (0), inactive (1), active (2). The possible values for the fail reason include the values in Table A-1.

Power supply *number* at *switch name* is *state*

This trap indicates the specified chassis power supply in the specified switch has changed state.

PPort *switch name, slot number, port number* is *state* with *alarm type*

The specified physical port on the specified IOM slot on the specified switch has changed state. Possible state values for the physical port are Up, Down, or Testing. Possible values for the alarm type are as follows:

None (0) — No alarm condition.

Red (1) — A loss of signal or out of frame error.

An out of frame error occurs when the receiver detects one of the following conditions:

- Two or more framing-bit errors within a 3 millisecond period
- Two or more errors within five or fewer consecutive framing bits

A loss of signal error occurs if the device detects 175+/-75 contiguous pulse positions of either positive or negative polarity.

After declaring a Red Alarm, the device sends a Yellow Alarm Signal to the far-end. The far-end then declares a Yellow Alarm.

Yellow (2) — A remote CSU is transmitting a Red Alarm. The remote CSU is not receiving any transmission signals from your circuit and the circuit is acting as a one-way link.

Blue (4) — A keep-alive condition exists. This condition occurs when the T1 multiplexer fails or is disconnected and the CSU sends continuous unframed 1s to the network in order to keep the signal alive.

Carrier loss (8) — A loss of T1 synchronization on the inbound (1x) signal has occurred.

Loopback (16) — The CSU is currently in a loopback state. See Chapter 5, “Testing Modules, Ports, and Channels” for more information about loopbacks.

PPort at *switch name*, *slot number, port number* has mismatched interface type (actual: *interface*, configured: *interface*)

This trap indicates the actual physical interface is different than the configured physical interface.

Pport *slot number.pport number* in switch *switch name* issues Threshold Crossing Alert on *ATM TCA ID*

This trap indicates that a threshold crossing problem was detected and the ATM TCA identified by the ATM TCA ID, slot number and physical port number was issued.

PPort *switch name.slot number.port number* has just gone *loopback status*

The loopback status of a D3/E3 or T1/E1 card has changed to one of the following status types:

Noloop — No loopback. The card currently has a loopback status of normal, no loopback is in effect.

Payloadloop — Payload loopback (a near-end loopback). When a payload loopback is activated, the signal transmitted beyond the loopback point (the forward signal) is the same as the received signal at the loopback point.

Line — Line loopback (a near-end loopback). A line loopback operates upon receipt of specific framed pulse patterns. The line loopback pulse codes and functions are either Activate or Deactivate.

Power supply #3 at switch *switch name* is *state*

This trap indicates power supply #3 has changed state (toggled between up and down states). Power supply status values include the following:

- up (1)
- down (2)
- marginal (4)

PRAM File *PRAM filename* download to switch *switch name* is complete

The download of the specified file from the NMS to the specified switch is complete. This trap should follow any PRAM synchronization attempt that the user performs from the NMS. Note that the affected module still must complete the automatic post-download warmboot before returning to full operation.

PRAM File *PRAM filename* download to switch *switch name* has failed

The download of the specified file from the NMS to the specified switch has failed. This trap may follow a PRAM synchronization attempt that the user performs from the NMS if the file download is unsuccessful for any reason. If this occurs, the PRAM synchronization should be reattempted.

Release the backup trunk associated with lport *lport name* on switch *switch name*

This trap indicates that the backup trunk associated with the specified logical port has been released.

Set DS0 *channel* on pport *switch name.slot number.port number* to DS0 far end loopback has failed

This trap indicates that the request to set a DS0 into far end loopback has failed.

Slot s*lot number* in switch *switch name* did not respond to the poll from the CP/SP/NP

This trap indicates that the IOM or CP/SP/NP in the specified slot in the specified switch has stopped responding to polls from the CP/SP/NP. This may be an indication of a problem with the IOM; under normal conditions, the IOM or CP/SP/NP should always respond to a poll from the CP/SP/NP. This trap will occur any time a card is either warm- or cold-booted and may occur during heavy congestion of the IOM CPU.

Slot s*lot number* in switch *switch name* has just come up

This trap indicates that the module in the specified slot in the specified switch has started to respond to polls from the CP, SP, or NP. This trap normally occurs after a module has completed its reboot cycle.

Slot *slot number* in switch *switch name* issues Threshold Crossing Alert on *ATM TCA ID*

This trap indicates the detection of a threshold crossing problem and that the ATM TCA identified by the ATM TCA ID and slot number was issued.

Pport *switch name.slot number.physical port number* DS1 ESF Data Link (FDL) status has changed state to *DS1 ESF Data Link (FDL) status*

This trap indicates a change in the status of the DS1 ESF Data Link (FDL). The DS1 ESF Data Link (FDL) status is the status as detected on the port and can be inService (1), outOfService (2).

Slot *slot number* at switch *switch name* transmit clock synchronization has changed state to *synchronization status*

The IOM transmit clock PLL synchronization status has changed.

Slot s*lot number* at switch *switch name* primary clock reference has changed state to *primary clock status*

The IOM system primary clock reference status has changed. Status values are normal (1) and failure (2).

Slot s*lot number* at switch *switch name* secondary clock reference has changed state to *secondary clock status*

The IOM system secondary clock reference status has changed. Status values are normal (1) and failure (2).

Slot s*lot number* at switch *switch name* clock reference has changed state to *sys primary clk status*

Indicates that the IOM system primary clock reference has changed to the specified system primary clock status as detected on the card. The sys primary clk stat variable can be either normal (1) or failure (2).

Slot s*lot number* at switch *switch name* secondary clock reference has changed state to *system secondary clk status*

Indicates that the IOM system secondary clock reference status has changed to the specified system secondary clock status as detected on the card. The system secondary clk stat value can be either normal (1) or failure (2).

SVC failure threshold has been exceeded on Lport *Lport name* at switch *switch name*

This trap indicates that the number of ATM and Frame Relay SVC failures that have occurred on the specified lport on the specified switch has exceeded the provisioned threshold. The default value of this threshold is 1 failure every 15 minutes (meaning that if 1 failure occurs in a 15-minute period, this trap will be displayed). If more than one failure occurs, another trap will not be displayed for another 15 minutes. Use the Show All Failed SVCs dialog box for specific information about the failures. See "Viewing ATM SVC Failed Calls" on page 13-77 for information on failed ATM SVCs. See "Viewing Frame Relay SVC Failed Calls" on page 14-45 for information on failed Frame Relay SVCs.

SW File *SW filename* download to switch *switch name* is complete

This trap indicates that an NMS-initiated download of the specified software file to the specified switch has succeeded and is now complete.

SW File *SW filename* download to switch *switch name* has failed

This trap indicates that an NMS-initiated download of the specified software file to the specified switch has failed. If this occurs, the user should reattempt the download.

Switch *switch name* up with possible changes (SNMP coldStart trap)

A coldStart trap indicates that the sending protocol entity is reinitializing itself and the agent's configuration or the protocol entity implementation may be altered.

Switch *switch name* up with no changes (SNMP warmStart trap)

A warmStart trap indicates that the sending protocol entity is reinitializing itself and neither the agent configuration nor the protocol entity implementation is altered.

Switch *switch name* interface down (SNMP linkDown trap) on Lport *lport name*

The sending protocol entity recognizes a failure in one of the communication links in your network configuration. The following conditions cause this trap to occur:

- The Admin Status of a physical port was set to down.
- The Admin Status of a logical port was set to down.
- A physical port has lost its input modem signals.
- An IOM was removed.
- An active optimum trunk had a status change and is now inactive.
- An active virtual circuit had a status change and is now inactive.
- An active T1/T3 channel had a status change and is now inactive.
- An active SLIP connection had a status change and is now inactive.
- A timeout was detected on an ethernet line.
- A persistent transmit stall was detected on a physical port.
- An active trunk received no response to five consecutive Keep Alive messages.
- An active trunk received an incorrect response to a Keep Alive message.
- An active trunk received a logical down response to a Keep Alive message.

Switch *switch name* interface up (SNMP linkUp trap) on Lport *lport name*

The sending protocol entity recognizes that one of the communication links represented in your network configuration has become active. The following conditions cause this trap to occur:

- The Admin Status of a physical port was set to up.
- The Admin Status of a logical port was set to up.
- A physical port has recovered its input modem signals.

- An IOM that was removed is now active.
- An inactive optimum trunk had a status change and is now active.
- An inactive virtual circuit had a status change and is now active.
- An inactive T1/T3 channel had a status change and is now active.
- An inactive SLIP connection had a status change and is now active.
- An inactive ethernet line is now active.

Switch *switch name*: Incorrect community name (SNMP authentication failure trap)

The sending protocol entity has received a protocol message that is not properly authenticated.

Switch *switch name*: EGP neighbor down (SNMP egpNeighborLoss Trap) for neighbor *ifIndex egpNeighAddr*

An EGP neighbor is down.

Switch *switch name* is reachable

This trap indicates that the specified switch is now reachable by the NMS.

Switch *switch name* is unreachable

This trap indicates that the specified switch is no longer reachable by the NMS. If this occurs, verify that the connectivity between the NMS workstation and the switch is intact and functioning (i.e., try using an NMS workstation to **ping** the switch).

Switch *switch name* trace table full

This trap indicates the node trace table was full and, for this reason, was copied to a TFTP buffer that will be transferred to the NMS.

Switch *switch name* diagnostic log table full

This trap indicates the diagnostic log table was full and, for this reason, was copied to a TFTP buffer that will be transferred to the NMS.

Switch *switch name* checksum or CRC-32 error occurred in flash

A checksum or CRC-32 error occurred in flash memory.

Switch *switch name* checksum error or battery problem occurred in PRAM

This trap indicates a checksum error or battery problem occurred in the PRAM.

Switch *switch name* fatal internal error encountered and system needs to be rebooted

This trap indicates the system encountered a fatal internal hardware or software error. Reboot the system in order to correct this problem.

Switch *switch name* IO error occurred in DRAM or SRAM

This trap indicates an I/O error occurred in DRAM or in SRAM.

Switch *switch name* has reported a non fatal error: Src=*source*, Time=*time*, Major=*major errcode*, Minor=*minor errcode*, String=*ASCII string*

This trap indicates a component in the switch discovered a non-fatal error condition. Possible values for the source variable are:

- power-on diagnostics (1)
- background-diagnostics (2)
- fault (3)
- frame-heap (4)

The time variable indicates the time that the last non-fatal error was reported. The major error code variable indicates the major error code of the last non-fatal error. The minor error code variable indicates the minor error code of the last non-fatal error. The ASCII string variable indicates the ASCII string that describes the last non-fatal error.

Slot *slot* in *Switch name* has reported a non fatal error: Src=*source*, Time=*time*, Major=*major errcode*, Minor=*minor errcode*, String=*ASCII string*

This trap indicates that the card in the reported slot discovered a non-fatal error condition. Possible values for the source variable are:

- power-on diagnostics (1)
- background-diagnostics (2)
- fault (3)
- frame-heap (4)

The time variable indicates the time that the last non-fatal error was reported. The major error code variable indicates the major error code of the last non-fatal error. The minor error code variable indicates the minor error code of the last non-fatal error. The ASCII string variable indicates the ASCII string that describes the last non-fatal error.

Slot *card logical slot*, Subcard *subcard physical slot* (Type=*subcard actual type*) in switch *switch name* now has an operational state of *state*

This trap indicates that a GX 550 subcard has changed to the specified state.

Slot *card logical slot*, Subcard *subcard physical slot* (Type=*subcard actual type*) in switch *switch name* has had a switchover

This trap indicates that a GX 550 subcard underwent a switchover.

Switch *switch name* Reserved for Frame Relay SVC

The specified switch name is reserved for Frame Relay SVC use.

Switch *switch name* primary synchronization reference operational state has changed to *primary clock synchronization reference*

Specifies that the Primary Synchronization Reference operational state has changed to the specified primary clock synchronization reference. Possible values include the following:

externala (1) — T1 Rate External Clock 1.

externalb (2) — T1 Rate External Clock 2.

portrefa (3) — IOM Port Reference Clock 1.

portrefb (4) — IOM Port Reference Clock 2.

internal (5) — Internal Free Running Clock.

Switch *switch name* secondary synchronization reference operational state has just changed to *primary clock synchronization reference*

Specifies that the Primary Synchronization Reference operational state has changed to the specified primary clock synchronization reference. Possible values for the Primary Synchronization Reference include the following:

externala (1) — T1 Rate External Clock 1.

externalb (2) — T1 Rate External Clock 2.

portrefa (3) — IOM Port Reference Clock 1.

portrefb (4) — IOM Port Reference Clock 2.

internal (5) — Internal Free Running Clock.

Switch *switch name* external reference clock *number* operational state has just changed to *state*

This trap indicates that the specified external reference clock (the T1 or E1 clock wired to the back of the switch SPA) on the specified switch has changed state. The following states are possible:

Active — The clock has been restored and is operational.

Detected Loss of Signal — The clock signal is no longer present.

Detected AIS Alarm — An AIS alarm has been received on the external clock port.

Detected Loss of Frame — The framing has been lost on the received signal.

Switch *switch name* external Reference Clock 1 operational state has just changed to *current state ext clk 1*

The External Reference Clock 1 operational state has changed to the specified current state of external clock 1. Possible values for *current state ext clk 1* include:

active (1) — Valid.

ais (2) — Detected AIS Alarm.

los (3) — Detected Loss Of Signal.

lof (4) — Detected Loss Of Frame.

