Diagnostic and Troubleshooting Guide for B-STDX

Ascend Communications, Inc.

Product Code: 80018
Revision 01
March 1997

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

11 Resolving Problems

A Console Commands

B DS3 and DS1 Statistics

C Using Copy Database

Index

About This Guide

The *Diagnostic and Troubleshooting Guide for B-STDX/STDX* provides you with a comprehensive set of instructions about how to monitor and troubleshoot activity and events on a Cascade switch network. Specifically, this guide describes how to perform CascadeView/UX, Release 2.3 tasks that are supported in Cascade switch software, Release 4.2. For information on using HP OpenView functions, refer to the appropriate HP documentation.

What You Need to Know

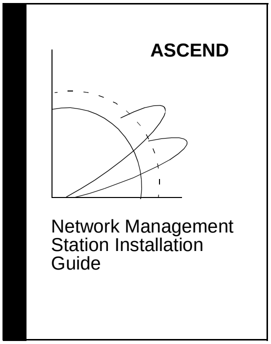
As a reader of this guide, you should be familiar with basic UNIX operating system commands and know how to use a mouse. You should possess a working knowledge of relational database software to properly maintain SYBASE, which is the database used by CascadeView/UX.

This guide assumes that you have installed the Cascade switch hardware. Refer to the appropriate hardware installation guide for more information:

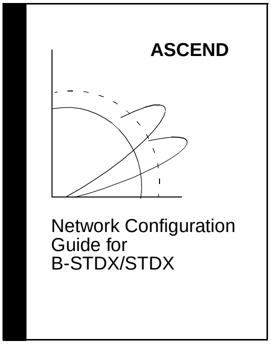
- *STDX 6000 Hardware Installation Guide*
- *B-STDX 8000/9000 Hardware Installation Guide*

Documentation Reading Path

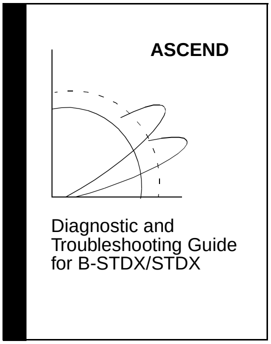
The following manuals provide the complete document set for the NMS Release 2.3:



This guide describes prerequisite tasks, hardware and software requirements, and Solaris, HPOV, and CascadeView/UX installation on the NMS.



After setting up your NMS and installing CascadeView/UX, use this guide to define your network, configure switches, and download your configuration from the NMS to the switch.



After configuring your network, use this guide to monitor and troubleshoot your network.

Customer Comments

Customer comments are welcome! Please fill out the Customer Comment Form located at the back of this guide and return it to us.

How to Use This Guide

This guide is intended for those users **who are using Release 2.3 of the CascadeView/UX NMS** to monitor the status of a Cascade 8000/9000 or 6000 switch and its components.

Before you read this guide, read the Software Release Notice (SRN) that accompanies the software.

Table 1. Description of Guide Contents

Read	To Learn About
Monitoring	
Chapter 1	Monitoring Cascade objects on your network.
Chapter 2	Monitoring trunks, circuits, and routes in your network.
Chapter 3	Generating diagnostic, statistical and reporting information for Cascade switches on the network.
Chapter 4	Generating and monitoring DS1, DS3, DS0, and PVC loopbacks.
Generating Statistics	
Chapter 5	Provides an overview about generating statistical information, setting the polling interval, and creating reports for Cascade switches on the network.
Chapter 6	Generating logical and physical port statistics for a Cascade switch.
Chapter 7	Generating statistics for a channelized DS3 module.
Chapter 8	Generating trunk and circuit summary statistics.

Read	To Learn About
Using the MIB Browser and the Events Browser	
Chapter 9	Monitoring Management Information Base (MIB) values in the Cascade MIB.
Chapter 10	Interpreting trap alarm conditions for Cascade switches.
Resolving Common Problems	
Chapter 11	Troubleshooting techniques for resolving potential problems, common problems and their solutions, and information about contacting the Cascade Technical Response Center.
Installation	
Chapter 12	Reinstalling the operating system software and clearing Parameter Random Access Memory (PRAM) from the switch.
Appendices	
Appendix A	Console commands that you can enter to perform various tasks on the switch, or to obtain information from the switch.
Appendix B	DS3 and DS1 statistics for the channelized DS3 module.
Appendix C	Using the Copy Database utility.

Conventions

This guide uses the following conventions to emphasize certain information, such as user input, screen prompts and output, and menu selections. For example:

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.	CascadeView ⇒ Logon
Blue border surrounding text	Notes and warnings.	See examples below.
Italics	Book titles, new terms, and emphasized text.	*CascadeView/UX Network Management Station Installation Guide*

Provides helpful suggestions or reference to materials not contained in this manual.

Warns the reader to proceed carefully in order to avoid equipment damage or personal harm.

Related Documentation

This section lists the related Cascade and third-party documentation that may be useful to reference.

Cascade

- *STDX 6000 Hardware Installation Guide (80006)*
- *B-STDX 8000/9000 Hardware Installation Guide (80005)*
- *CBX 500 Hardware Installation Guide (80011)*
- *Networking Services Technology Overview (80001)*
- *Network Management Station Installation Guide (80014)*
- *Network Configuration Guide for B-STDX/STDX (80017)*
- *Configuring ISDN Services for B-STDX/STDX (80039)*
- *CBX 500 Network Administrator's Guide (80012)*
- *Cascade Enterprise MIB Definitions (80015)*
- *SYBASE 11 SQL Server Upgrade Guide (80040)*
- *Upgrading to Solaris 2.5.1 and HP OpenView 4.11 (80045)*
- *Bulk Statistics Collector for B-STDX/STDX (80032)*

Third Party

- *Solaris 2.4 System Configuration and Installation Guide*
- *HP OpenView Windows User's Guide* (for HP 9000 Series and Sun SPARCstation)
- *SYBASE Commands Reference Manual*
- *SYBASE System Administration Guide*

What's New in This Guide

This section lists the product features in this 2.3 release of the NMS, as well as the enhancements and changes made to this guide.

Table 2. Release 2.3 New Features/Functions

New Features	Enables You to...	Described in...
Channelized DS3 Statistics	Generate statistics for the channelized DS3 module.	Chapter 7 Appendix B
ATM IWU (Interworking Unit) I/O module	Perform 155 Mbps cell switching with FR-ATM Interworking. Statistics screens enable you to monitor Physical and Logical Port Statistics for the ATM IWU module.	Chapter 6
Monitoring Logical Port Attributes	Monitor the logical port attributes, such as Administrative, Congestion Control, and Trap Control for each I/O module's logical port.	Chapter 1
Monitoring Subnets, Clusters, VPNs, Management VPI/VCIs.	Monitor a subnet, cluster, Virtual Private Network (VPN), and customers in a VPN. In addition, the monitoring VPI/VCI function enables you to monitor the status of all ATM interworking connections.	Chapter 2 Appendix B
VPN/Customer View	Monitor the trunks, logical ports, and PVCs for a selected customer or VPN.	Chapter 2
Limit the use of the CascadeView/UX NMS to the Monitor functions	Provide a user with the ability to monitor network resources without the ability to provision.	Chapter 2
Loopbacks on the channelized DS3 module	Performing DS1 loopback tests and DS1 BERT testing.	Chapter 4

Table 2. Release 2.3 New Features/Functions

New Features	Enables You to...	Described in...
RIP console commands	Display information about the routing information protocol (RIP) attributes and statistics.	Appendix A
New SMDS Console commands	Display SMDS information by using a variety of different show smds commands.	Appendix A
Copy Database Utility	Copy data in to or out of a CascadeView/UX database. The utility does not require you to know which schema you should use for the new database.	Appendix C
Single OSPF Domain	Monitor B-STDX switches and CBX-500 switches using one NMS.	Throughout the manual

Table 3. Enhancements to this Guide

Changes/Enhancements to This Guide	Described in...
HP OpenView SNMP Management Platform, Version 4.11 menu options. In HP OpenView, 4.11, CascadeView/UX menu options appear on different menus than in HP OpenView, 3.3.1. This guide references the location of the menu options for HP OpenView, Version 4.11.	Chapter 1 Chapter 2 Chapter 9
Descriptions now included for accessing the MIB Browser to view the Cascade MIB.	Chapter 9
Backup Procedures are now included in the *Network Management Station Installation Guide.*	

Table 3. Enhancements to this Guide

Changes/Enhancements to This Guide	Described in...
Changes due to all Tech Tip corrections have been included to update and correct descriptions throughout the book as necessary.	Throughout the manual

1

Monitoring Switch Objects

This chapter explains how to retrieve status information about the various objects that make up an Ascend network. Table 1-1 on page 1-2 lists the section of the book that describes each of the Monitor functions.

You do not need to log on to monitor switch objects.

Table 1-1. Monitor Functions and Associated Descriptions

To Monitor	Refer to...
Object Descriptions	"Reviewing an Object Description" on page 1-3
Switch Details	"Displaying a Submap Description" on page 1-8
Standby 3000/6000 Status	"Reviewing Standby STDX 3000/6000 Status" on page 1-17
Physical Port Attributes	"Reviewing the Status of Physical Ports" on page 1-19
Logical Port Attributes	"Reviewing the Status of Logical Ports" on page 1-28
Subnets	"Reviewing the List of Subnets" on page 1-49
Clusters	"Reviewing the List of Clusters" on page 1-50
Switch Status	"Reviewing the Status of Switches" on page 1-51
Trunk Status	"Reviewing the Status of Trunks" on page 2-2
Circuit Status	"Reviewing the Status of Circuits" on page 2-10
Multicast DLCIs	"Reviewing the Status of Multicast DLCIs" on page 2-24
Management DLCIs	"Reviewing the Status of Management DLCIs" on page 2-26
Management VPI/VCIs	"Reviewing the Status of Management VPI/VCIs" on page 2-28
SMDS Management Addresses	"Reviewing the Status of SMDS Management Addresses" on page 2-31
Customer/VPN	"Reviewing Customer/VPN Parameters" on page 2-33
SMDS Routes	"Reviewing the Status of SMDS Routes" on page 2-40

Reviewing 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
- Submap description for a selected object
- Map description for a selected object

Displaying an Object Description

To display an object description for a selected object icon, complete the following steps:

1. On the network map, select the object icon. The selected object is highlighted.
2. From the Edit menu, select Describe/Modify Object. The Object Description dialog box appears.