Switch *switch name* external Reference Clock 2 operational state has just changed to *current state ext clk 2*

The External Reference Clock 2 operational state has changed to the current state of External Clock 2. Possible values for *current state ext clk 2* include the following:

active (1) — Valid.

ais (2) — Detected AIS Alarm.

los (3) — Detected Loss Of Signal.

Switch *switch name* port Reference Clock 1 operational state has just changed to *current state port clk A*

The Port Reference Clock 1 operational state has changed to the current state of port Reference Clock A. Possible values for *current state port clk A* include the following values:

active (1) — Valid.

down (2) — Invalid.

Switch *switch name* port Reference Clock 2 operational state has just changed to *current state port clk B*

The Port Reference Clock 2 operational state has changed to the current state of the Port Clock B reference. Possible values for *current state port clk B* include the following values:

active (1) — Valid.

down (2) — Invalid.

Switch to Accounting Server communication for *service number* has failed and a usage file transfer has failed to complete

This trap indicates a failed communication between a switch and an Accounting Server and that a usage file transfer has failed to complete.

Switch to ATM Accounting Server (AS) communication has failed for Switch *switch name* (Primary AS Address = *Primary Accounting Server Address*, Secondary AS Address = *Secondary Accounting Server Address*, Accounting Switch Control = *Switch Level Accounting Control*). A usage file transfer has failed to complete. *Number of Acctg Svr Comm Failures* have occurred during the day.

This trap indicates a failed communication between a switch and an ATM Accounting Server and that a usage data file transfer has failed to complete.

Switch to ATM Bulk Statistics Server communication has failed for Switch *switch name* (Server Address = *number*). A usage file transfer has failed to complete. Switch-to-Server communication failures have occurred during the day.

This trap indicates a failed communication between a switch and an ATM Bulk Statistics Adjunct Processor and that a usage data file transfer has failed to complete.

Switch to Frame Relay Accounting Server (AS) communication has failed for Switch *switch name* (Primary AS Address = *Primary Accounting Server Address*, Secondary AS Address = *Secondary Accounting Server Address*, Accounting Switch Control = *Switch Level Accounting Control*). A usage file transfer has failed to complete. *Number of Acctg Svr Comm Failures* have occurred during the day.

This trap indicates a failed communication between a switch and a Frame Relay Accounting Server and that a usage data file transfer has failed to complete.

The Accounting Server *accounting server IP address* failed to transfer one or more AMA files to the BOS

This trap indicates that the accounting server failed to transfer one or more accounting files to the BOS (Billing Operations Server).

The Accounting Server *accounting server IP address* has received data from a switch that is not in the configuration. Please update the Accounting Server configuration.

This trap indicates that the accounting server received data from a switch that is not defined in its configuration.

The Accounting Server *accounting server IP address* has been shut down

This trap indicates that the accounting server has been shut down.

The Accounting Server *accounting server IP address* is operational

This trap indicates that the accounting server is operational.

The ATM Accounting Control at the Logical Port (LP) level has been changed for Switch *switch name.* (LP Accounting Control = *logical-port--level accounting control,* LP Interface Index = *Lport If Index,* Slot ID = *slot ID,* Physical Port ID = *pport ID,* LP ID = *lport ID*).

This trap indicates that ATM accounting has been enabled or disabled on the specified logical port. The switch does not generate this trap when it boots (that is, when the global atmacctControl object is modified). The switch only generates this trap when the value of atmacctLportControl object is modified for a specific logical port.

The ATM Accounting Control has been changed for Switch *switch name* to *switch-level accounting control*

This trap indicates that ATM accounting has been enabled or disabled on the switch. The switch generates this trap when it boots or when the value of atmacctControl object is modified.

The backup clock source *backup clock source* is selected on port *pport number*, slot *slot number*, switch *switch name*

This trap indicates that the physical port has lost the external clock source and is switching over to the selected backup clock (if the physical port's IOM is in external clock source mode).

The DS0 *channel* on pport *switch name.slot number.port number* has just gone into the DS0 far end loopback

This trap indicates that the request to set a DS0 into far end loopback has succeeded.

The DS0s on port *Pport number,* slot *slot number,* switch *switch name* have just gone into the ds0 loopback

One or more DS0s have been put into loopback.

The DS0s on port *Pport number,* slot *slot number,* switch *switch name* have just gone out of loopback

One or more DS0s have returned from a status of loopback to a status of normal.

The external clock is recovered and the pport *pport number*, slot *slot number*, switch *switch name* will switch back to external clock

This trap indicates that the external clock has recovered and that the physical port will switch back to the external clock.

The Frame Relay Accounting Control has been changed for Switch *switch name* to *switch-level accounting control*

This trap indicates that Frame Relay accounting has been enabled or disabled on the switch. The switch generates the trap when it boots or when the value of fracctControl object is modified.

The Frame Relay Accounting Control at the Logical Port (LP) level has been changed for Switch *switch name.* (LP Accounting Control = *logical-port--level accounting control*, LP Interface Index = *Lport If Index,* Slot ID = *slot ID,* Physical Port ID = *pport ID,* LP ID = *lport ID*).

This trap indicates that Frame Relay accounting has been enabled or disabled on the specified logical port. The switch does not generate this trap when it boots (that is, when the global fracctControl object is modified). The switch only generates this trap when the value of fracctLportControl object is modified for a specific logical port.

The LPort NTM Congestion status of *interface index* at *switch name* has changed to *congestion status*

This trap indicates that there is a change of congestion status on a logical port. Possible values for the severe congestion status include the following:

- Not congested (1)
- Congested (2)

The NDC Threshold has been crossed (*switch name*, *interface number, source connection identification number*) with Incoming Discarded CLP0 Cells = *number* for the associated threshold value of *value*

This trap is a Network Data Collection Threshold Crossing Alarm for the number of CLP0 cells discarded in a PVC on an IOM. It is generated not more than once within the 15-minute NDC measurement interval.

The NDC Threshold has been crossed (*switch name*, *interface number, source connection identification number*) with Incoming Discarded CLP0+1 Cells = *number* for the associated threshold value of *value*

This trap indicates a Network Data Collection Threshold Crossing Alarm for the number of CLP0+1 cells discarded in a PVC on an IOM. It is generated not more than once within the 15-minute NDC measurement interval.

The operational state of the ATM accounting system on switch *switch name* has changed to *operational state of ATM accounting system*. The current Switch Level Accounting Control is *switch-level accounting control*.

This trap indicates that the operational state of the ATM accounting system on the switch has changed. The switch generates this trap when the ATM accounting system enters the non-operational state due to a critical failure of communications with the ATM Accounting Server. The switch also generates this trap upon recovery from this critical condition. This trap is not generated upon change of the atmacctOperState object in conjunction with an operator change of the atmacctControl object.

The operational state of the Frame Relay accounting system on switch *switch name* has changed to *operational state of Frame Relay accounting system*. The current Switch Level Accounting Control is *switch-level accounting control*.

This trap indicates that the operational state of the Frame Relay accounting system on the switch has changed. The switch generates this trap when the Frame Relay accounting system enters the non-operational state due to a critical failure of communications with the Frame Relay Accounting Server. The switch also generates this trap upon recovery from this critical condition. This trap is not generated upon change of the fracctOperState object in conjunction with an operator change of the fracctControl object.

The port *pport number* on slot *slot number*, switch *switch name* does not support external clock

This trap indicates that the physical port on the IOM (and the IOM itself) is not capable of running external clock.

The PPP LCP has entered the CLOSED state on LPort *lport name* at switch *switch name*

This trap indicates that PPP LCP has entered the CLOSED state on the specified logical port.

The PPP LCP has entered the OPEN state on LPort *lport name* at switch *switch name*

This trap indicates that PPP LCP has entered the OPEN state on the specified logical port.

The previous file transfer request *request* on switch *switch name* is *file transfer status*

This trap reports the outcome of a previous file transfer request.

The reference time server *IP address of reference time server* on the switch *switch name* fails to respond to an NTP time request and no other time servers are available

This trap indicates that a time server has failed to respond and that no other time server is available.

The stand-by card in *slot number* at *switch name* has become the active card

This trap indicates the card in the specified slot number is now the active partner of the pair (succeeding its partner to become the active partner).

The state of communications to the ATM accounting system on switch *switch name* has changed to *current state of communications to ATM accounting system*. The current Switch Level Accounting Server Control is *switch-level accounting server control* (Primary Accounting Server = *primary accounting server address,* Secondary Accounting Server = *secondary accounting server address)*.

This trap indicates a changed state of communications with the ATM accounting server.

The state of communications to the Frame Relay accounting system on switch *switch name* has changed to *current state of communications to ATM accounting system*. The current Switch Level Accounting Server Control is *switch-level accounting server control* (Primary Accounting Server = *primary accounting server address,* Secondary Accounting Server = *secondary accounting server address)*.

This trap indicates a changed state of communications with the Frame Relay accounting server.

The status of the ATM signaling function has changed to *status* on *lport name* at *switch name*

The ATM signaling function status has changed on the logical port. Status indicates the operational status of this function on the specified port.

The status of the ATM ILMI function has changed to *state* on Lport *Lport name* at switch *switch name*

This trap indicates that the ATM ILMI function has changed state for the specified logical port on the specified switch. This trap will only occur if the ILMI option on the logical port has been set to enabled. The following states are possible:

Up — Indicates that the logical port is successfully exchanging ILMI poll traffic between the switch and the attached device.

Down — Indicates that the logical port is no longer successfully exchanging ILMI poll traffic between the switch and the attached device. The logical port statistics screen can be used to help determine the specific cause of this problem.

The status of the ATM signalling function has change to *state* on *LPort name* at *switch name*

The ATM UNI or NNI signalling function has changed state for the specified logical port on the specified switch. This trap will only occur if the signalling option on the logical port has been set to enabled. The following states are possible:

Up — Indicates that the logical port is successfully exchanging Q.SAAL traffic (for UNI signalling) between the switch and the attached device.

Down — Indicates that the logical port is no longer successfully exchanging Q.SAAL traffic between the switch and the attached device. The logical port statistics screen can be used to help determine the specific cause of this problem.

Connecting — Indicates that the logical port is transmitting Q.SAAL traffic to the attached device but is not receiving any response from the attached device. The logical port statistics screen can be used to provide additional information.

The time on the switch *switch name* has been changed by *time difference* milliseconds. The new time is *the new time*.

This trap indicates that the time on the switch has changed, spanning a second boundary.

The time-of-day clock on switch *switch name* is invalid or has not been configured

This trap indicates that the time-of-day clock on the specified switch is invalid or has not been configured. This trap is generated only at CP/SP/NP boot-time.

Trunk *trunkname* in *switch name* is down. Following PVCs are also down: *circuit name list.*

The specified trunk is down; as a result, the specified circuits are also down.

Trunk *trunk name* at switch *switch name* is *state*

The specified trunk has changed states. Possible values for the state variable are:

ndown (0) — The switches cannot establish a communication link.

nattempt (1) — A switch is attempting to contact another switch but has not yet received a response.

ninit (2) — A one-way communication exists between the switches.

n2way (3) — A bidirectional communication exists between the switches.

nexstart (4) — The switches are about to exchange information on the network topology.

nexchange (5) — The switches are exchanging network topology information.

nloading (6) — The switches are requesting the most recent link state information.

nfull (7) — The trunk is up and operational between the switches.

btdefined (9) — A backup trunk is ready.

User *login name* has logged on to switch *switch name* from *location*

A user with the specified login name has logged into the specified switch name. The location variable identifies the user's location. This location is either an IP address (for Telnet) or a console number (for a serial port).

User *login name* has logged out from switch *switch name* through *location*

A user with the specified login name has logged out of the specified switch name. The location variable identifies the user's location. This location is either an IP address (for Telnet) or a console number (for a serial port).

B

Summary of Error Codes

You can interpret error codes differently, depending on the diagnostics source. For example, if the major/minor error code combination is 2.1 and the source is "Frame-heap," then the code indicates an outbound heap low condition. However, if the major/minor error code combination is 2.1 and the source is "Background diagnostics," then the code indicates a link stall detection condition.

Table B-1 on page B-2 summarizes the major and minor error codes when the source of the codes is background diagnostics. Table B-2 discusses some miscellaneous fatal error codes. See "Background Diagnostics" on page 5-2 for instructions on displaying these error codes.

For information on error codes from sources other than background diagnostics, consult the Ascend Core Switching (CS) Technical Assistance Center (TAC). See "Contacting the Ascend CS TAC" on page 17-19 for more information.

► An asterisk (*) appears after the Major Error Number to indicate that additional information about the error is included in the 960 trace area. If any of these errors occur on your system, contact the TAC at 1-800-DIAL-WAN (1-800-342-5926). Your TAC Representative can create a dump of the 960 trace area to determine the cause of the error. See "Contacting the Ascend CS TAC" on page 17-19 for more information on contacting the TAC.

This table also specifies those error numbers that indicate fatal error conditions. *For fatal error conditions, call the TAC. This manual does not describe how to resolve fatal errors.*

Table B-1. Summary of Error Codes for Background Diagnostics

Major Error	Minor Error	Status	Explanation
1	See Explanation	Non-Fatal	Background diagnostics stalled. The minor error number is seconds in this state. This error occurs when an I/O module is not defined in the processor module or there is an internal software problem. To resolve the error, configure the I/O slot and reinitialize the switch. See the *NavisCore NMS Getting Started Guide* for more information about initializing the switch. Call the TAC for assistance.
2 - 16	See Explanation	Non-Fatal	Link-stall detection. Transmit completions stalled. This error occurs when the switch cannot transmit because there is no clock present on the outbound interface. The major error number indicates the slot number, and the minor error number indicates the port number. To resolve, check the physical port configuration, particularly the IOM attributes. See Chapter 2, "Viewing Switch, Module, and Physical Port Details." Specify the clock configuration if there is no clock present.
20*	0	Fatal	Interrupt vectors corrupted. Call the TAC.
21*	See Explanation	Fatal	960 SRAM corrupted. The minor error number is the pointer to the bad SRAM location. Call the TAC.
22*	0	Fatal	Fault table corrupted. Call the TAC.
23	0	Fatal	Interrupts disabled. Call the TAC.
24	1	Fatal	Processor kernel force bad parity bit is on. Call the TAC.
24	2	Fatal	IOM force bad parity bit is on. Call the TAC.
25	0	Fatal	OS counter/timer is disabled. Call the TAC.
26*	See Explanation	Fatal	Stack overflowed. The minor error number specifies the ID of the corrupted stack. Call the TAC.
30*	2	Fatal	Heap error – invalid heap header on free. Call the TAC.
30*	3	Fatal	Heap error – out of memory on allocate. Call the TAC.
30	4	Fatal	Heap error – heap corrupted. Call the TAC.
31	1	Non-Fatal	PRAM initialized. This error is caused by resetting the PRAM. To resolve, resynchronize the PRAM in the card. See the *NavisCore NMS Getting Started Guide*.

Table B-1. Summary of Error Codes for Background Diagnostics (Continued)

Major Error	Minor Error	Status	Explanation
31	2	Non-Fatal	PRAM corrupted (header). To resolve, resynchronize the PRAM in the card. See the *NavisCore NMS Getting Started Guide*.
31	3	Non-Fatal	PRAM corrupted (bank 0). To resolve, resynchronize the PRAM in the card. See the *NavisCore NMS Getting Started Guide*.
31	4	Non-Fatal	PRAM corrupted (bank 1). To resolve, resynchronize the PRAM in the card. See the *NavisCore NMS Getting Started Guide*.
31	5	Non-Fatal	The PRAM version that this card is using is obsolete. The layout of the PRAM is incompatible with the software and the switch. To resolve, resynchronize the PRAM in the card. See the *NavisCore NMS Getting Started Guide* for more information.
31	6	Non-Fatal	Some PRAM records were discarded. To resolve, resynchronize the PRAM in the card. See the *NavisCore NMS Getting Started Guide* for more information.
31	7	Non-Fatal	PRAM is uninitialized or empty. To resolve, resynchronize the PRAM in the card. See the *NavisCore NMS Getting Started Guide* for more information.
32	0	Fatal	SRAM code space corrupted. Call the TAC.
33	0	Fatal	IRAM code space corrupted. Call the TAC.
35*	0	Fatal	960 fault 1. Call the TAC.
36*	0	Fatal	960 fault 2. Call the TAC.
37*	0	Fatal	960 fault 3. Call the TAC.
38*	0	Fatal	960 fault 4. Call the TAC.
39*	0	Fatal	960 fault 5. Call the TAC.
40*	0	Fatal	960 fault 6. Call the TAC.
41*	0	Fatal	960 fault 7. Call the TAC.
42*	0	Fatal	960 fault 8. Call the TAC.
43*	0	Fatal	960 fault 9. Call the TAC.
44*	0	Fatal	960 fault 10. Call the TAC.
46	0	Fatal	Parity error – IRAM (3000/6000). Call the TAC.
47	0	Fatal	Parity error – FMEM (3000/6000). Call the TAC.

Table B-1. Summary of Error Codes for Background Diagnostics (Continued)

Major Error	Minor Error	Status	Explanation
48	0	Fatal	FMEM self test failure. Call the TAC.
49	0	Fatal	Initialization error – device tables (3000/6000). Call the TAC.
50	0	Fatal	Initialization error – bd out heap (3000/6000). Call the TAC.
51	0	Fatal	Initialization error – bd in heap (3000/6000). Call the TAC.
52	0	Fatal	Initialization error – bd initialization (3000/6000). Call the TAC.
53	0	Fatal	Ethernet driver error. Call the TAC.
56	0	Fatal	Fatal internal error. Call the TAC.
57	0	Fatal	Obsolete
58	0	Fatal	Circular virtual circuit list on the rate enforcement queue. Call the TAC.
59	0	Fatal	Obsolete
128	0	Fatal	Cannot download bus. Call the TAC.
129	0	Fatal	Warm boot. Call the TAC.
130	0	Fatal	Cold boot. Call the TAC.
132	0	Fatal	The standby side of a redundant pair is shooting the active side. Call the TAC.
133	0	Non-Fatal	The PRAM is in conflict; PRAM is configured for another node. Each node has a unique ID. A card configured for one switch is now in use in a different switch. To resolve, resynchronize the PRAM in the card. See the *NavisCore NMS Getting Started Guide*.
134	0	Non-Fatal	The Admin Status of a card is set to Down. A card that has its Admin Status set to Down is not an operational card. To resolve, reactivate the card by setting the Admin Status field to Up on the Modify Logical Port dialog box. See the *NavisCore NMS Getting Started Guide* for more information.
135	0	Non-Fatal	Unused.
136	0	Fatal	The NMS caused a redundant switchover. This is a normal NMS procedure.

Table B-1. Summary of Error Codes for Background Diagnostics (Continued)

Major Error	Minor Error	Status	Explanation
137	See Explanation	Fatal	Illegal interrupt vector. This condition could be caused by either a software or hardware problem. The minor error number specifies the vector code. Call the TAC.
138	0	Fatal	Proxy message from the wrong card. Call the TAC.
144	0	Non-Fatal	A standby card is using a different version of the software. This error code indicates that the software revisions on the standby and active cards do not match. This is a warning condition and will not cause an interrupt in service. However, if you have to switch to the standby card, the older software revision may not support some features you are using on the active card. To resolve, update the standby card with the new software.
145	0	Fatal	IOM configured for MULTI. Call the TAC.
146	0	Fatal	Card service change. Call the TAC.
147	0	Fatal	Some I/O to PRAM failed. Call the TAC.
148	0	Fatal	One of the processor modules in a redundant pair of processor modules is incapable of the requested admin capability. Call the TAC.
149	0	Non-Fatal	A standby processor module card type is incapable of a requested administrative task. This error code indicates that the standby model type does not match the active model type. This is a warning condition and will not interrupt service. However, if you have to switch to the standby model type, the older version may not support some features you are using on the active type. To resolve, replace the standby processor module card type so that it matches the active processor module type.
149	1	Non-Fatal	A standby processor module type is incapable of a requested admin capability, however, the system allowed the admin change to be made. This warning condition will not interrupt service. However, if you have to switch to the standby processor module card type, the older version may not support some features that you are using on the active card. To resolve, replace the standby processor module so that it matches the active processor module.

Table B-1. Summary of Error Codes for Background Diagnostics (Continued)

Major Error	Minor Error	Status	Explanation
149	2	Non-Fatal	A standby processor module card type is incapable of a requested admin capability or SNMP set specified an invalid type. This condition is a warning condition and will not cause an interrupt in service. However, if you have to switch to the standby processor module card type, the older version may not support some features that you are using on the active card type. To resolve, replace the standby processor module so that it matches the active processor module.
149	3	Non-Fatal	The active IOM cannot perform a requested operation capability. For example, an SMDS request could have been made for a card that is for Frame Relay only. To resolve, replace the IOM with the correct card type.
149	4	Non-Fatal	The standby IOM cannot perform a requested operation capability. To resolve, replace the standby card with the correct card type at your earliest convenience.
150	1	Fatal	OSPF error – RTR Link State Address (LSA) is too big. Call the TAC.
150	2	Fatal	OSPF error – No LSA in the age bin. Call the TAC.
150	3	Fatal	OSPF error – Link State (LS) database is corrupted. Call the TAC.
150	4	Fatal	OSPF error – Bad LSA in NBR queue. Call the TAC.
150	5	Fatal	OSPF error – Bad LSA in NBR2 queue. Call the TAC.
150	6	Fatal	OSPF error – LSA not found. Call the TAC.
150	7	Fatal	OSPF error – NBR not found. Call the TAC.
150	8	Fatal	OSPF error – Error in timer queue. Call the TAC.
150	9	Fatal	OSPF error – Bad LSA in send Link State Uppath (LSU). Call the TAC.
150	10	Fatal	OSPF error – Duplicate Autonomous System Entry (ASE). Call the TAC.
150	11	Fatal	OSPF error – No areas. Call the TAC.
150	12	Fatal	OSPF error – Bad VL. Call the TAC.
150	13	Fatal	OSPF error – No BB Ifs. Call the TAC.
150	14	Fatal	OSPF error – No BB. Call the TAC.

Table B-1. Summary of Error Codes for Background Diagnostics (Continued)

Major Error	Minor Error	Status	Explanation
150	15	Fatal	OSPF error – No memory. Call the TAC.
150	16	Fatal	OSPF error – Bad receive packet. Call the TAC.
151	1	Fatal	OSPF error – Console logging errors. Call the TAC.
152	0	Fatal	Permanent Virtual Circuit (PVC) manager errors. Call the TAC.
153	0	Non-Fatal	Virtual circuit table errors; buffer limit reached. There are too many PVCs defined between two logical ports. To resolve, check the network configuration and reroute some PVCs. See the configuration guides for Frame Relay, ATM and IP Navigator for more information about how to configure PVCs.
154	1	Fatal	Fatal internal error. Call the TAC.
154	2	Fatal	The card cannot read the configuration. Call the TAC.
155	See Explanation	Fatal	Memory protection NMI. Call the TAC.
156	See Explanation	Non-Fatal	Congestion thresholds that have been specified are invalid.
157	See Explanation	Fatal	SAR chip HW error. These chips provide VC and VP shaping capabilities on ATM IWU and ATM CS modules. Call the TAC.
158	0	Non-Fatal	System timing reference problem. To resolve, check the source(s) for the system timing reference (see “Viewing System-Timing Options” on page 2-25). Make sure the timing source is properly configured and functional. If you cannot resolve the problem, contact the TAC for assistance.
159	See Explanation	Non-Fatal	SNMP errors, such as an OID length of 0.
160	See Explanation	Non-Fatal	MPT errors.
161	See Explanation	Non-Fatal	PNNI errors.
162	See Explanation	Non-Fatal	Signaling errors.
163	See Explanation	Non-Fatal	Invalid traffic class setting.

Table B-1. Summary of Error Codes for Background Diagnostics (Continued)

Major Error	Minor Error	Status	Explanation
164	See Explanation	Non-Fatal	Disk error detected by scandisk.
165	See Explanation	Non-Fatal	Software manager errors.

Table B-2. Summary of Miscellaneous Fatal Error Codes

Major Error	Minor Error	Fatal?	Explanation
3.2	See Explanation	Fatal	When this error appears on a processor module, it indicates a warm boot has occurred. This is an informational error message and it requires no intervention.
4	See Explanation	Fatal	Indicates chain corruption in a memory block. Call the TAC for assistance.
5	See Explanation	Fatal	Indicates a fatal error that you cannot resolve without assistance. Call the TAC.

Using Copy Database

Overview

The Copy Database utility enables you to copy data in to or out of any NavisCore database. The utility copies both data and schema definitions that represent the data. The utility does not require you to know which schema you should use for the new database.

Prerequisites

Before you run the Copy Database utility you must check the values for the following environment variables in the cvdb.cfg file:

- DSQUERY
- SYBASE

The Copy Database command format enables you to specify an optional server_name parameter that overrides the DSQUERY environment variable value. However, you cannot use the command format to override the Sybase environment variable. Use the instructions in the *Network Management Station Installation Guide* for information about setting the Sybase environment variable. You cannot access a Sybase server unless the server is specified in the Sybase interface file.

Naming Conventions

The Copy Database utility automatically creates a DDL script when copying data out from an existing NavisCore database. The data files and the DDL scripts are bundled into a single tar file. (Bulk Copy generates the data files, which only contain data. There is one file for each table in the database).The tar file name uses the following format:

CVCOPY_existing database name_data.tar

For example, if you want to copy a database named Boston, the tar file name would be:

CVCOPY_boston_data.tar

Processing

Figure C-1 illustrates the process flow for the Copy Database utility when you use the utility to copy in data.