> *This dialog box enables you to access a variety of object attribute settings. Refer to the* HP OpenView User's Guide f*or information about modifying Object Capabilities and General Attributes.*

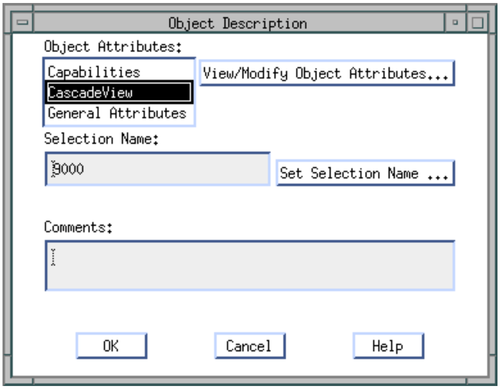


Figure 1-1. Object Description Dialog Box

3. In the Object Attributes field, select CascadeView and choose View/Modify Object Attributes. The Attributes for Object dialog box appears.

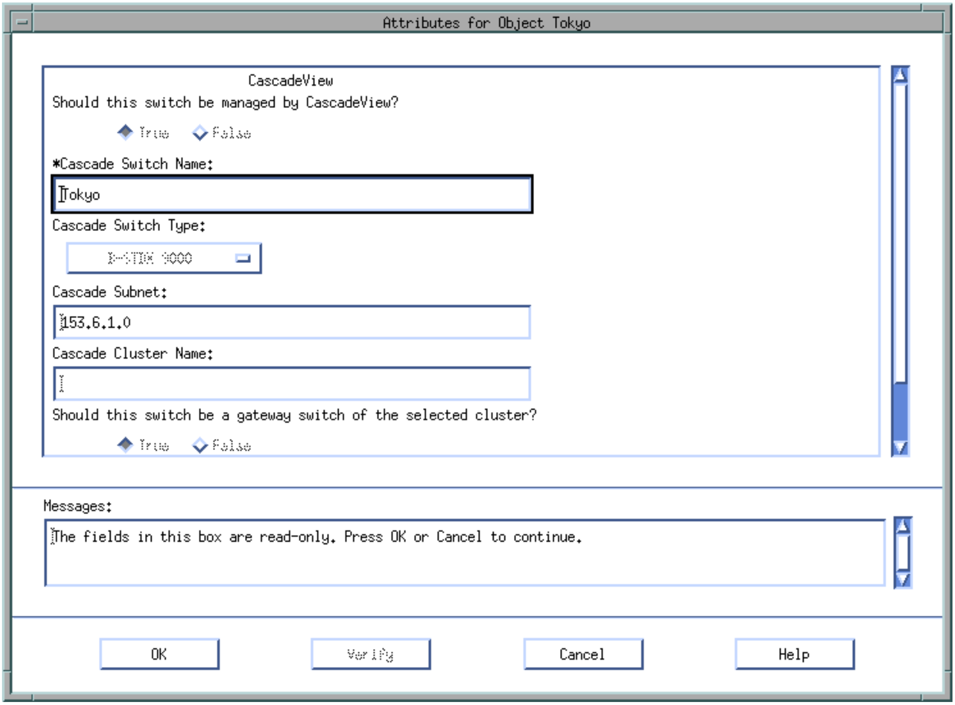


Figure 1-2. Attributes for Object Dialog Box

Table 1-2 describes each of the dialog box fields.

Table 1-2. Attributes for Object Fields

Field	Action/Description
Should this switch be managed by CascadeView?	Set this field to *True* to enable CascadeView to manage it.
Cascade Switch Name	Displays the switch name.
Cascade Switch Type	Displays the switch type (STDX 3000, STDX 6000, B-STDX 8000, or B-STDX 9000).
Cascade 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. Refer to the *Network Configuration Guide for B-STDX/STDX* for further details.
Cascade Cluster Name	Displays the name of the cluster to which this subnet belongs.
Should this switch be a gateway switch of the selected cluster?	Displays True or False to indicate whether or not the switch is a gateway switch for the cluster.
Messages	Provides additional information about the fields in the Object for Attributes dialog box.

Displaying a Map Description

To display a map description for a selected object icon, complete the following steps:

1. On the network map, select the object icon. The selected object appears highlighted.
2. From the Map menu, select Maps ⇒ Describe/Modify. The Map Description dialog box appears.

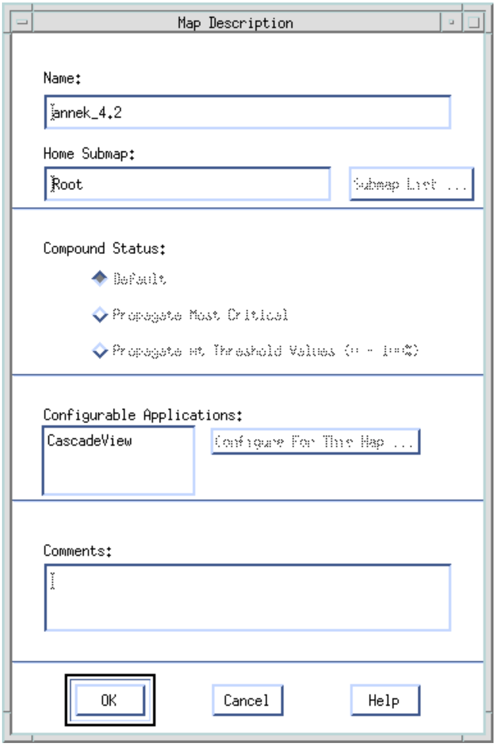


Figure 1-3. Map Description Dialog Box

Table 1-3 on page 1-7 describes each of the dialog box fields.

Table 1-3. Map Description Fields

Field	Action/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.
Compound Status	Select the desired status propagation: *Default* – Causes HP 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%)* – Displays four fields that enable you to set threshold values that determine when HP OpenView propagates status. The number shown for each field is its default value. – %warning 30 – %minor 20 – %major 10 – %critical 5 Compound status is 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, refer to the *HP OpenView User's Guide*.
Configurable Applications	Select CascadeView and choose Configure for this map to display the map configuration.
Comments	Additional comments that further describe the map.

Displaying a Submap Description

To display a submap description for a selected object icon, complete the following steps:

1. On the network map, select the object icon. The selected object is highlighted.
2. From the Map menu, select Submap ⇒ Open/List. The Submaps in Map dialog box appears.

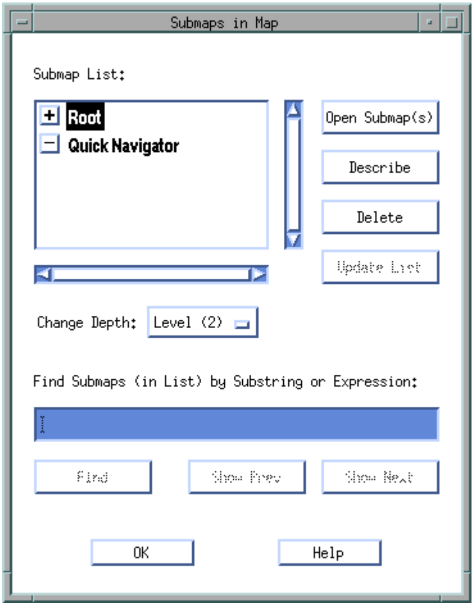


Figure 1-4. Submaps in Map Dialog Box

3. Select a submap from the Submap List and choose Describe. The Submap Description dialog box appears.

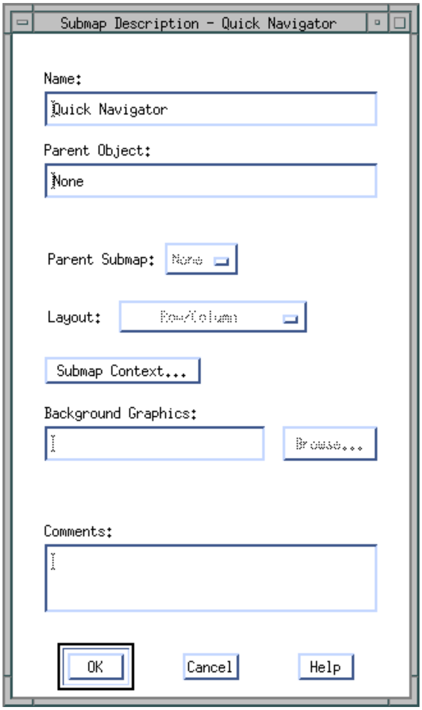


Figure 1-5. Submap Description Dialog Box

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

Table 1-4. Submap Description Fields

Field	Action/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 child submaps can be configured to be the home submap.
Layout	CascadeView/UX 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.

Reviewing the Details of a Switch

Use the Show Detail function to review the details of a switch.

The Show Detail function displays a graphical representation of the back panel configuration of a switch. The Show Detail function polls the switch and returns the appropriate operational status of the power supplies, fan modules, and I/O modules.

Procedure for Using the Show Detail Function

To display the details for a selected switch, complete the following steps:

1. On the network map, select the appropriate switch icon.

   The selected object is highlighted.

2. From the Monitor menu, select Cascade Objects ⇒ Show Detail.

   The Switch Back Panel dialog box displays. Figure 1-6 on page 1-12 illustrates the Switch Back Panel dialog box. Refer to “Switch Back Panel Status Light Indicators” on page 1-13 for a description of each of the indicators.

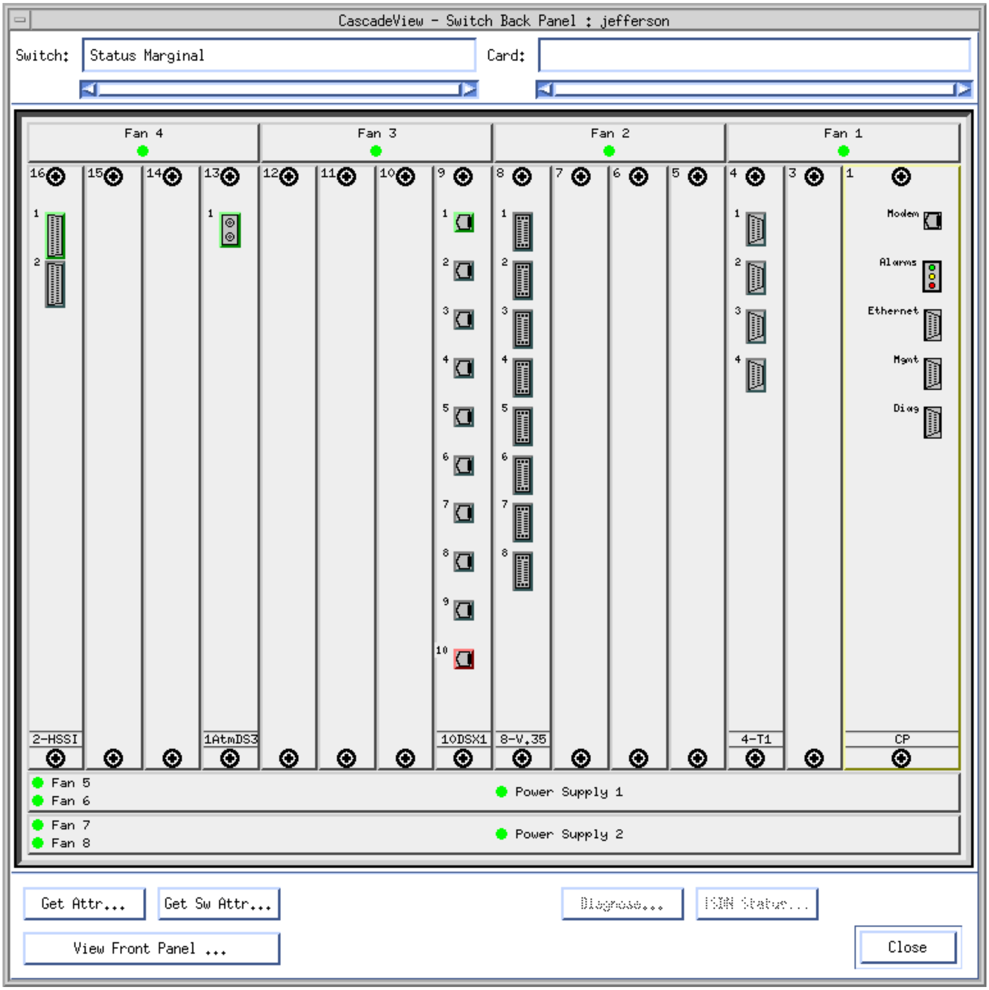


Figure 1-6. Switch Back Panel Dialog Box

Slots 1 and 2 are reserved for the main control processor (CP) module and the optional redundant CP. Slot 1 is usually configured with the main CP module.

3. The following list identifies each of the Switch Back Panel dialog box command buttons.

Choose	To
Get Attr	Display slot- or port-specific information for a selected slot or port (or switch if no slot or port is selected).
Get Sw Attr	Display summary information for a specific switch.
View Front Panel	Display a graphical representation of the B-STDX 8000/9000 front panel. Refer to “Viewing the Front Panel” on page 1-14 for more detailed information about this function.
Diagnose	Run foreground diagnostics or display background diagnostics for the selected switch’s I/O modules and ports. Refer to Chapter 3, “Running Diagnostics” for more information about background and foreground diagnostics.
ISDN Status	*(ISDN modules only)* Displays the status for an ISDN module. Refer to *Configuring ISDN Services for B-STDX* for further details about ISDN configuration options.
Close	Exit the dialog box and return to the network map.

Switch Back Panel Status Light Indicators

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

- Green LED indicates that the fan or power supply unit is operational.
- Red LED indicates that the fan or power supply unit is not operational.
- Blue LED on a fan or power supply unit indicates that the NMS cannot access the unit for status.

Switch Back Panel Port Colors

Physical ports change color to indicate their 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.
- 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 and/or an Operational Status of Down.

Switch Back Panel Card Colors

B-STDX 8000/9000 cards also change color to indicate their operational status. They use the following color scheme:

- A red B-STDX 8000/9000 card indicates that the card has failed or is not present.
- A yellow B-STDX 8000/9000 card indicates that the card may be in a marginal state or out of sync.
- A gray B-STDX 8000/9000 card indicates that it is operational.

Viewing the Front Panel

The Show Switch Front Panel dialog box displays a graphical representation of the front panel configuration of a switch.

Procedure for Displaying the Front Panel

Use the following step to display the front panel of a switch:

1. Choose View Front Panel from the Switch Back Panel dialog box (Figure 1-6).

   The Show Switch Front Panel dialog box displays as shown in Figure 1-7.

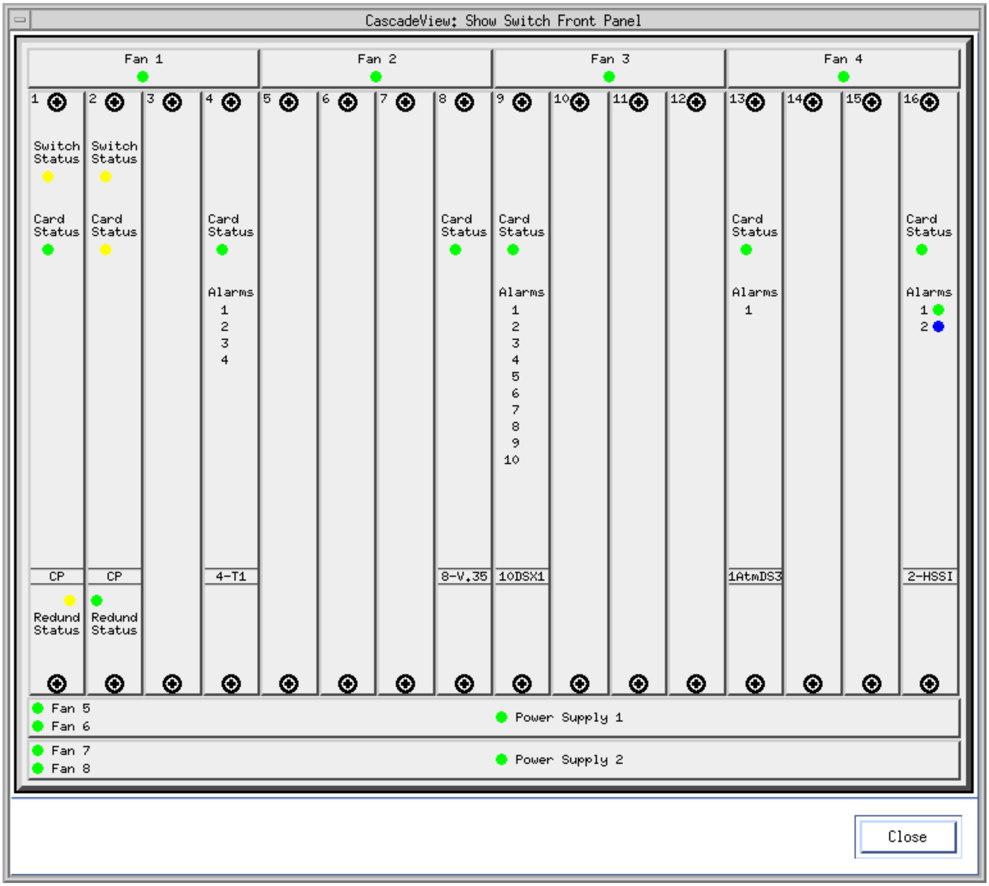


Figure 1-7. Show Switch Front Panel Dialog Box

Switch Front Panel Status Light Indicators

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

Switch and Card Status Light Indicators

- Green LED indicates the module is operational.
- Red LED indicates the module is not operational.
- Blue LEDs are used on the STDX 3000/6000 Packet Processor (PP), the B-STDX 8000/9000 Control Processor (CP), and on fan and power supply units. Blue indicates that the NMS cannot access the unit for status.

Alarm Status Light Indicators

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

- No LED indicates there are no alarm conditions on the 4-port T1/E1, 10-port DSX, HSSI, ATM DS3, or channelized DS3 cards.
- Red LED indicates a red alarm condition.
- Yellow LED indicates a yellow alarm condition.

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 is not applicable for B-STDX 8000/9000s which have redundant I/O modules rather than a redundant switch partner. To configure a redundant I/O module for the B-STDX 8000/9000, refer to the* Network Configuration Guide for B-STDX/STDX.