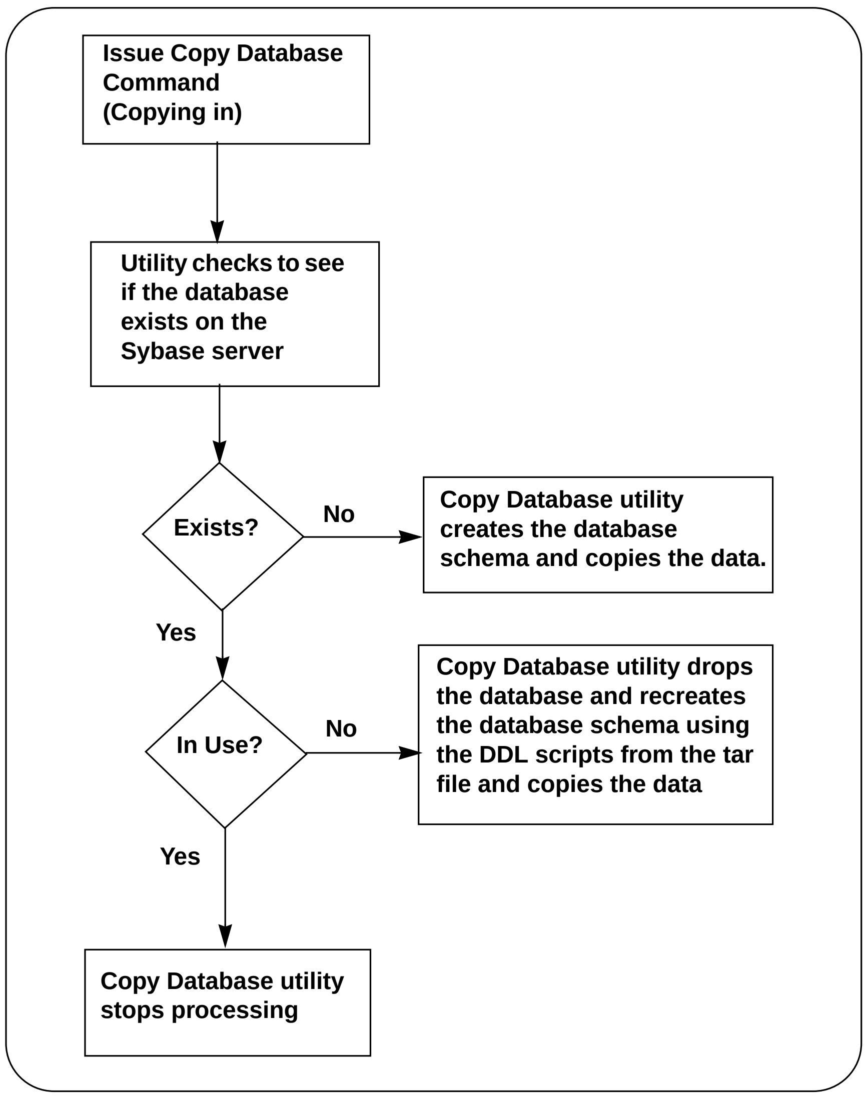


Figure C-1. Process Flow for Using Copy Database to Copy In

Figure C-2 illustrates the process flow for the Copy Database utility when you use the utility to copy out data.

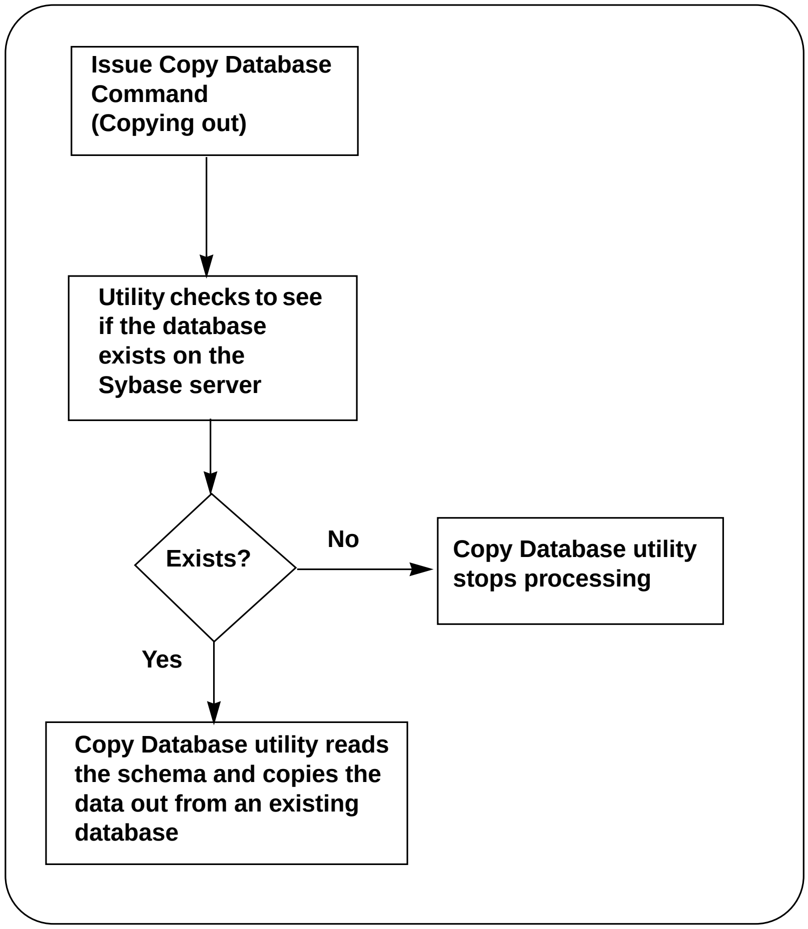


Figure C-2. Process Flow for Using Copy Database to Copy Out

Command Format

Issue the following command to run the Copy Database utility.

cv-copydb.sh (out/in) ***db_name [/server_name] password directory new_db_name [/server_name]***

Table C-1 describes the Copy Database utility commands.

Table C-1. Copy Database Utility Commands

Parameter	Specifies
in	That the utility should copy in data from a saved tar file to a new database.
out	That the utility should copy out data from an existing database.
db_name [/server_name]	One of the following depending on whether you are copying data in or out: db_name • *If you are copying data in***,** this is the database name that the utility uses to find the correct tar file for the database. • *If you are copying data out***,** this is the database that the utility copies. server_name • (Optional) When you are copying data *in*, the utility ignores this parameter if the *new_db_name* parameter is used. If you are copying data *in***,** this value overrides the server name defined in the cvdb.cfg file. • (Optional) If you are copying data *out***,** this value overrides the server name defined in the cvdb.cfg file. (The server that you specify for this parameter must be already defined in the Sybase interface file.)
password	The password for the system administrator.
directory	One of the following depending on whether you are copying data in or out: • *If you are copying data in***,** this is the directory where the saved tar file is located. • *If you are copying data out***,** this is the directory that the utility copies the data files to.
new_db_name [/server_name]	(Optional, for copying data *in* only) The name of the new database. This name must be at least 6 characters in length.

Examples

```
cv-copydb.sh out cascview superbase /cn/home/xxx
```

This command causes the Copy Database utility to copy out data from an existing database named cascview. The DSQUERY and Sybase environment variables are specified in the cvdb.cfg file.

```
cv-copydb.sh in cascview superbase /cn/home/xxx
```

This command causes the Copy Database utility to copy in data from a data file named CVCOPY_cascview_data.tar, and specifies the file's location as /cn/home/xxx. The DSQUERY and Sybase environment variables are specified in the cvdb.cfg file.

```
cv-copydb.sh in cascview superbase /cn/home/xxx testdb
```

This command causes the Copy Database utility to copy in data from a data file named CVCOPY_cascview_data.tar to another database named testdb. The DSQUERY and Sybase environment variables are specified in the cvdb.cfg file.

```
cv-copydb.sh out cascview/WEST11 superbase/tmp
```

This command causes the Copy Database utility to copy out data from an existing database named *cascview* from server *WEST11*. Sybase is set according to the environment variable specified in cvdb.cfg. The DSQUERY environment variable is overridden by the *WEST11* parameter value.

Errors

The following errors can occur when you use the Copy Database utility.

General Errors

The Sybase server defined in cvdb.cfg is not accessible.

This problem can be caused by a number of factors. The most common cause is a lack of space. Contact the Technical Assistance Center (TAC) for further information about how to resolve this error.

Cannot log into the database server $DSQUERY. Please check your input parameters, exiting now.

The specified database does not exist in the Sybase server. Check the database name and server name and reenter using a valid name.

Cannot locate the database $DB_NAME from server $DSQUERY, exiting now.

You have not specified a valid input database name for the db_name parameter. Check the value and reenter the command.

Make sure that no one else is running cv-copydb.sh with the directory $DATA_DIR. If no one is running the utility, remove the files CVOPY_${DB_NAME}_dbschema, CVCOPY_${DB_NAME}_crdb and all files that have the file name prefix of CVCOPY_BCP_${DB_NAME}, then run the utility again.

This error is due to one of the following problems:

- The specified database exists in the Sybase server and is in use. You cannot copy a database while it is in use. Use the Copy Database utility at another time.
- Another user is running the Copy Database utility using the same directory. You cannot copy a database while it is in use. Use the Copy Database utility at another time.
- The files specified in the error message need to be removed.

After you check and resolve the cause of the error, reissue the copy database command.

Copy-Out Errors

Error discovered when running dbschema to generate schema output file. Please check to make sure you have installed perl5 files and the dbschema file provided by Cascade under ${CV_ROOT} directory. Exiting now.

The Copy Database utility discovered an error when generating the schema output file. Check to make sure that the files specified in the message are installed.

Error discovered while using bulkcopy to copy out data for table *$table.*

Contact the TAC.

Copy-In Errors

Cannot drop the database $TEMP_DB_NAME, because it is in use.

The specified database is in use. Re-run the Copy Database utility at another time.

Error discovered when trying to create the database $TEMP_DB_NAME. Make sure that you have enough device space before running the utility. The output is saved in $TMPFILE1.

The utility discovered an error due to lack of available device space when creating the temporary database. Free the available device space and re-run the utility.

Error: unable to allocate enough data space for the database. Check CVCOPY_${TEMP_DB_NAME}_crdb file to make sure that the data size in the create database command is correct. Get instructions about how to change the data size in the CVCOPY_${TEMP_DB_NAME}_crdb file.

Change the data size for the database and run the utility again.

Unable to allocate enough log space for the database. Check CVCOPY_${TEMP_DB_NAME}_crdb file to make sure that the log size in the create database command is correct. Get instructions about how to change the log size in the CVCOPY_${TEMP_DB_NAME}_crdb file.

Change the log space value and run the utility again.

Fatal error discovered when trying to create the schema for $TEMP. For more information about the error, please read $TMPFILE.

Review the $TMPFILE for more information about this error.

D

Signalled QoS, BBC, ATC, and BEI Service Category Mappings

This appendix describes how the CBX 500 and GX 550 map ATM Forum Quality of Service (QoS) classes, Broadband Bearer Classes (BBC), ATM Transfer Capability (ATC), and the Best Effort Indicator (BEI) to the CBX 500 and GX 550 service categories.

> ATC applies to ATM UNI 4.0 signalling and PNNI 1.0 signalling only.
>
> ATM UNI 4.0/PNNI 1.0 signalling is a superset of ATM UNI 3.0/3.1 signalling. Unless otherwise noted, the signalling-related information in this appendix applies to all signalling variants.

QoS service classes are designed to accommodate the various types of traffic, such as video and LAN traffic, in the network. These classes include Constant Bit Rate (CBR), Variable Bit Rate Real-Time (VBRrt), Variable Bit Rate Non-Real-Time (VBRnrt), Available Bit Rate (ABR), and Unspecified Bit Rate (UBR). See "Definition of Specified QoS Classes" on page D-2 for more information on these classes.

When PVCs are provisioned, the CBX 500 or GX 550 service class is selected by the operator as part of the provisioning process.

For SVCs that use ATM UNI 3.0/3.1 and Q.2931 signalling, the CBX 500 or GX 550 selects the service class, based on the QoS, BBC, and BEI contained in the received UNI Signalling SETUP message. If the QoS class is unspecified, the BBC and BEI provide information that allow the service provider (i.e., the CBX 500 or GX 550) to select the appropriate QoS class.

For SVCs that use ATM UNI 4.0 or PNNI 1.0 signalling, the CBX 500 or GX 550 selects the service category, based on the QoS, BBC (which contains the ATC), and BEI contained in the received UNI Signalling SETUP message. If the QoS class is unspecified, the BBC and the ATC/BEI combination provide information that allow the service provider (i.e., the CBX 500 or GX 550) to select the appropriate QoS class.

This appendix references specific sections from the *ATM Forum's UNI Appendix A specifications (3.0 and 3.1)* and from the *ATM Forum's UNI Signalling Specification Version 4.0*. For detailed information on the QoS, BBC, and BEI role in ATM UNI 3.0/3.1, see the *ATM Forum's UNI Appendix A specifications (3.0 and 3.1)*. For detailed information on the QoS, BBC, ATC and BEI role in ATM UNI 4.0, see the *ATM Forum's UNI Signalling Specification Version 4.0*.

Definition of Specified QoS Classes

From ATMF UNI 3.1 Appendix A, Section A.4.1:

This section describes the ATM Forum's definition of the specified QoS classes. It is helpful to review these definitions in order to understand how the CBX 500 and GX 550 map ATMF QoS elements. The following text is an excerpt from ATMF UNI 3.1 Appendix A, Section A.4.1. Comments specific to the CBX 500 and GX 550 are noted in italics.

A Specified QoS class provides a quality of service to an ATM virtual connection (VCC or VPC) in terms of a subset of the ATM performance parameters defined in section 3 of ATMF UNI 3.1 Appendix A. For each Specified QoS class, there is one specified objective value for each performance parameter identified as defined in section 3 of ATMF UNI 3.1 Appendix A.

Initially, each network provider should define objective values for a subset of the ATM performance parameters of section 3 for at least one of the following Service Classes from ITU-T recommendation I.362 in a reference configuration that may depend on mileage and other factors:

Service Class A — Circuit Emulation, Constant Bit Rate Video (*CBX 500/GX 550 CBR service category*).

Service Class B — Variable bit Rate Audio and Video (*CBX 500/GX 550 VBR-RT service category*).

Service Class C — Connection-Oriented Data Transfer (*CBX 500/GX 550 VBR-NRT service category*).

Service Class D — Connectionless Data Transfer (*CBX 500/GX 550 ABR/UBR service category*).

In the future, more ‘QoS Classes’ may be defined for a given ‘Service Class’ described above.

The following Specified QoS Classes are currently defined:

Specified QoS Class 1 — Support a QoS that will meet Service Class A performance requirements.

Specified QoS Class 2 — Support a QoS that will meet Service Class B performance requirements.

Specified QoS Class 3 — Support a QoS that will meet Service Class C performance requirements.

Specified QoS Class 4 — Support a QoS that will meet Service Class D performance requirements.

The Specified QoS Class 1 should yield performance comparable to current digital private line performance. Specified QoS Class 2 is intended for packetized video and audio in teleconferencing and multi-media applications. Specified QoS Class 3 is intended for interoperation of connection oriented protocols, such as Frame Relay. Specified QoS Class 4 is intended for interoperation of connectionless protocols, such as IP, or SMDS.

You may configure the same performance for all, or a subset of Specified QoS Classes, provided the requirements of the most stringent Service Class are met. (*The CBX 500/GX 550 provides a separate service category for each of the specified QoS classes*.)

For example, assuming the SVC SETUP message contains the proper combination and structure, the following guidelines apply:

- *A signalled QoS class of 1 will result in a CBX 500/GX 550 service category of CBR.*
- *A signalled QoS class of 2 will result in a CBX 500/GX 550 service category of VBR-RT.*
- *A signalled QoS class of 3 will result in a CBX 500/GX 550 service category of VBR-NRT.*
- *A signalled QoS class of 4 will result in a CBX 500/GX 550 service category of UBR.*

Definition of Unspecified QoS Class

The Unspecified QoS class requires special handling by the CBX 500 and GX 550 because the ATMF Unspecified QoS does not directly map to any specific service category. This is reinforced in the following excerpts from ATMF UNI 3.1 Appendix A, Section A.4.2. Comments specific to the CBX 500 and GX 550 are noted in italics.

In the Unspecified QoS class, no objective is specified for the performance parameters. However, the network provider may determine a set of internal objectives for the performance parameters. In fact, these internal performance parameter objectives need not be constant during the duration of a call. Thus, for the Unspecified QoS class there is no explicitly specified QoS commitment on either the CLP=0 or the CLP=1 cell flow.

Services using the Unspecified QoS class may have explicitly specified traffic parameters. This means the "network provider" (*or the CBX 500/GX 550*) has several options for handling unspecified QoS. For ATM UNI 3.1, this involves the role of the BBC and BEI. For ATM UNI 4.0, this involves the role of the BBC, ATC, and the BEI.

An example application of the Unspecified QoS class is the support of "best effort" service. For this type of service, the user selects the Best-Effort Capability, the Unspecified QoS class and only the traffic parameter for the Peak Cell Rate on CLP=0+1. As indicated in Section 3.6.2.4, this capability can be used to support users that are capable of regulating the traffic flow into the network and to adapt to time-variable available resources. (*The Unspecified QoS class with a signalled Best Effort traffic descriptor is the type of service requested by the majority of ATM SVC capable CPE. This maps directly to the CBX 500/GX 550 UBR service category.*)

The Unspecified QoS class is identified by the integer zero (0) in the ILMI MIB or a code point in a signalling message for the requested QoS class. (*This is why unspecified QoS class is also called QoS class 0.*)

Using unspecified QoS, the CBX 500 and GX 550 use the BBC information element and the presence (or non presence) of the BEI to determine what service category should be used for the SVC. For a detailed description of each BBC, see the ATM Forum UNI specifications.

Support of Class X, Class A, and Class C ATM Transport Services

For ATM UNI 3.0/3.1 signalling and Q.2931 signalling, when dealing with unspecified QoS, the CBX 500 and GX 550 use the BBC information and the presence (or lack of) of the BEI as a means of determining what service category should be used for the SVC. The ATMF UNI 3.1 specification also provides information on each BBC meaning.

For ATM UNI 4.0 signalling, when dealing with unspecified QoS, the CBX 500 and GX 550 use the following elements as a means of determining what service category should be used for the SVC:

- Broadband Bearer Class (BBC) in octet 5 of the Broadband bearer capability information element.
- The value of the ATC, if present, and the absence or presence of the BEI in octet 18 of the ATM Traffic Descriptor information element.

The following ATMF excerpts from ATM Forum UNI 3.1 Chapter 5, Section 5.1.2.6 describe the Broadband Bearer Class greater detail.

Class X service is a connection-oriented ATM transport service where the AAL, traffic type (VBR or CBR) and timing requirements are user defined (i.e., transparent to the network). The user chooses only the desired bandwidth and QoS with appropriate information elements in a SETUP message to establish a class X connection.

Class A service is a connection-oriented, constant bit rate ATM transport service. Class A service has end-to-end timing requirements. Class A service may require stringent cell loss, cell delay, and cell delay variation performance. The user chooses the desired bandwidth and the appropriate QoS in the SETUP message to establish a Class A connection.

Class C service is a connection-oriented, variable bit rate ATM transport service. Class C service has no end-to-end timing requirements. The user chooses the desired bandwidth and QoS with appropriate information elements in a SETUP message to establish a class C connection.

The Phase 1 Signalling specified in this document supports Class X, Class A and Class C service. Class D service is not directly supported by signalling. It can be supported via a Class X or Class C connection to a connectionless server.

The ATMF specifications do not directly indicate how a network provider (i.e., Ascend) should map BBC to service category. In switch software Release 1.1.x (and previous releases), the CBX 500 and GX 550 always mapped unspecified QoS to the UBR service category, regardless of the BBC. In switch software Release 1.2.1 (and future releases), changes were made to utilize the BBC when deciding which service category to map to unspecified QoS.

The specific mappings were made as a result of the ATMF guidelines and customer requirements. Because the BBC information element also contains traffic type and timing requirement fields, it is difficult to make general statements about which BBC maps to which CBX 500/GX 550 service category. Instead, it is important to reference ATMF UNI 3.1 Appendix F or Annex 9 of the *ATM Forum's UNI Signalling Specification Version 4.0*. Appendix F and Annex 9 list several guidelines and describe the valid combinations of BBC and QoS for ATM UNI 3.0/3.1 and Q.2931 signalling and ATM UNI 4.0 signalling. Excerpts of this appendix and this annex are provided in the following section.

Guidelines on Use of Bearer Class, Traffic Parameters, and QoS

From ATMF UNI 4.0 Signalling Annex 9:

▶ Corresponding descriptions in *ATM UNI 3.1 Appendix F* are almost identical.

The following are brief descriptions of the various BCOB classes in the Bearer capability information element (see ITU-T Recommendation F.811 for additional information).

BCOB-A (*ATMF UNI 4.0 Section A9.1.1*)

This class is only used for requesting a virtual channel service. When the user specifies BCOB-A, the user is requesting more than an ATM-only service. The network may look at the AAL information element to provide interworking based upon its contents. One example of such interworking would be between an ATM user calling a non-ATM user who has switched DS1 capability. In this case, the network interworking function would need to know the AAL used to be able to perform this interworking function. Another example is for internetworking with N-ISDN circuit switching service.

BCOB-C (*ATMF UNI 4.0 Section A9.1.2*)

This class is only used for requesting a virtual channel service. As for BCOB-A, when the user specifies BCOB-C, the user is requesting more than an ATM only service. The network may look at the AAL information element to provide internetworking based upon its contents.

BCOB-X (*ATMF UNI 4.0 Section A9.1.3*)

This class is only used for requesting a virtual channel service. When the user specifies BCOB-X, the user is requesting an ATM-only service from the network. In this case, the network shall not process any higher layer protocols (e.g., AAL protocols).

The difference between BCOB-X and the other classes is what service is being requested from the network. For the VBR user that wants only a ATM cell relay service, the user should specify BCOB-X and Traffic Type VBR.

A user who is placing a DS1 circuit emulation call (but does not want to allow interworking) should specify BCOB-X and Traffic Type CBR. If the user wishes to allow interworking, then the user should specify BCOB-A.

Transparent VP Service (*ATMF UNI 4.0 Section A9.1.4*)

> Transparent VP Service applies to ATM UNI 4.0 and PNNI 1.0 only.

When the user specifies Transparent VP Service, the user is requesting an ATM-only service from the network. This service offers BCOB-X in that with the Transparent VP Service, both the VCI field (except for VCI values 0, 3, 4, and 6 through 15) and Payload Type field will be transported transparently by the network.

Allowed Combination of Bearer Capabilities, Traffic Parameters, and QoS in ATM UNI 3.0/3.1 and Q.2931

From Section F.2:

The parameters specified in the Broadband Bearer Capability IE, the Traffic Descriptor IE, and the Quality of Service Parameters IE of the SETUP message should be consistent. Table D-1 shows the allowable combinations of the Broadband Bearer Capability classes, the Traffic Descriptor parameters and the Quality of Service classes based on tables 5-7 and 5-8. If an illegal combination of parameters is specified, the call should be cleared with cause #63 “service or option not available, unspecified.”

Table D-1 (*from Table F-1 in ATMF UNI 3.1*) uses the following entries:

- PCR = Peak Cell Rate, SCR = Sustainable Cell Rate, MBS = Maximum Burst Size
- Y = Yes, N = No, S= Specified
- Y/N = either Yes or No is allowed.
- * = allowed QOS class values are a network option. Class 0 is always supported for alignment with ITU-T.
- & = parameter is coded to either “No indication” or “VBR” or octet 5a (Traffic Type/Timing Required) is absent; these three codings are treated as equivalent.
- && = parameter is coded to either “No indication” or “No” or octet 5a (Traffic Type / Timing Required) is absent; these three codings are treated as equivalent.
- A blank entry in the table indicates that the parameter is not present.

Table D-1. Allowable Combinations of Traffic Related Parameters in the SETUP message (ATM UNI 3.0/3.1 and Q.2931)

Broadband Bearer Capability	1	2	3	4	5	6	7	8	9	10	11	12
Broadband Bearer	A,C	X	X	C	X	C	X	A,C	X	X	C	X
Traffic Type		CBR	&		&		&		CBR	&		&
Timing Required		Y	&&		&&		&&		Y	&&		&&
Traffic Descriptor												
PCR (CLP=0)	S	S	S									
PCR (CLP=0+1)	S	S	S	S	S	S	S	S	S	S	S	S
SCR (CLP=0)				S	S							
SCR (CLP=0+1)						S	S					
MBS (CLP=0)				S	S							
MBS (CLP=0+1)						S	S					
Best Effort											S	S
Tagging	Y/N	Y/N	Y/N	Y/N	Y/N	N	N	N	N	N	N	N
QoS Classes	*	*	*	*	*	*	*	*	*	*	0	0

Specific Service Category Mappings in ATM UNI 3.0/3.1 and Q.2931

In an effort to simplify the interpretation of the ATMF UNI 3.1 Appendix F specification and other ATMF UNI 3.1 specification excerpts in this appendix, Table D-2 simplifies the process of determining the specific CBX 500/GX 550 service category mappings.

Table D-2 lists the CBX 500/GX 550 service category for a number of QoS and BBC combinations. The table uses the following entries:

- BEI = NO indicates the BEI is not present.
- BEI = YES indicates the BEI is present.
- N/A indicates the parameter is either not applicable or not allowed.
- CC 63 indicates the CBX 500 or GX 550 will reject the SVC with the cause code of 63 or “service or option not available, unspecified.”

The QoS information presented in this table (and in the Show All Failed SVCs dialog box) is the signalled QoS, not the actual service category. For signalled QoS classes 1 through 4, the mapping is clear. For unspecified QoS, you must look at the BBC contents and use Table D-2 to determine the actual service category. Although you can use the View QoS Parameters dialog box to determine the service category, the information on the dialog box may be difficult to interpret if many VCs exist on a logical port.