Procedure to Display the Status of a Standby Switch

To display the status of a standby switch:

1. On the network map, select the switch icon that contains the redundant partner.

2. From the Monitor menu, select Cascade Objects ⇒ Show Standby Switch. The Show Standby Switch dialog box appears.

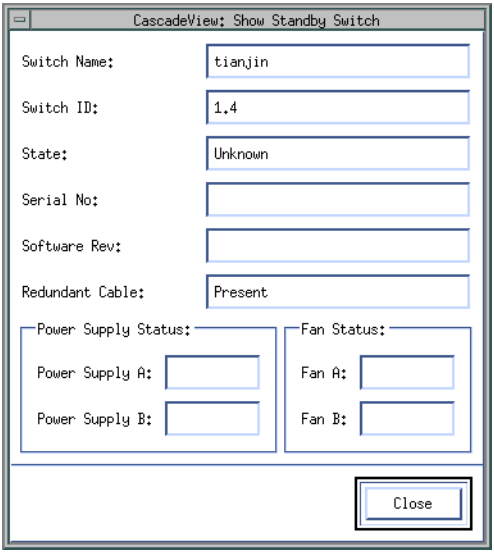


Figure 1-8. Show Standby Switch Dialog Box

3. When you finish reviewing the status information, choose Close. This causes the system to exit the dialog box and return to the network map.

Reviewing the Status of Physical Ports

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, complete the following steps:

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

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

   The system then displays a dialog box to enable you to view the attributes of the selected physical port. The title of the dialog box and the dialog box options differ depending on the type of physical port that you are monitoring. Figure 1-9 on page 1-19 illustrates an example of the type of dialog box that the system displays for an ATM UNI E3 physical port.

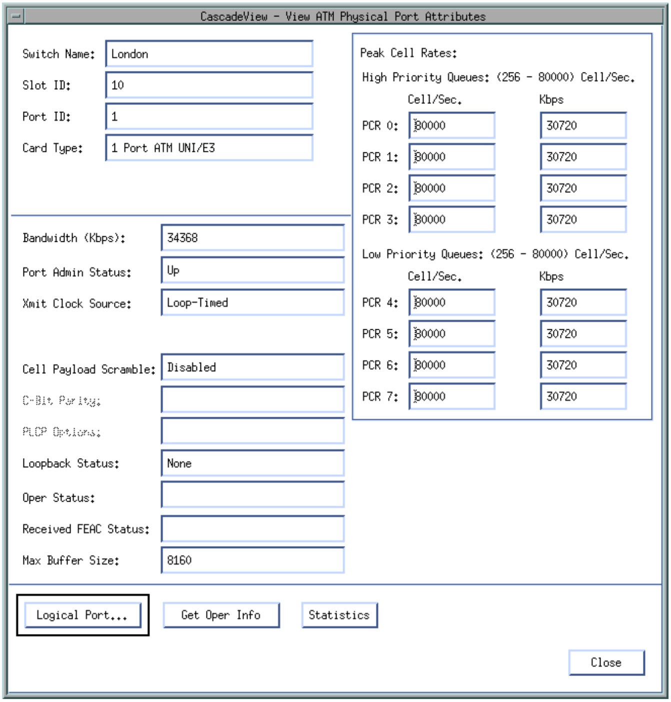


Figure 1-9. View Physical Port Attributes Dialog Box

The following command buttons on the View Physical Port Attributes dialog box enable you to obtain additional information about the physical port.

Choose	To
Logical Port	Display the Show All Logical Ports in PPort dialog box.
Get Oper Info	Display a status message in the Oper Status field that provides a brief status for the selected port.
Statistics	Display the summary statistics for the selected physical port.
DS3 Statistics	*(DS3 Only)* Display the DS3 Statistics dialog box to enable you to select one of the following types of statistics: configuration, current, interval, or total. All DS3 Statistics options display error and performance information (for a specified time period). Refer to "Channelized DS3 Summary Statistic Options" on page 7-1.
Chan Alarm Status	*(DS3 Only)* Display the alarm status for all 28 DS1 channels. Refer to "Displaying Channel Alarm Status" on page 7-5.
Diagnose	*(DS3 Only)* Display foreground diagnostic information for a selected channel.
Channel Attr	*(DS3 Only)* Display the channel attributes for a selected channel.
Close	Exit the dialog box and return to the network map.

Table 1-5 briefly describes the fields on the View Physical Port Attributes dialog box. The options that the system displays vary depending on the type of physical port you are viewing.

Table 1-5. View (or Show) Physical Port Attributes Fields

Field	Action/Description
Switch Name	The name entered to identify the switch at the time of configuration.
Slot ID	Indicates the back panel physical slot number where the I/O module that contains the selected logical port is installed.
Port ID	Displays the ID number of the selected physical port.
Port Type	Displays the type for the selected physical port.
Bandwidth	A read-only field that displays the amount of bandwidth available for this physical port.
Port Admin Status	A value of *Up* indicates that the port is activated. A value of *Down* indicates that the port has never been activated or that the port is off-line so that diagnostics can be run to test the port. A card with an Admin Status of *Down* is not operational.
Oper Status	Displays a brief status to indicate the operational status of the selected port.

Table 1-5. View (or Show) Physical Port Attributes Fields (Continued)

Field	Action/Description
Link Framing	*(T1 only)* Specifies 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.
Transmit Clock Source	Specifies the transmit clock source and can be any one of the following values: *Loop Time* – The clock source is derived from the timing received. (This value is called DTE on HSSI and UIO modules). *Internal* – The internal T1 timing generator provides the clock source. (This value is called DCE on HSSI and UIO modules). *External* – An external connection provides the clock source. The default is Loop Time.

Table 1-5. View (or Show) Physical Port Attributes Fields (Continued)

Field	Action/Description
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. Refer to the B-STDX 8000/9000 Hardware Installation Guide for cable diagram pinouts.
Clock Speed (Kbps)	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, CascadeView displays an error message.
Received FEAC Status	The Received Far End Alarm and Control (FEAC) Status enables you to monitor the performance of T3 circuits. The system displays a value in this field if the C-Bit Parity option is selected and a loopback test has been sent from a remote source.

Table 1-5. View (or Show) Physical Port Attributes Fields (Continued)

Field	Action/Description
Maximum Buffer Size (48 - 8142 bytes)	Specifies the maximum number of bytes in the reassembly buffer. The default is 8152. By selecting a smaller size, you provide more buffers to reassemble packets; 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.
Zero Encoding	*(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 8 bits is literally implemented by forcing a pulse in bit 8 of each channel. E1 selection is set at HDB3.
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.

Table 1-5. View (or Show) Physical Port Attributes Fields (Continued)

Field	Action/Description
Connection Type	*(T1 only)* The 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.
Line Build Out	(DS3 only) Specifies the length of the cable from the switch to the network equipment to which it is attached. The default value for this field is either 0 – 225 feet for a short cable or 226 – 450 feet for a long cable.
C-Bit Parity	(DS3 only). Provides a way to monitor the end-to-end performance of T3 circuits. M13 is the default value for this field. The DS3 signal is partitioned into M-frames of 4760 bits each. The M-frames are divided into seven M-subframes of 680 bits. The first C-bit in M-subframe 1 is used as an application identification channel (AIC) to identify the specific DS3 M-frame. This determines the mode of operation for a DS3 signal. Options include: *M13 (default)* – Uses C-bits in a frame to indicate the presence or absence of stuffing bits. C-bit Parity – Uses the first C-bit in M-subframe 1 to identify the format as C-bit parity. **Note:** *This feature requires C-bit parity-compatible customer premise equipment.*

Table 1-5. View (or Show) Physical Port Attributes Fields (Continued)

Field	Action/Description
PLCP Options	*(ATM UNI DS3 only)* Allows you to enable or disable the Physical Layer Convergence Protocol. When you *enable* PLCP, the ATM DS3 module uses a PLCP frame that transmits 12 ATM cells every 125 us. The ATM cell payload bandwidth is 36.9 Mbps. The enable option is used if the customer premise equipment can handle PLCP frames. When you *disable* PLCP, the DS3 module uses ATM direct mapping to pack ATM cells into the DS3 bit stream. The ATM cell payload bandwidth is 40 Mbps. The disable option is used if you can disable PLCP for the customer premise equipment that you connect to.
Loopback Status	*(DS3 only)* The default value for this field is *none*. If you enable diagnostic loopback tests, this field displays the DS3 card's loopback status. A loopback test enables you to test the physical path for data transmission by looping back traffic in one or both directions. For more information about loopbacks, refer to Chapter 4, "Loopbacks".
Cell Payload Scramble	(ATM only) This option enables or disables the Cell Payload Scramble function. The Cell Payload Scramble function prevents user data from being misinterpreted (ATM cell header deliniation). Enable is the default value for this field. However, the enable option is not used if the equipment that you connect to does not support Cell Payload Scramble.

Table 1-5. View (or Show) Physical Port Attributes Fields (Continued)

Field	Action/Description
Peak Cell Rates	*(ATM only)* Peak Cell Rate (PCR) 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, refer to the *Network Configuration Guide for B-STDX/STDX*.
Optical Transmitter	(ATM IWU only) A safety feature intended to prevent personal injury when you repair or replace the module, or connect cables to the module. By default, this option is set to Off. The Off setting disables the transmit laser 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.
BIP Error Threshold	*(ATM IWU only)* The Bit Interleaving Parity error threshold. Select one of the following options to indicate the physical port's sensitivity to network errors. • 10^-6 errors • 10^-5 errors • 10^-4 errors • ignore

Table 1-5. View (or Show) Physical Port Attributes Fields (Continued)

Field	Action/Description
Traffic Shaper Parameters	(ATM IWU only) Each shaper has associated default values for priority, SCR, PCR, and MBS. Refer to the *Network Configuration Guide for B-STDX/STDX* for further details about ATM IWU traffic shaper parameters.

Reviewing the Status of Logical Ports

Logical ports define the software attributes of the physical port. CascadeView/UX provides the following functions that enable you to review the attributes of a logical port:

- Show All Logical Ports in a Switch – displays the specifics of all logical ports defined for a selected switch.
- Show All Logical Ports in a Physical Port – displays the specifics of all logical ports defined for a physical port.

Reviewing All Logical Ports for a Switch

To display the logical ports for a selected switch, complete the following steps:

1. On the network map, select the appropriate switch icon.
2. From the Monitor menu, select Cascade Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears (Figure 1-10 on page 1-29). Table 1-6 through Table 1-13 describe all of the possible fields on this dialog box.