Table D-2. CBX 500/GX 550 ATM UNI 3.0, 3.1, Q.2931 Service Category Mappings (Based on Signalled QoS, BBC, BEI)

Table D-1 (App F.) Column	QoS	BBC	BEI	Traffic Type	Timing Req.	Service Category	Notes
1	0	A	NO	N/A	N/A	CBR	x
1	0	C	NO	N/A	N/A	VBR-NRT	x
1	1	A	NO	N/A	N/A	CBR	x
1	1	C	NO	N/A	N/A	CBR	x
1	2	A	NO	N/A	N/A	VBR-RT	x
1	2	C	NO	N/A	N/A	VBR-RT	x
1	3	A	NO	N/A	N/A	VBR-NRT	x
1	3	C	NO	N/A	N/A	VBR-NRT	x
1	4	A	NO	N/A	N/A	UBR	x
1	4	C	NO	N/A	N/A	UBR	x
2	0	X	NO	CBR	e/e tmg req’d	CBR	x
2	1	X	NO	CBR	e/e tmg req’d	CBR	x
2	2	X	NO	CBR	e/e tmg req’d	N/A	CC 63
2	3	X	NO	CBR	e/e tmg req’d	N/A	CC 63
2	4	X	NO	CBR	e/e tmg req’d	N/A	CC 63
3	0	X	NO	No indication	No indication	VBR-NRT	x
3	1	X	NO	No indication	No indication	N/A	CC 63
3	2	X	NO	No indication	No indication	VBR-RT	x
3	3	X	NO	No indication	No indication	VBR-NRT	x

Table D-2. CBX 500/GX 550 ATM UNI 3.0, 3.1, Q.2931 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

Table D-1 (App F.) Column	QoS	BBC	BEI	Traffic Type	Timing Req.	Service Category	Notes
3	4	X	NO	No indication	No indication	UBR	x
3	0	X	NO	VBR	e/e tmg not req'd	VBR-NRT	x
3	1	X	NO	VBR	e/e tmg not req'd	N/A	CC 63
3	2	X	NO	VBR	e/e tmg not req'd	VBR-RT	x
3	3	X	NO	VBR	e/e tmg not req'd	VBR-NRT	x
3	4	X	NO	VBR	e/e tmg not req'd	UBR	x
4	0	C	NO	N/A	N/A	VBR-NRT	x
4	1	C	NO	N/A	N/A	CBR	x
4	2	C	NO	N/A	N/A	VBR-RT	x
4	3	C	NO	N/A	N/A	VBR-NRT	x
4	4	C	NO	N/A	N/A	UBR	x
5	0	X	NO	No indication	No indication	VBR-NRT	x
5	1	X	NO	No indication	No indication	N/A	CC 63
5	2	X	NO	No indication	No indication	VBR-RT	x
5	3	X	NO	No indication	No indication	VBR-NRT	x
5	4	X	NO	No indication	No indication	UBR	x
5	0	X	NO	VBR	e/e tmg not req'd	VBR-NRT	x
5	1	X	NO	VBR	e/e tmg not req'd	N/A	CC 63

Table D-2. CBX 500/GX 550 ATM UNI 3.0, 3.1, Q.2931 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

Table D-1 (App F.) Column	QoS	BBC	BEI	Traffic Type	Timing Req.	Service Category	Notes
5	2	X	NO	VBR	e/e tmg not req'd	VBR-RT	xx
5	3	X	NO	VBR	e/e tmg not req'd	VBR-NRT	x
5	4	X	NO	VBR	e/e tmg not req'd	UBR	x
6	0	C	NO	N/A	N/A	VBR-NRT	x
6	1	C	NO	N/A	N/A	CBR	x
6	2	C	NO	N/A	N/A	VBR-RT	x
6	3	C	NO	N/A	N/A	VBR-NRT	x
6	4	C	NO	N/A	N/A	UBR	x
7	0	X	NO	No indication	No indication	VBR-NRT	x
7	1	X	NO	No indication	No indication	N/A	CC 63
7	2	X	NO	No indication	No indication	VBR-RT	x
7	3	X	NO	No indication	No indication	VBR-NRT	x
7	4	X	NO	No indication	No indication	UBR	x
7	0	X	NO	VBR	e/e tmg not req'd	VBR-NRT	x
7	1	X	NO	VBR	e/e tmg not req'd	N/A	CC 63
7	2	X	NO	VBR	e/e tmg not req'd	VBR-RT	x
7	3	X	NO	VBR	e/e tmg not req'd	VBR-NRT	x
7	4	X	NO	VBR	e/e tmg not req'd	UBR	x

Table D-2. CBX 500/GX 550 ATM UNI 3.0, 3.1, Q.2931 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

Table D-1 (App F.) Column	QoS	BBC	BEI	Traffic Type	Timing Req.	Service Category	Notes
8	0	A	NO	No indication	No indication	CBR	x
8	1	A	NO	No indication	No indication	CBR	x
8	2	A	NO	No indication	No indication	VBR-RT	x
8	3	A	NO	No indication	No indication	VBR-NRT	x
8	4	A	NO	No indication	No indication	UBR	x
8	0	C	NO	No indication	No indication	CBR	x
8	1	C	NO	No indication	No indication	CBR	x
8	2	C	NO	No indication	No indication	VBR-RT	x
8	3	C	NO	No indication	No indication	VBR-NRT	x
8	4	C	NO	No indication	No indication	UBR	x
9	0	X	NO	CBR	e/e tmg req’d	CBR	xx
9	1	X	NO	CBR	e/e tmg req’d	CBR	x
9	2	X	NO	CBR	e/e tmg req’d	N/A	CC 63
9	3	X	NO	CBR	e/e tmg req’d	N/A	CC 63
9	4	X	NO	CBR	e/e tmg req’d	N/A	CC 63
10	0	C	NO	No indication	No indication	VBR-NRT	x

Table D-2. CBX 500/GX 550 ATM UNI 3.0, 3.1, Q.2931 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

Table D-1 (App F.) Column	QoS	BBC	BEI	Traffic Type	Timing Req.	Service Category	Notes
10	1	C	NO	No indication	No indication	N/A	CC 63
10	2	C	NO	No indication	No indication	VBR-RT	x
10	3	C	NO	No indication	No indication	VBR-NRT	x
10	4	C	NO	No indication	No indication	UBR	x
10	0	C	NO	VBR	e/e tmg not req'd	VBR-NRT	x
10	1	C	NO	VBR	e/e tmg not req'd	N/A	CC 63
10	2	C	NO	VBR	e/e tmg not req'd	VBR-RT	x
10	3	C	NO	VBR	e/e tmg not req'd	VBR-NRT	x
10	4	C	NO	VBR	e/e tmg not req'd	UBR	x
11	0	C	YES	N/A	N/A	UBR	x
11	1	C	YES	N/A	N/A	N/A	CC 63
11	2	C	YES	N/A	N/A	N/A	CC 63
11	3	C	YES	N/A	N/A	N/A	CC 63
11	4	C	YES	N/A	N/A	N/A	CC 63
12	0	X	YES	No indication	No indication	UBR	x
12	1	X	YES	No indication	No indication	N/A	CC 63
12	2	X	YES	No indication	No indication	N/A	CC 63
12	3	X	YES	No indication	No indication	N/A	CC 63

Table D-2. CBX 500/GX 550 ATM UNI 3.0, 3.1, Q.2931 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

Table D-1 (App F.) Column	QoS	BBC	BEI	Traffic Type	Timing Req.	Service Category	Notes
12	4	X	YES	No indication	No indication	N/A	CC 63
12	0	X	YES	VBR	e/e tmg not req'd	UBR	x
12	1	X	YES	VBR	e/e tmg not req'd	N/A	CC 63
12	2	X	YES	VBR	e/e tmg not req'd	N/A	CC 63
12	3	X	YES	VBR	e/e tmg not req'd	N/A	CC 63
12	4	X	YES	VBR	e/e tmg not req'd	N/A	CC 63

Determination of ATM Service Category in ATM UNI 4.0/PNNI 1.0

From ATMF UNI 4.0 Signalling, Section A9.2:

The ATM service categories assigned to connections at UNI 4.0 and PNNI 1.0 are defined in the ATM Forum Traffic Management Specification, Version 4.0. An explicit way of requesting a particular ATM service category is provided in UNI 4.0 (and PNNI 1.0) signaling. Instead, the requested ATM service category must be derived from three pieces of information in a signalling message. The ATM service category is derived from:

1. The Broadband bearer class in octet 5 of the Broadband bearer capability (BBC) information element.
2. The absence or presence of the ATM transfer capability (ATC) octet (octet 5a) in the Broadband bearer capability information element.
3. The value of the ATC if present, and the absence or presence of the Best effort indicator in octet 18 of the ATM Traffic Descriptor information element.

The octet representing ATC has been changed from containing two relevant fields in UNI 3.x to a single field in UNI 4.0. The two fields in UNI 3.x were “Traffic Type” which indicated whether the traffic was CBR or VBR, and “Timing Requirements” which indicated whether end-to-end timing was required or not. In UNI 4.0, the entire octet 5a was changed to a single field and named the ATM Transfer Capability. For reasons of backward compatibility valid pairs of codepoint from the previous two fields were maintained and incorporated into single-field codepoints for ATC. In addition, new codepoints for the ATC have been defined.

Table D-3 summarizes the different combinations of Broadband bearer class, ATC, and Best effort indicator which define the ATM service categories. In addition the table provides a correlation between the single-field ATC codepoints and meaning of these codepoints in terms of the old two fields in octet 5a of the BBC information element in UNI 3.0/3.1.

Table D-3. Derivation of ATM Service Categories from Signalling Information (ATM UNI 4.0 and PNNI 1.0)

ASC (a)	BBC (b)	ATC (c)	BEI (d)	Equivalent UNI 3.0/3.1 Octet 5a Definitions	Comment
CBR	A	abs	No	Absent	None
		7		CBR traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding
	X	4	No	CBR traffic type, timing not indicated	None
		5		CBR traffic type, end-to-end timing required	None
		6		CBR traffic type, end-to-end timing not required	None
		7		CBR traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding
	VP	5	No	CBR traffic type, end-to-end timing required	New in UNI 4.0
		7		CBR traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding
rt-VBR	C	9	No	VBR traffic type, end-to-end timing required	None
		19		Undefined traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding
	X	1	No	Traffic type not indicated, end-to-end timing required	None
		9		VBR traffic type, end-to-end timing required	None
		19		Undefined traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding
	VP	9	No	VBR traffic type, end-to-end timing required	New in UNI 4.0
		19		Undefined traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding

Table D-3. Derivation of ATM Service Categories from Signalling Information (ATM UNI 4.0 and PNNI 1.0) (Continued)

ASC (a)	BBC (b)	ATC (c)	BEI (d)	Equivalent UNI 3.0/3.1 Octet 5a Definitions	Comment
nrt-VBR	C	abs	No	absent	None
		11		VBR traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding
	X	abs	No	Absent	None
		0	No	Traffic type not indicated, timing not indicated	None
		2	No	Traffic type not indicated, end-to-end timing not required	None
		8	No	VBR traffic type, timing not indicated	None
		10	No	VBR traffic type, end-to-end timing not required	None
		11	No	VBR traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding
	VP	abs	No	Absent	New in UNI 4.0
		10	No	VBR traffic type, end-to-end timing not required	New in UNI 4.0
		11	No	VBR traffic type, reserved timing requirement	New in UNI 4.0, invalid UNI 3.1 BBC octet 5a coding
UBR	C	abs	Yes	Absent	None
	X	abs	Yes	Absent	None
		0	Yes	None	None
		2	Yes	None	None
		8	Yes	None	None
		10	Yes	None	None
	VP	abs	Yes	Absent	New in UNI 4.0
		10	Yes	VBR traffic type, end-to-end timing not required	New in UNI 4.0

Table D-3. Derivation of ATM Service Categories from Signalling Information (ATM UNI 4.0 and PNNI 1.0) (Continued)

ASC (a)	BBC (b)	ATC (c)	BEI (d)	Equivalent UNI 3.0/3.1 Octet 5a Definitions	Comment
ABR	C	12	No	Undefined traffic type, timing not indicated	New in UNI 4.0, invalid in UNI 3.1 BBC octet 5a coding
	X				
	VP				

Legend:
(a) ATM Service Category as defined by ATM Forum Traffic Management Specification, Version 4.0 Specification.
(b) Broadband Bearer Class in octet 5 of Broadband bearer capability information element.
(c) ATM Transfer Capability as defined in this Specification (octet 5a of the Broadband Bearer Capability information element).
(d) Best Effort Indicator – Octet 18 of ATM Traffic descriptor information element (yes - present, no - not present).

Allowed Combination of Bearer Capabilities, Traffic Parameters, and QoS in ATM UNI 4.0 and PNNI 1.0

From ATMF UNI 4.0 Signalling, Section A9.3:

The parameters specified in the Broadband Bearer Capability information element, the ATM traffic descriptor information element, the Extended QoS parameters information element, the End-to-End transit delay information element, and the QoS parameter information element of the SETUP message should be consistent. Table D-4 shows the allowable combinations of the Broadband Bearer Class, the ATM traffic descriptor parameters, the Extended QoS parameters, the End-to-end transit delay, and the QoS classes.

If a SETUP message is received containing a combination of Broadband Bearer Class, ATC and Best Effort Indicator that does not match an entry in Table D-4, the call shall be cleared with Cause #65, “Bearer capability not implemented.” If the combination of Traffic parameters, QoS parameters and QoS class in a SETUP message is not a combination allowed for the ATM Service Category, the call shall be cleared with Cause #73, “Unsupported combination of traffic parameters.”