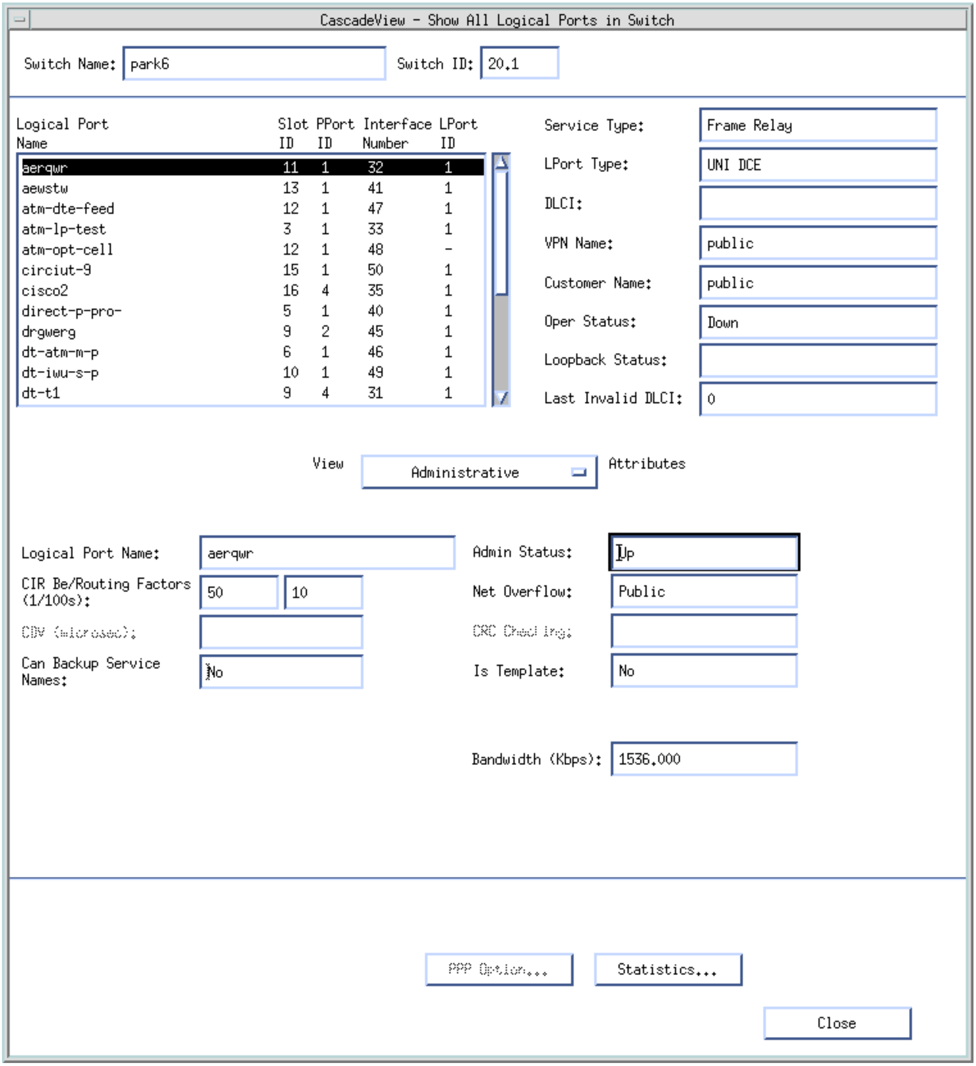


Figure 1-10. Show All Logical Ports in Switch Dialog Box

Show All Logical Ports in Switch Option Buttons

The following command buttons on the Show All Logical Ports in Switch dialog box enable you to obtain additional information about the logical port.

Choose	To
VPN/Customer	Display Virtual Private Network (VPN) and customer information for the selected port.
Get Oper Info	Display a status message in the Oper Status field that provides a brief status for the selected port.
PPP option	*(ISDN modules only)* Display the Show PPP Options dialog box to show the point-to-point protocol options for an ISDN module. Refer to *Configuring ISDN Services for B-STDX/STDX* for further details about ISDN configuration options.
Statistics	Display the summary statistics for the selected physical port. For more information about summary statistics, refer to Chapter 5, "Generating Statistics and Reports".
Diagnose	Display foreground diagnostic information for a selected port.
View Qos	*(ATM Only)* Display the Quality of Service parameters for a selected port.
Close	Exit the dialog box and return to the network map.

Show All Logical Ports in Switch Fields

Table 1-6 through Table 1-13 describe all of the possible fields on the Show All Logical Ports in Switch dialog box. The options that the system displays vary depending on the type of port you are viewing.

Table 1-6. Show All Logical Ports in Switch Identification Fields

Field	Action/Description
Customer Name	Displays the name of the customer using the VPN.
Switch Name	Displays the name entered to identify the switch at the time of configuration.
Logical Port Name	Displays the name assigned to the LPort at the time of configuration. The LPort ID uniquely identifies each logical port within the physical port.
Slot ID	Indicates the back panel physical slot number where the I/O module that contains the selected logical port is installed.
PPort ID	Displays the ID number of the physical port for which the selected logical port is configured.
Interface Number	Displays 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*).
Last Invalid DLCI	This field is for B-STDX Frame Relay Networks only. If the system displays a value in this field, the value indicates the last invalid DLCI that was detected by the switch. This value indicates that there is a problem with a configuration either at the switch or at the Customer Premise Equipment (CPE). Check this value if you have a DLCI that is not receiving traffic.

Table 1-6. Show All Logical Ports in Switch Identification Fields (Continued)

Field	Action/Description
Loopback Status	*(DS3 only)* The default value for this field is *none*. If you enable diagnostic loopback tests, this field displays the ATM DS3 card's loopback status. A loopback test enables you to test the physical path for data transmission by looping back traffic in one or both directions. For more information about loopbacks, refer to Chapter 4, "Loopbacks".
LPort ID	Displays the ID number that uniquely identifies each logical port. • For UNI-DCE physical ports, the LPort ID is always 1. • For T1 and E1 physical ports, you enter the LPort ID when you add the T1 or E1 port. • For Frame Relay trunking, the LPort ID specifies the DLCI of the Frame Relay Trunk.
LPort Type	Displays the configured type of the selected logical port.
Oper Status	Indicates whether the selected port is operationally Up, Down, or Unknown. Unknown indicates that the NMS is unable to contact the switch to retrieve status.
VPN Name	Displays a virtual private network name. Refer to "VPN Overview" on page 2-33 for more information.

3. You can use the *Statistics* command to display the summary statistics for the selected logical port. For more information about summary statistics, refer to Chapter 6, “Logical and Physical Port Statistics”.

4. Choose the View Attributes option to display various attributes for the logical port.

5. When you finish reviewing the logical port information, choose Close to exit the dialog box and return to the network map.

Logical Port Attributes

The system displays Logical Port Attribute information at the bottom of the Show All Logical Ports in Switch dialog box. The attribute information that the system displays differs depending on the attribute that you select from the View Attributes option.

Table 1-7 identifies each of the different attribute types along with a reference to the table that describes these attributes.

Table 1-7. Logical Port Attribute Types

For Information About	See...
Administrative	Table 1-8 on page 1-34
Congestion Control	Table 1-9 on page 1-37
Trap Control	Table 1-10 on page 1-39
Link Mgmt	Table 1-11 on page 1-41
SMDS	Table 1-12 on page 1-45
ISDN	*Configuring ISDN Services for B-STDX/STDX* for further details about ISDN attributes.

Administrative Attributes

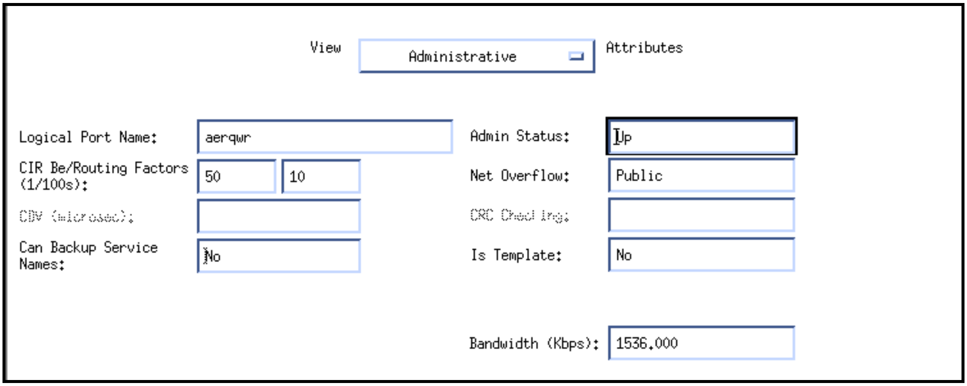


Figure 1-11. Administrative Attributes

Table 1-8. Administrative Attributes Fields

Field	Action/Description
Admin Status	Displays 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 off-line so that diagnostics can be run to test the port. A logical port with an Admin Status of *Down* is not operational.
Bandwidth (Kbps)	Displays the bandwidth for the selected logical port.
Bit Stuffing	Designates whether bit stuffing is enabled for the selected logical port. This parameter only applies to T1/E1 and DSX-1 modules.
Can Backup Service Names	Displays either Yes or No to specify whether or not this logical port can be backed up to a service name binding.
CIR Be/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 include any value between 50-100 percent. The default value is 50 percent.

Table 1-8. Administrative Attributes Fields (Continued)

Field	Action/Description
CDV (microsec)	*(ATM, Optimum Cell Trunks only)* Displays the maximum cell delay variation (in microseconds) for this logical port. This value only applies to CBR traffic, and specifies the maximum variation in time delays between cells going out of this logical port. The UPC uses this value to police the requested traffic descriptor. The default value is 684 for DS3 ports, or 191 for OC3c 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.
CRC Checking	*(HSSI modules only)* Specifies 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	Displays either Yes or No to indicate whether you can use this logical port configuration as a template.
Net Overflow	Displays *Public* if the customer (on a private network) 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 private network. For more details, refer to "Private Net Overflow" on page 2-33. **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 of a trunk failure.

Table 1-8. Administrative Attributes Fields (Continued)

Field	Action/Description
VPI/VCI	*(ATM, Optimum Cell Trunks Only)* Displays the value for the VPI number and VCI number. The **VPI number** displays a number between 0 and 15 to identify the 4-bit virtual path for the ATM logical port. 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. The **VCI number** identifies the virtual channel. 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 that the system displays for this field is equivalent to the VCI value in the ATM cell header. If this is a logical port on a frame-based I/O module, the value should be a number from 32 to 63. If this is a logical port on an ATM-based I/O module (such as the ATM DS3 module), the value should be a number from 32 to 255. **Note:** The VPI and VCI are used only for establishing connections between two ATM entities, not the end-to-end connection.

Congestion Control Attributes

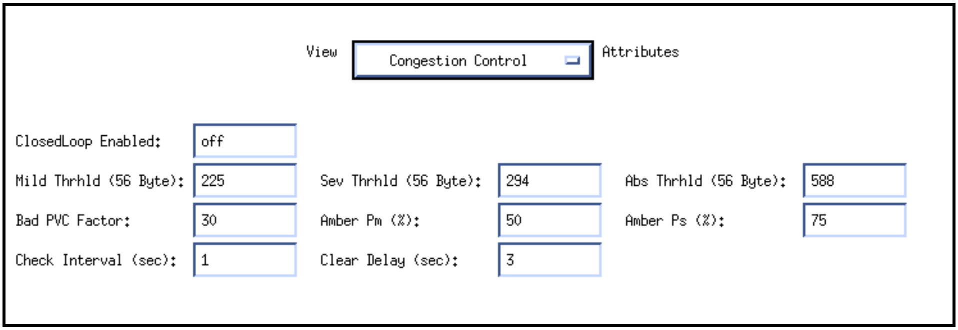


Figure 1-12. Congestion Control Attributes

Table 1-9. Congestion Control Attributes Fields

Field	Action/Description
Closed Loop Enabled	Set to on or off to indicate whether or not the specified congestion control values are applied. The default value for this field is off.
Mild Thrhld	Displays the mild threshold value which determines how the switch reacts to congestion at the mild threshold state. This value is specified when you configure the logical port and can be modified. The threshold has a default value that is relative to the value of the bandwidth.
Sev Thrhld (56 Byte)	Displays the severe threshold value which determines how the switch reacts to congestion at the severe threshold state. This value is specified when you configure the logical port and can be modified. The threshold has a default value that is relative to the value of the bandwidth.

Table 1-9. Congestion Control Attributes Fields (Continued)

Field	Action/Description
Abs Thrhld (56 Byte)	The absolute congestion threshold value. This value is specified when you configure the logical port and can be modified. The threshold has a default value that is relative to the value of the bandwidth. The threshold value is specified in units of data buffers queued for transmit. On the B-STDX 9000, the threshold value is specified in 56-byte buffer units.
Bad Pvc Factor	The factor used to determine the threshold for bad PVC detection. The range of values for this field is from 0 through 32.
Amber Pm (%)	Controls the reduction percentage of the excess burst size (Be) when mild congestion occurs. The default value for this field is 50.
Amber Ps (%)	Controls the reduction percentage of the excess burst size (Be) when server congestion occurs. The default value for this field is 100. If 100 is used, all amber packets are discarded.
Check Interval	The time interval (in seconds) between two successive congestive state checkings. The default value for this field is 1.
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.

Refer to the Network Configuration Guide for B-STDX/STDX *for detailed information about how to set congestion thresholds for a logical port.*

Trap Control Attributes

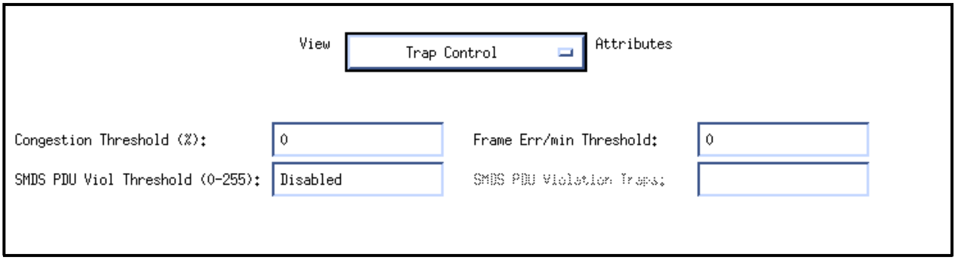


Figure 1-13. Trap Control Attributes

Table 1-10. Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold (%)	If the rate of congestion over a one-minute period exceeds the threshold percentage specified, a trap is sent to the NMS. Valid values are 0 to 100; the default value is zero. A congestion trap is generated and sent to the NMS if the rate of congestion over a one-minute period exceeds the congestion threshold percentage value. 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 will only generate a trap for serious network congestion. Using a default value of 0 disables the congestion threshold feature. If your system displays a value of 0 for the congestion threshold, no traps are generated for the logical port. Refer to the *Network Configuration Guide for B-STDX/STDX* for more details about how to configure a logical port.

Table 1-10. Trap Control Attributes Fields (Continued)

Field	Action/Description
Frame Err/min Threshold	Specifies the configured threshold of frame errors on the logical port that will trigger a trap to be sent to the NMS. The default value of 0 is set at the time of logical port configuration. The range of values for this field is from 0 to 16384.
SMDS PDU Viol Threshold (0 - 255)	Specifies the configured threshold of SMDS PDU violations. The default value of 0 is set at the time of logical port configuration. The range of values for this field is from 0 to 255.
SMDS PDU Violation Traps	A value of *enabled* specifies that the NMS will issue traps for PDU violations. An SMDS PDU violation can be either an SIP3 SMDS address failure or an invalid DXI2 frame header. These errors mean incoming frames are bad and this usually indicates problems with the CPE configuration. A value of *disabled* specifies that the NMS will not issue traps for SMDS PDU violations.

Link Management Attributes

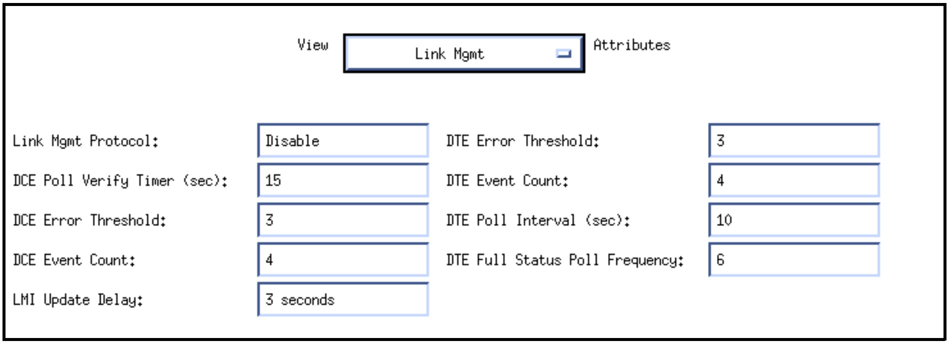


Figure 1-14. Link Management Attributes

Table 1-11. Link Management Attributes Fields

Field	Action/Description
Link Mgmt Protocol	Displays 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*** – is for international standard (European) use only. The network uses DLCI 0 for link management. ***Auto Detect*** – is used only if the attached customer premise equipment (CPE) provides the link management protocol. This logical port can automatically detect which protocol is in use. ***Disabled*** – is used only if the attached CPE does not support link management or if you need to disable link management for troubleshooting.

Table 1-11. Link Management Attributes Fields (Continued)

Field	Action/Description
DCE Poll Verify Timer (sec)	Displays 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 T392 seconds, the network records an error. The default is 15 seconds.
DCE Error Threshold	Displays the parameter used in conjunction with the DCE Events Count (N393) parameter. The Local Management protocol monitors the last N393 events. If N392 or more are found in error, 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 T392 timer. 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 1-11. Link Management Attributes Fields (Continued)

Field	Action/Description
LMI Update Delay	Displays a value from 1 to 9 seconds to enable asynchronous LMI updates. The default is 3 seconds. When you set this timer, the switch sends a signal (known as an event) to notify other network equipment (CPE) when a circuit on this logical port goes up or down. The period of time you specify creates a buffer. If the circuit recovers within this period of time, no event is issued. If you choose No Updates, the switch does not send a signal to the CPE. If you choose 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 increase the LMI Update Delay. This delay introduces a time element, which can minimize end-user visibility to a self-recoverable outage.
DTE Error Threshold	Displays the parameter used in conjunction with the DTE Events Count (N393) parameter. The Local Management protocol monitors the last N393 events. If N392 or more are found in error, the link is declared inactive. The default value is 3.
DTE Event Count	The number of events in a sliding window of events that you can monitor. An event is the receipt of a valid or an invalid Status message, or the non-receipt of a Status Enquiry message after T391 seconds. 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 1-11. Link Management Attributes Fields (Continued)

Field	Action/Description
DTE Poll Interval (sec)	Displays the number of seconds between the transmission of Status Enquiry messages. The default is 10 seconds.
DTE Full Status Poll Frequency	The number of T391 polling cycles between full Status Enquiry messages. The default is 6.