Table D-4. Allowable Combinations of Traffic and QoS Related Parameters in the SETUP Message (ATM UNI 4.0 and PNNI 1.0)

ATM Service Category	**CBR**								
Conformance	CBR.1 (note 10)			(Note 4)			(Note 4)		
Bearer Capability									
Broadband Bearer Class	A	X	VP	A	X	VP (note 5)	A	X	VP (note 5)
ATM Transfer Capability (Note 1)	7			Absent	4, 5, or 6	5	Absent	4, 5, or 6	5
Traffic Descriptor for a given direction									
PCR (CLP=0)							S		
PCR (CLP=0+1)	S			S			S		
SCR, MBS (CLP=0)									
SCR, MBS (CLP=0+1)									
Best Effort									
Tagging	N			N			Y/N		
Frame Discard	Y/N			Y/N			Y/N		
QoS Classes	*			*			*		
transit delay (note 2)	O			O			O		
peak-to-peak CDV	O			O			O		
CLR (CLP=0) (Note 11)				O			O		
CLR (CLP=0+1) (Note 11)	O								
ATM Service Category	**Real Time VBR (continues)**								
Conformance	VBR.1 (note 10)			VBR.2			VBR.3		
Bearer Capability									
Broadband Bearer Class	C	X	VP	C	X	VP	C	X	VP
ATM Transfer Capability	19			9	1 or 9	9	9	1 or 9	9

Table D-4. Allowable Combinations of Traffic and QoS Related Parameters in the SETUP Message (ATM UNI 4.0 and PNNI 1.0) (Continued)

ATM Service Category	Real Time VBR (continued)			
Traffic Descriptor for a given direction				
PCR (CLP=0)				
PCR (CLP=0+1)	S	S	S	
SCR, MBS (CLP=0)		S	S	
SCR, MBS (CLP=0+1)	S			
Best Effort				
Tagging	N	N	Y	
Frame Discard	Y/N	Y/N	Y/N	
QoS Classes	*	*	*	
transit delay (note 2)	O	O	O	
peak-to-peak CDV	O	O	O	
CLR (CLP=0) (Note 11)		O	O	
CLR (CLP=0+1) (Note 11)	O			
Conformance	(notes 4, 7)	(notes 4, 8)	(note 4)	
Bearer Capability				
Broadband Bearer Class	X	X	X	C or VP (note 5)
ATM Transfer Capability	1 or 9	1 or 9	1 or 9	9
Traffic Descriptor for a given direction				
PCR (CLP=0)	S			
PCR (CLP=0+1)	S	S	S	
SCR, MBS (CLP=0)				
SCR, MBS (CLP=0+1)			S	
Best Effort				
Tagging	Y/N	N	N	

Table D-4. Allowable Combinations of Traffic and QoS Related Parameters in the SETUP Message (ATM UNI 4.0 and PNNI 1.0) (Continued)

ATM Service Category	Real Time VBR (continued)		
Frame Discard	Y/N	Y/N	Y/N
QoS Classes	*	*	*
transit delay (note 2)	O	O	O
peak-to-peak CDV	O	O	O
CLR (CLP=0) (Note 11)	O	O	O
CLR (CLP=0+1) (Note 11)			

<table>
<tr><th>ATM Service Category</th><th colspan="9">Non-Real Time VBR (continues)</th></tr>
<tr><td>Conformance</td><td colspan="3">VBR.1 (note 10)</td><td colspan="3">VBR.2</td><td colspan="3">VBR.3</td></tr>
<tr><td colspan="10">Bearer Capability</td></tr>
<tr><td>Broadband Bearer Class</td><td>C</td><td>X</td><td>VP</td><td>C</td><td>X</td><td>VP</td><td>C</td><td>X</td><td>VP</td></tr>
<tr><td>ATM Transfer Capability (note 1)</td><td colspan="3">11</td><td>Absent</td><td>Absent, 0, 2, 8 or 10</td><td>Absent, 10</td><td>Absent</td><td>Absent, 0, 2, 8 or 10</td><td>Absent, 10</td></tr>
<tr><td>Traffic Descriptor for a given direction</td><td colspan="3"></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>PCR (CLP=0)</td><td colspan="3"></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>PCR (CLP=0+1)</td><td colspan="3">S</td><td colspan="3">S</td><td colspan="3">S</td></tr>
<tr><td>SCR, MBS (CLP=0)</td><td colspan="3"></td><td colspan="3">S</td><td colspan="3">S</td></tr>
<tr><td>SCR, MBS (CLP=0+1)</td><td colspan="3">S</td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>Best Effort</td><td colspan="3"></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>Tagging</td><td colspan="3">N</td><td colspan="3">N</td><td colspan="3">Y</td></tr>
<tr><td>Frame Discard</td><td colspan="3">Y/N</td><td colspan="3">Y/N</td><td colspan="3">Y/N</td></tr>
<tr><td>QoS Classes</td><td colspan="3">*</td><td colspan="3">*</td><td colspan="3">*</td></tr>
<tr><td>transit delay (note 2)</td><td colspan="3">(note 3)</td><td colspan="3">(note 3)</td><td colspan="3">(note 3)</td></tr>
<tr><td>peak-to-peak CDV</td><td colspan="3"></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>CLR (CLP=0) (Note 11)</td><td colspan="3"></td><td colspan="3">O</td><td colspan="3">O</td></tr>
</table>

Table D-4. Allowable Combinations of Traffic and QoS Related Parameters in the SETUP Message (ATM UNI 4.0 and PNNI 1.0) (Continued)

ATM Service Category	**Non-Real Time VBR (continued)**						
CLR (CLP=0+1) (Note 11)	O						
Conformance	(notes 4, 7)		(notes 4, 8)		(note 4)		
Bearer Capability							
Broadband Bearer Class	C	X	C	X	C	X	VP
ATM Transfer Capability (note 1)	ab-sent	Absent, 0, 2, 8 or 10	Absent	Absent, 0, 2, 8 or 10	Absent	Absen t, 0, 2, 8 or 10	Absen t, 10
Traffic Descriptor for a given direction							
PCR (CLP=0)	S						
PCR (CLP=0+1)	S		S		S		
SCR, MBS (CLP=0)							
SCR, MBS (CLP=0+1)					S		
Best Effort							
Tagging	Y/N		N		N		
Frame Discard	Y/N		Y/N		Y/N		
QoS Classes	*		*		*		
transit delay (note 2)	(note 3)		(note 3)		(note 3)		
peak-to-peak CDV							
CLR (CLP=0) (Note 11)	O		O		O		
CLR (CLP=0+1) (Note 11)							

ATM Service Category	**ABR (continues)**			**UBR (continues)**					
Conformance	ABR			UBR.1			UBR.2		
Bearer Capability									
Broadband Bearer Class	C	X	VP	C	X	VP	C	X	VP

Table D-4. Allowable Combinations of Traffic and QoS Related Parameters in the SETUP Message (ATM UNI 4.0 and PNNI 1.0) (Continued)

<table>
<tr><th>ATM Service Category</th><th>ABR (continued)</th><th colspan="6">UBR (continued)</th></tr>
<tr><td>ATM Transfer Capability</td><td>12</td><td>Absent</td><td>Absent, 0, 2, 8 or 10</td><td>Absent, 10</td><td>Absent</td><td>Absent, 0, 2, 8 or 10</td><td>Absent, 10</td></tr>
<tr><td>Traffic Descriptor for a given direction</td><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>PCR (CLP=0)</td><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>PCR (CLP=0+1)</td><td>S</td><td colspan="3">S</td><td colspan="3">S</td></tr>
<tr><td>SCR, MBS (CLP=0)</td><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>SCR, MBS (CLP=0+1)</td><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>ABR MCR</td><td>(note 6)</td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>Best Effort</td><td></td><td colspan="3">S (note 9)</td><td colspan="3">S (note 9)</td></tr>
<tr><td>Tagging</td><td>N</td><td colspan="3">N</td><td colspan="3">Y</td></tr>
<tr><td>Frame Discard</td><td>Y/N</td><td colspan="3">Y/N</td><td colspan="3">Y/N</td></tr>
<tr><td>QoS Classes</td><td>0</td><td colspan="3">0</td><td colspan="3">0</td></tr>
<tr><td>transit delay (note 2)</td><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>peak-to-peak CDV</td><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>CLR (CLP=0) (Note 11)</td><td></td><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>CLR (CLP=0+1) (Note 11)</td><td></td><td colspan="3"></td><td colspan="3"></td></tr>
</table>

Table D-4. Allowable Combinations of Traffic and QoS Related Parameters in the SETUP Message (ATM UNI 4.0 and PNNI 1.0) (Continued)

Table Notes: *Note 1* – Values 0, 1, 2, 4, 6, and 8 are not used on transmission but shall be understood on reception. *Note 2* – Maximum end-to-end transit delay objectives may only be specified for the forward direction. *Note 3* – Maximum end-to-end transit delay objectives may be specified for the ATM Service Category of Non-Real Time VBR for reasons of backward compatibility with ITU-T Recommendations. *Note 4* – Included for reasons of backward compatibility with UNI 3.1 and ITU-T Recommendations. With these conformance definitions, the CLR commitment is only for the CLP=0 traffic stream. *Note 5* – Included to allow switched virtual paths to use the UNI 3.1 conformance definitions. *Note 6* – Optional in the user-to-network direction. Specified in the network-to-user direction. *Note 7* – This combination should be treated as if the received PCR (CLP=0) parameter were a SCR (CLP=0) parameter and a MBS (CLP=0) parameter with a value of 1. *Note 8* – This combination should be treated as if an additional SCR (CLP=0) were received with the same value as the received PCR (CLP=0+1) parameter with a MBS (CLP=0) parameter with a value of 1. *Note 9* – The Best Effort indication applies to both the forward and backward directions. *Note 10* – This combination should only be used when the CLR commitment on CLP=0+1 traffic is required versus CLR commitment on CLP=0 traffic, since these combinations are not supported by UNI 3.0/3.1 nor ITU-T Q.2931. *Note 11* – In this table, the CLR parameter is shown as two entries to indicate explicitly whether the CLR commitment is for the CLP=0 or for the CLP=0+1 cells.
Table Abbreviations: PCR = Peak Cell Rate; SCR = Sustainable Cell Rate; MBS = Maximum Burst Size; Y = Yes; N = No; Y/N = Either “Yes” or “No” is allowed; S = Specified; (Blank) = Unspecified; * = Allowed QoS class values are a network option. Class 0 is always supported for alignment with ITU-T; O = Optional. May be specified using: - An individual QoS parameter encoded in the Extended QoS parameters information element or the end-to-end transit delay information element or, - Objectives implied from the QoS class If an extended QoS parameters information element is present and this parameter is not present in the message, then any value of this parameter is acceptable. If neither the parameter nor the Extended QoS parameters information element is present in the message, then the objective for this parameter is determined from the QoS class in the QoS parameter information element.

E

Using SVC Failure Information

This appendix describes how to use SVC failure location information displayed in the failure location and failure cause fields on the Show Failed Call Attributes dialog box for failed ATM SVCs (see "Viewing ATM SVC Failed-Call Attributes" on page 13-79) and failed Frame Relay SVCs (see "Viewing Frame Relay SVC Failed Calls" on page 14-45).

About SVC Cause Codes

For failed ATM SVCs, the Show Failed Call Attributes dialog box displays the reason for the SVC failure using the ATM Forum UNI 3.0/3.1/4.0 standard cause codes, and the location where the failure occurred.

For failed Frame Relay SVCs, the Show Failed Call Attributes dialog box displays the reason for the SVC failure using the Frame Relay Forum FRF.4 standard cause codes, and the location where the failure occurred.

Table E-1 describes the failure cause codes and the standards documents that you should reference for further information. Keep in mind that the ATM Forum UNI and Frame Relay Forum FRF.4 standards use many (but not all) of the same cause codes. The ATM UNI and Frame Relay Forum FRF.4 standards documents reference ITU standards documents for many of the cause codes.

Table E-1. SVC Setup Failure Causes

Cause	Description	See
unalloc-nmb (1)	Unallocated (unassigned) number. The called party number is not currently assigned. As a result, the called party cannot be reached.	ITU Q.850
no-route-transnet (2)	No route to transit network. The equipment sending this cause received a request to route the call through an unknown transit network. The transit network is unknown to the equipment because it does not exist or does not serve the equipment.	ITU Q.850
no-route-dest (3)	No route to destination. The network through which the call was routed does not serve the destination. As a result, the called party cannot be reached.	ITU Q.850
vcc-unacceptable-30 (10)	VPI/VCI is unacceptable to the sending entity for use in the call.	ATM Forum UNI 3.0/3.1
normal-call-clr-31 (16)	Normal call clearing.	ITU Q.850
user-busy (17)	User is busy. The called party is unable to accept another call because the user busy condition has been encountered.	ITU Q.850
no-user-response (18)	No user response. A called party did not respond to a call establishment message with either an alerting or connect indication within a designated time period.	ITU Q.850
call-reject (21)	Call has been rejected. Although the equipment sending this cause is neither busy nor incompatible, the equipment sending this cause does not want to accept the call. The cause can be generated by the network to indicate that the call may have been cleared as a result of a supplementary service constraint.	ITU Q.850
nmb-changed (22)	Number has changed. The number of the called party is no longer assigned. A new number must be used to call the called party.	ITU Q.850
call-reject-clir (23)	User rejects all calls with CLIR (calling line identification restriction). The called party returns this cause code when the call comes in without calling party number information and the called party requires this information.	ATM Forum UNI 3.0/3.1
dest-out-of-order (27)	Destination is out of order. The user cannot reach it because the interface to the destination is not functioning properly (that is, a signalling message could not be delivered to the destination).	ITU Q.850
invalid-nmb-format (28)	Invalid number format. The called party is unreachable because the number of the called party is not in the proper format or it is incomplete.	ITU Q.850

Table E-1. SVC Setup Failure Causes (Continued)