SMDS Attributes

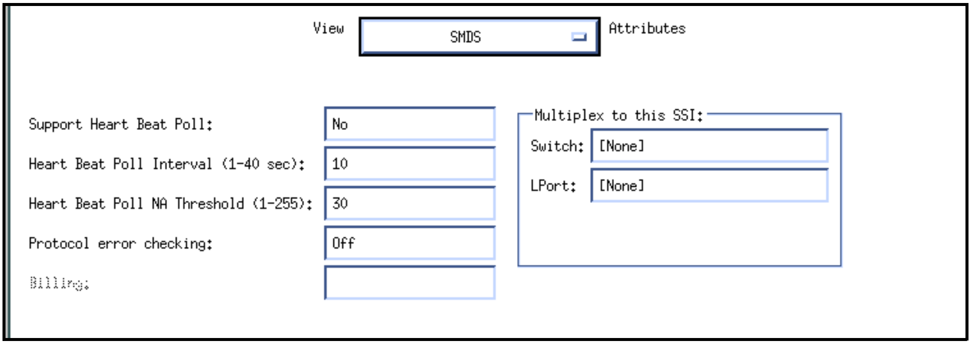


Figure 1-15. SMDS Attributes

Table 1-12. SMDS Attributes Fields

Field	Description/Action
Support Heart Beat Poll	Heart beat polls check for a keep-alive signal coming from the CPE. Displays *Yes* (*default*) only if the CPE connected to this port supports heart beat poll responses; otherwise this value is *No*.
Heart Beat Poll Interval (1 - 40 sec)	The lapse of time that is to occur 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 is sent to the NMS each time the threshold for the DXI/SNI 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.

Table 1-12. SMDS Attributes Fields (Continued)

Field	Description/Action
Protocol error checking	This selection enables you to determine the level of protocol error checking to perform on PDUs received by this logical port. This field is **enabled for debugging purposes only**. *Off (default)* – Minimal address checking occurs. *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.
Multiplex to this SSI: Switch	If this is a DXI/SNI logical port that is multiplexed to a specific SSI-DTE, this value specifies an individual address.
Multiplex to this SSI: Lport	If this is a DXI/SNI logical port that is multiplexed to a specific SSI-DTE logical port, this value specifies the SSI-DTE logical port.

Reviewing All Logical Ports in a Physical Port

To display the logical ports for a selected physical port, complete the following steps:

1. Display the View (or Show) Physical Port Attributes dialog box (Figure 1-9 on page 1-19). Refer to "Reviewing the Status of Physical Ports" on page 1-19 if you are not sure how to perform this step.
2. Choose the *Logical Port* command button.

   The Show All Logical Ports in PPort dialog box (Figure 1-16) displays.

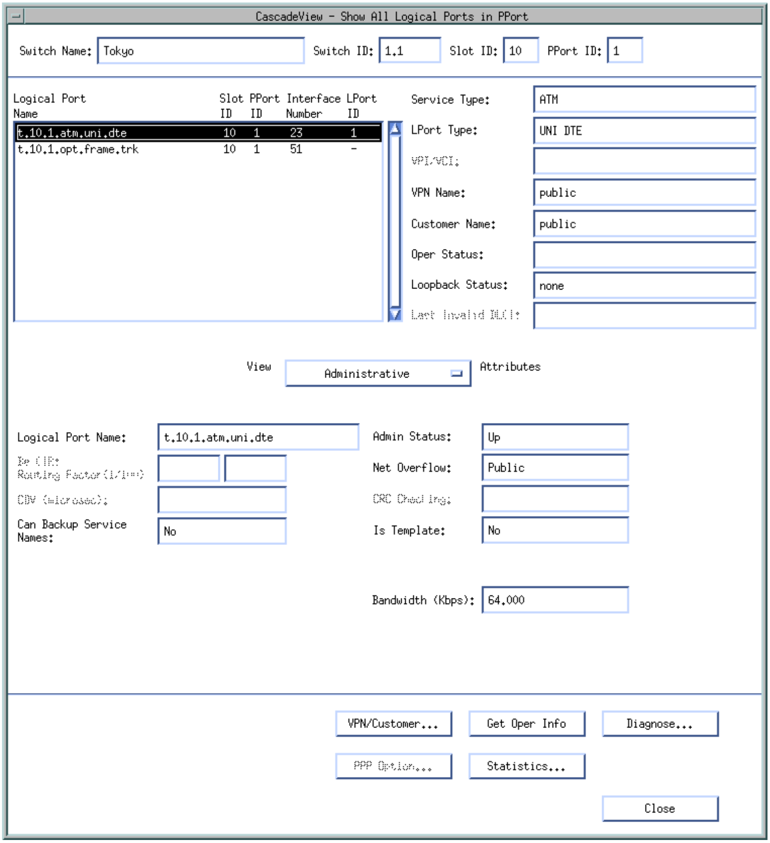


Figure 1-16. Show All Logical Ports in PPort Dialog Box

The Show All Logical Ports in PPort dialog box displays identifying information about the Physical Port and associated Logical Ports at the top of the dialog box.

Logical Port Attributes

Attribute information is displayed at the bottom of the dialog box. The attribute information that the system displays will differ depending on the attribute that you select from the View Attributes option.

Table 1-13 identifies each of the different attribute types along with a reference to a description of these attributes.

Table 1-13. Attribute Descriptions

For information about	Refer to...
Administrative	Table 1-8 on page 1-34
Congestion Control	Table 1-9 on page 1-37
Trap Control	Table 1-10 on page 1-39
Link Management	Table 1-11 on page 1-41
SMDS	Table 1-12 on page 1-45
ISDN	*Configuring ISDN Services for B-STDX* for further details about ISDN attributes.

Reviewing the List of Subnets

The Show All Subnets function displays a list of subnets defined for a switch.

To display a list of the switches on the currently displayed network map, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Subnets. The Show All Subnets dialog box appears.

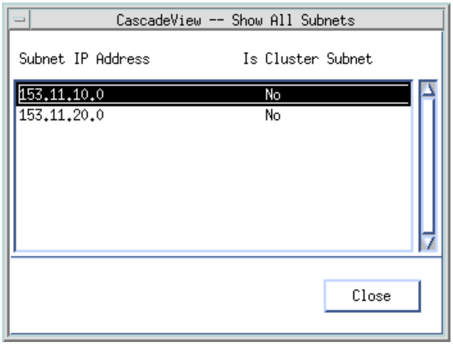


Figure 1-17. Show All Subnets Dialog Box

Table 1-14. Show All Subnets Fields

Field	Action/Description
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. Refer to the *Network Configuration Guide for B-STDX/STDX* for further details.
Is Cluster Subnet	Displays Yes or No to specify whether or not the subnet is part of a cluster.

Reviewing the List of Clusters

The Show All Clusters function displays a list of clusters defined for a switch. For further details about how to configure a cluster in a subnet, refer to the *Network Configuration Guide for B-STDX/STDX*. To display a list of the clusters defined for a switch on the currently displayed network map, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Clusters. The Show All Clusters dialog box appears.

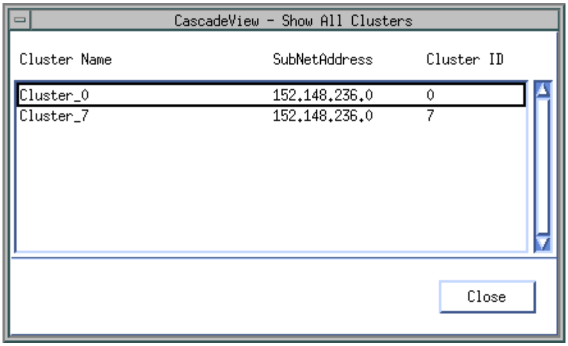


Figure 1-18. Show All Clusters Dialog Box

Table 1-15 describes the fields in the Show All Clusters dialog box.

Table 1-15. Show All Clusters Fields

Field	Action/Description
Cluster Name	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. Refer to the *Network Configuration Guide for B-STDX/STDX* for details.
Cluster ID	Displays a value from 0 to 7 to indicate the cluster ID portion of the IP address.

Reviewing the Status of Switches

The Show All Switches function displays switch configuration information for any switch on the network map.

To display a list of the switches on the currently displayed network map, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Switches. The Show All Switches dialog box appears.

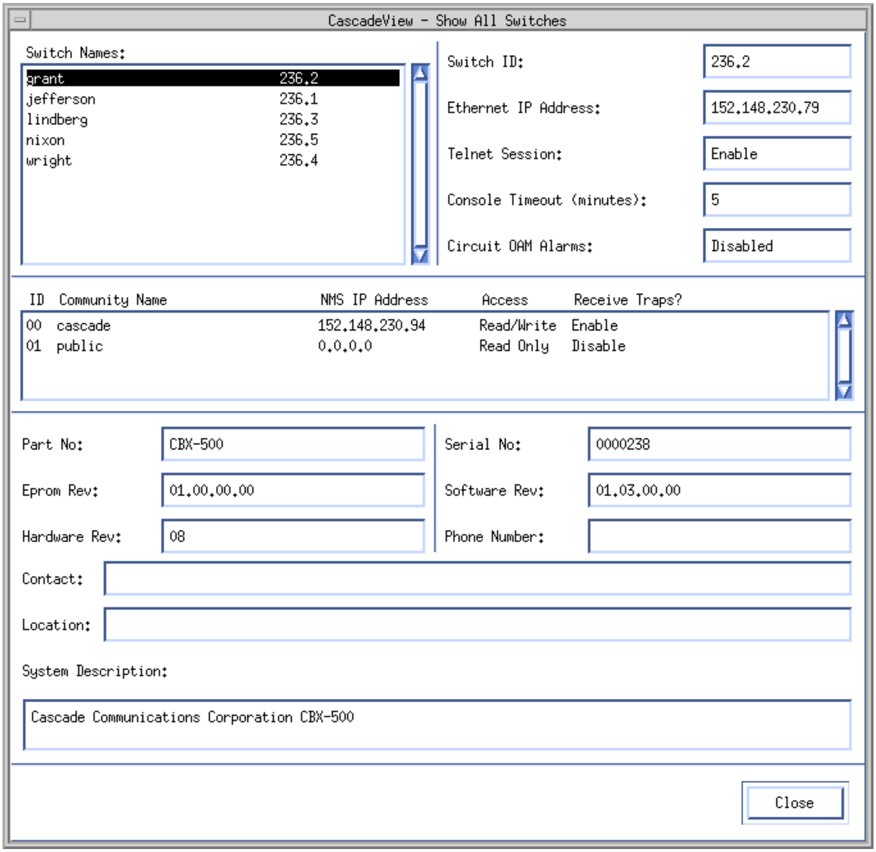


Figure 1-19. Show All Switches Dialog Box

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

3. When you finish reviewing the status information, choose Close to exit from the dialog box and return to the network map.