Cause	Description	See
response-stat-enq (30)	Response to STATUS ENQUIRY. A STATUS message was sent in response to receipt of a STATUS ENQUIRY message.	ITU Q.850
normal-unspecified (31)	Normal unspecified. A normal event occurred for which no other cause applies. As a result, the event is normal, but unspecified.	ITU Q.850
pending-add-party (32)	Too many pending ADD PARTY requests.	ATM Forum PNNI 1.0
req-vcc-unavailable (35)	Requested VPCI/VCI is unavailable. The ATM SVC attempted to use a VPCI/VCI that is unavailable.	ITU Q.2610
vcc-fail-31 (36)	VPCI/VCI assignment failure. A VPCI/VCI could not be assigned to the ATM SVC.	ITU Q.2610
rate-unavail-31 (37)	User cell rate is unavailable. The requested cell rate is unavailable for the ATM SVC.	ITU Q.2610
network-out-of-order (38)	Network is out of order. The problem will probably last a long period of time (that is, an immediate retry of the call is not likely to succeed).	ITU Q.850
temp-fail (41)	Temporary failure. The problem will probably last a short period of time (that is, an immediate retry of the call has a good chance to succeed).	ITU Q.850
access-info-discard (43)	Access information has been discarded. The network failed to deliver access information (e.g., user-to-user, low-layer compatibility, high-layer compatibility, or sub-address) to the remote user.	ITU Q.850
circuit-unavailable (44)	Requested circuit/channel is not available.	ITU Q.850
no-vcc-available (45)	No VPCI/VCI is available. A VPCI/VCI is not available for the ATM SVC.	ITU Q.2610
resources-unavailable (47)	Resources are unavailable/unspecified. A resource is unavailable, and no other cause exists to report this event.	ITU Q.850
qos-unavailable (49)	Quality of Service is unavailable. The requested QoS class is unavailable for the SVC.	ITU Q.850
rate-unavailable-30 (51)	User cell rate is unavailable. The requested cell rate is unavailable for the ATM SVC.	ATM Forum UNI 3.0/3.1
PGL-change (53)	Call cleared due to change in PGL (Peer Group Leader).	ATM Forum PNNI 1.0
b-cap-not-authorized (57)	Bearer capability is not authorized. The SVC user requested a bearer capability for which the user is not authorized.	ITU Q.850

Table E-1. SVC Setup Failure Causes (Continued)

Cause	Description	See
b-cap-unavailable (58)	Bearer capability is not available. The SVC user requested a bearer capability that is not available at this time.	ITU Q.850
service-unavailable (63)	Service or option is unavailable. A service or option is unavailable, and no other cause code exists to report this event.	ITU Q.850
b-cap-not-implemented (65)	Bearer capability is not implemented. The equipment that generates this cause does not support the requested bearer capability.	ITU Q.850
combination-unsupported (73)	Unsupported combination of traffic parameters.	ATM Forum UNI 3.0/3.1
aal-params-unsupp-31 (78)	ATM Adaptation Layer (AAL) parameters cannot be supported.	ITU Q.2610
invalid-call-reference (81)	Invalid call reference. The equipment that sends this cause has received a message with a call reference that is not currently in use on the user-network interface.	ITU Q.850
no-channel (82)	Identified channel does not exist. The equipment sending this cause received a request to use a channel that was not activated on the call interface. For example, if a user subscribed to those channels on a primary rate interface numbered from 1 to 12, this cause would be generated if the user equipment or the network attempts to use channels 13 through 23.	ITU Q.850
dest-incompatible (88)	Incompatible destination. The equipment sending this cause received a request to establish a call with low-layer compatibility, high-layer compatibility, or other compatibility attributes (e.g., data rate) which cannot be accommodated.	ITU Q.850
invalid-endpoint-ref (89)	Invalid endpoint reference. The equipment sending this cause received a message with an endpoint reference that is currently not in use on the user-network interface.	ATM Forum UNI 3.0/3.1
invalid-transit-net (91)	Invalid transit network selection. A transit network identification was received that is formatted incorrectly. Correct formats are defined by Annex C in the Q.931 standard.	ITU Q.850
too-many-add-pty-req (92)	Too many ADD PTY requests were generated on the SVC. This condition occurs when the calling party sends an ADD PTY request, but the network cannot accept another ADD PTY message because its queues are full. This is a temporary condition.	ATM Forum UNI 3.0/3.1
aal-params-unsupp-30 (93)	AAL parameters cannot be supported.	ITU Q.2610
invalid-message (95)	Invalid message, unspecified. This cause reports an invalid message event when no other invalid message cause applies.	ITU Q.850

Table E-1. SVC Setup Failure Causes (Continued)

Cause	Description	See
info-element-missing (96)	Mandatory information element is missing. The equipment sending the cause received a message that is missing a mandatory information element.	ITU Q.850
msg-type-not-imp (97)	Message type is not implemented. The equipment sending the cause received a message of one of the following message types: • Not defined • Defined but not implemented by the equipment sending the cause	ITU Q.850
info-element-not-imp (99)	Information element is not implemented. The equipment sending the cause received a message that includes information elements or parameters that meet one of the following criteria: • Not recognized because they are not defined • Defined but not implemented by the equipment sending the cause The cause indicates that the elements or parameters were discarded. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.	ITU Q.850
invalid-info-element (100)	Invalid information element. The equipment sending this cause received an information element that it has implemented, but one or more fields in the information element are coded in a way that has not been implemented.	ITU Q.850
message-not-compatible (101)	Message type is not compatible with call. A message was received that is incompatible with the call state.	ITU Q.850
timer-recovery (102)	Recovery on timer expiration. A procedure has been initiated by the expiration of a timer that is related to error handling procedures.	ITU Q.850
invalid-message-len (104)	Incorrect message length.	ATM Forum UNI 3.0/3.1
protocol-error (111)	Unspecified protocol error. A protocol error occurred for which there is no defined protocol error.	ITU Q.850
optional-element-error (127)	Optional information element content error (non-standard). This cause indicates the occurence of internetworking with a network that does not provide causes for actions it takes. The precise cause for any message that is sent cannot be ascertained.	ITU Q.850
no-route-next-node (128)	Next node unreachable.	ATM Forum PNNI 1.0

Table E-1. SVC Setup Failure Causes (Continued)

Cause	Description	See
dtl-not-my-node (160)	DTL Transit not my node ID.	ATM Forum PNNI 1.0

Example

This section describes how cause codes are used. The following example uses ATM SVCs that connect CBX 500 switches and campus networks.

Using the sample network shown in Figure E-1, the CBX 500 switches are deployed in a UNI signalling environment where Links A-D are running UNI signalling. The majority of UNI signalling activity involves users (workstation and routers) at Campus ATM Network #1 using SVCs to establish ATM connectivity with users at Campus ATM Network #2. If one of these SVC attempts fail, the CBX 500 records the event.

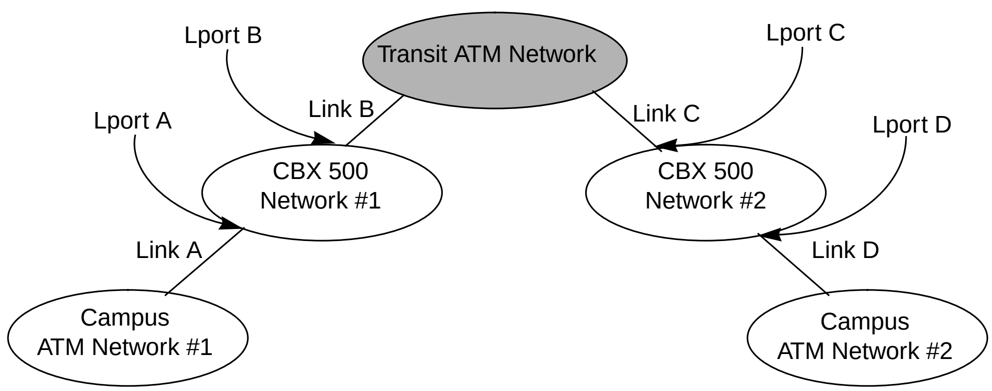


Figure E-1. Transit ATM Network

Table E-2 describes the failure conditions that may occur and displays the failed SVC information (see Figure 13-34 on page 13-77). The information in Table E-2 uses the sample network shown in Figure E-1 as an example. All SVC attempts described in this table are from Campus Network 1 to Campus Network 2.

The following abbreviations are used in the table:

- Loc = the switch/lport reported in the SVC Failure Location fields.
- No entry = no SVC failure reported at this lport.
- Rel = whether the RELEASE was received (rx) on the logical port or transmitted (tx) by the logical port.

Table E-2. SVC Failure Location information for Sample Transit Network

Failure Type	Failure location entry at				Notes
	LPort A	LPort B	LPort C	LPort D	
Link A down	No entry	No entry	No entry	No entry	Link A is down – call never reaches CBX 500 #1.
Link B down	Loc=A Rel=tx	No entry	No entry	No entry	Link B is down – routing never sends attempt to B. Failure is only reported at A.
Link C down	Loc=B Rel=tx	Loc=B Rel=rx	No entry	No entry	Link C is down – SVC attempts sent to transit network but release is returned from transit network.
Link D down	Loc=B Rel=tx	Loc=B Rel=rx	Loc=C Rel=tx	No entry	Link D is down – SVC attempt is sent to transit network but release is returned from CBX 500 #2 and passed back to CBX 500 #1 via transit network.
Called party user down at Campus 2	Loc=B Rel=tx	Loc=B Rel=rx	Loc=D Rel=tx	Loc=D Rel=rx	Release is received from Campus 2 and forwarded back to CBX 500 #2, transit, CBX 500 #1.

The public/private network indication is extracted from the release message that is either transmitted by the CBX 500 or received by the CBX 500. You should take the following into consideration when you use the SVC failure location information:

- If the release message is transmitted by the CBX 500, the CBX 500 inserts “public” or “private” based on the lport setting (for DCE lports).
- If the release message is received by the CBX 500, the information inserted by the other switch is used in the SVC failure location field.

In general, different switches exhibit different behavior in this area. For this reason it is difficult to use public/private as a true indication of where the failure occurs.

The configuration shown in Figure E-1 on page E-6 uses a transit network between two CBX 500 networks. In this configuration, troubleshooting is more difficult. The SVC failure location information shown in Figure E-2 is more useful because SVC information can be shared between the two networks (over the direct or OPTimum trunks). This is not the case when a UNI interface exists between the two networks.

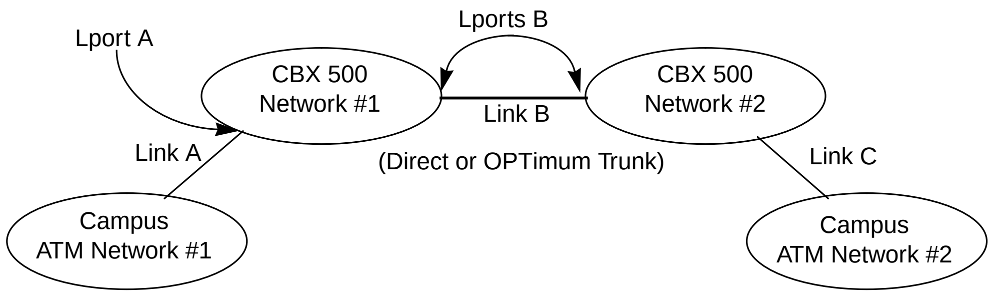


Figure E-2. Two CBX 500 Networks (Direct or OPTimum Trunk)

Table E-3 describes the failure conditions that may occur (using the example in Figure E-2) and displays the Show All Failed SVC log information. All SVC attempts described in this table are from Campus Network 1 to Campus Network 2.

Table E-3. SVC Failure Location Information for all CBX 500 Scenarios

Failure Type	Failure location entry at			Notes
	LPort A	LPort B	LPort C	
Link A down	No entry	Failure info only provided on UNI ports (not trunk ports)	No entry	Link A is down – call never reaches CBX 500 #1.
Link B down	Loc=A Rel=tx	Failure info only provided on UNI ports (not trunk ports)	No entry	Link B is down – routing never sends attempt to B. Failure is only reported at A.
Link C down	Loc=B Rel=tx	Failure info only provided on UNI ports (not trunk ports)	No entry	Link C is down – routing never sends attempt to B, so failure is only reported at A.
Called party user down at Campus 2	Loc=B Rel=tx	Failure info only provided on UNI ports (not trunk ports)	Loc=D Rel=tx	Release is received from Campus 2 and forwarded back to CBX #2 and CBX #1.

F

Accessing Control Files

In order to troubleshoot some serious file-related problems (such as file corruption) on the active disk, you can access files from the switch console on B-STDX CP, CBX 500 SP, and GX 550 NP hard disks. You can access the active disk only; you cannot access the standby disk.

> ⚠ Consult the Ascend Core Switching Technical Assistance Center before you access files on B-STDX CP, CBX 500 SP, and GX 550 NP hard disks.

You can connect to the switch console using standard terminal emulation programs such as Telnet. Once you access the console, you can perform the following actions:

- Issue the DIR command to obtain a directory and file listing. This command is similar to the DOS DIR command.
- Issue the SCANDISK command to analyze the disk's file system for problems such as data corruption. This command is similar to the SCANDISK command that can be run under DOS or Windows 95.
- Download software images and PRAM files using kermit.
- Remove PRAM files with the RESET PRAM command.

To perform these tasks:

1. Access the switch console. See the *NavisCore NMS Getting Started Guide* for descriptions of the various ways you can access the switch console.

   If the NMS is connected to the switch, select the appropriate switch object on the network map. Then, from the Misc menu, select Terminal Connect ⇒ Telnet.

2. At the login prompt, enter "debug."

3. At the password prompt, enter your debug password. If you do not know this password, contact the Ascend Core Switching Technical Assistance Center.

You may now issue the DIR, SCANDISK and RESET PRAM commands. You may also download software images and PRAM files using kermit. See the *NavisCore NMS Getting Started Guide* for more information on RESET PRAM, and for more information on downloading software images and PRAM files.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V