Table 1-16 describes the fields in the Show All Switches dialog box.

Table 1-16. Show All Switches Fields

Field	Action/Description
Switch Names	Displays the name assigned to each switch map.
Switch ID	Displays the switch number used as the host assignment in the switch's internal IP Address.
Ethernet IP Address	Displays the external IP address for the switch's LAN side. You assign this IP address to the Ethernet module in the gateway switch during configuration.
Telnet Session	Displays whether Telnet access to the switch is enabled or disabled.
Console Timeout (minutes)	Displays the time period (in minutes) of inactivity before the RS232 console port is logged off. A value of 0 specifies that there is no console timeout period so that the console will not time out during periods of inactivity.
Circuit OAM Alarms	(*ATM CS and IWU modules only*) A value of *Enabled* allows this circuit to generate OAM alarms to indicate whether the circuit is up or down. These alarms send a signal to the logical port whenever the circuit goes down or comes back up. A value of *Disabled* indicates that this option is not used.

Table 1-16. Show All Switches Fields (Continued)

Field	Action/Description
Community Name	Displays the name used to control access to the switch's configuration. The Community Name is used in conjunction 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 lowercase (case-sensitive) *cascade*.
NMS IP Address	Displays the address of the NMS that is configured to communicate with the selected switch. Traps generated from the selected switch are also sent to this IP Address. In order to send SNMP commands to the switch and to download switch software, the NMS IP Address must be the same as the IP Address of the switch.
Access	Displays the access privileges the NMS has with the selected switch. The first NMS always has Read/Write privileges. An NMS with Read only privileges can receive traps but is restricted from sending write commands to the switch.
Receive Traps	Indicates 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.	Displays the part number of the Packet Processor for an STDX 3000 or 6000, or the part number of the Control Processor for a B-STDX 8000/9000.
Eprom Rev	Displays the switch's EPROM revision level; 2.0 or greater.

Table 1-16. Show All Switches Fields (Continued)

Field	Action/Description
Hardware Rev	Displays the revision level of the Packet Processor for an STDX 3000 or 6000, or the revision level of the Control Processor for a B-STDX 8000/9000.
Serial No	Displays the serial number of the selected switch, obtained from the MAC Ethernet Address of the switch.
Software Rev	Displays the revision number for the firmware currently running on the selected switch.
Phone Number	Displays the telephone number of the contact person who is responsible for the selected switch.
Contact	Displays the name of a contact person who is responsible for the selected switch.
Location	Displays the physical location of the selected switch.
System Description	Displays the switch type, either STDX 3000, STDX 6000, B-STDX 8000 or B-STDX 9000. This parameter is taken directly from the switch and therefore is displayed only if the NMS is actively communicating with the selected switch.

2

Monitoring Trunks and Circuits

This chapter explains how to monitor trunks, circuits, and SMDS routes. You use the CascadeView/UX Monitor menu to access each of the functions described in this chapter. For more information about all of the functions that you use to monitor switch objects and where these functions are described, see Table 1-1 on page 1-2.

> *You do not need to log on to monitor switch objects.*

Reviewing the Status of Trunks

The Show All Trunks function displays the operational status and available bandwidth of a specified trunk. A trunk represents a link from one Cascade switch to another Cascade switch for the purpose of transporting user traffic, routing updates, network management pools, and other management traffic.To display trunks for a currently displayed network map, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Trunks. The Show All Trunks dialog box appears.

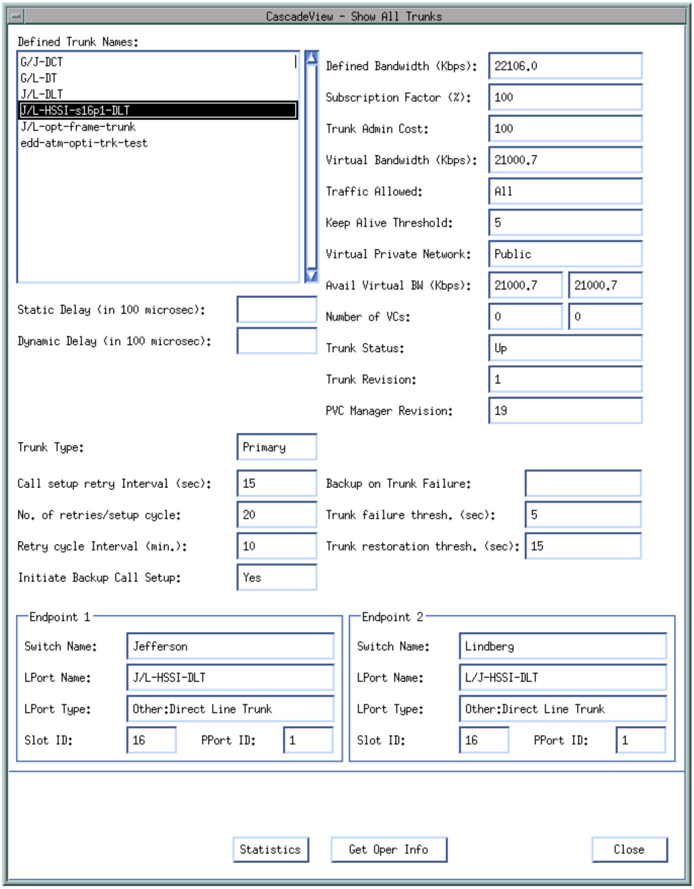


Figure 2-1. Show All Trunks Dialog Box

> *A negative value in the Avail Virtual BW field 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 value.*

2. In the Defined Trunk Names list, select the name of the trunk from which you want to retrieve status information.
3. You can choose the *Statistics* option to display the summary statistics for the selected trunk. For more information about summary statistics, refer to Chapter 8, “Trunk and Circuit Statistics”.
4. If the selected trunk is an ATM direct cell trunk, you can use the View QoS option to display the Logical Port Quality of Service statistics for the selected trunk. For more information about QoS statistics, refer to “Displaying QOS Statistics for ATM Direct Cell Trunks” on page 8-4.
5. When you finish reviewing the status information for the selected trunk, choose Close to exit the dialog box and return to the network map.

   Table 2-1 describes the Show All Trunks fields.

Table 2-1. Show All Trunks Fields

Field	Action/Description
Defined Trunk Names	Displays the names of the trunks configured for the current network map.
Defined Bandwidth (Kbps)	Displays the amount of bandwidth, in Kbps, for the selected trunk line.
Subscription Factor (%)	Displays the percentage used to calculate the Available Virtual Bandwidth for the selected trunk. Because Cascade allocates the bandwidth of the CIR when you configure the circuit, this K factor enables you to over-configure 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.
Trunk Admin Cost	Displays the cost of using this trunk for a virtual circuit when a virtual circuit is dynamically created on the switch. A larger value makes it less likely that the trunk will be used for a virtual circuit. A smaller value makes it more likely that the trunk will be used for a virtual circuit. The range of values for this field is 1 - 65534; the default value is blank.
Virtual Bandwidth (Kbps)	Displays 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 purposes.

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

Field	Action/Description
Allowed Traffic	Displays *All* to indicate that the trunk can carry both user data and network management traffic. Displays *Mgmt Only* to indicate that the trunk can carry only network management traffic, such as SNMP communication between a switch and the NMS.
Keep Alive Threshold	The number of seconds that the trunk protocol will exchange Keep Alive (KA) control frames without getting a response from the remote node. The retry interval is represented in seconds. The keep alive threshold can be any value between 3 and 255 seconds. The default is 5 seconds. **Note:** If you are running different switch code versions in your network, for example Version 4.1 and Version 4.2, you must accept the default value of 5 seconds. **Note:** Service is disrupted if you change this value after the trunk is online.
Virtual Private Network	Displays a virtual private network name. Refer to "VPN Overview" on page 2-33 for more information.
Private Net Overflow	Displays *Public* if the customer (on a private network) 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 private network. For more details, refer to "Private Net Overflow" on page 2-33. **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 of a trunk failure.

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

Field	Action/Description
Avail Virtual BW (Kbps)	Displays the amount of bandwidth, in Kbps, available for circuit configuration and allotment on the selected trunk. 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.
Number of VCs	The number of virtual circuits.

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

Field	Action/Description
Trunk Status	Displays the current status of the selected trunk. The possible values include the following: *Unknown* – The NMS cannot reach one or both switches. *Down* – The switches are unable to 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* – 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 in the process of exchanging the network topology. *Loading* – The two switches are requesting the most recent link state. *Up* – The trunk is up and operational between the two switches. *bt Defined* – A backup trunk is ready for backup.
Static Delay	The recently measured one-way delay of the trunk, in units of 100 microseconds. This value may vary from the Dynamic Delay value due to congestion. A value of zero indicates that the delay value is not available for this trunk.
Dynamic Delay	The measured one-way delay of the trunk, in units of 100 microseconds. A value of zero indicates that the delay value is not available for this trunk.

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

Field	Action/Description
Trunk Revision	The trunk revision.
PVC Manager Revision	The PVC manager software revision.
Trunk Type	Displays *Normal*, *Primary,* or *Backup*. 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 Trunk to be 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.
Backup on Trunk Failure	Displays *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.
Switch Initiating the Call Setup	(Backup Trunks only) The name of the switch that performs the call setup for the trunk.
Call setup retry Interval (sec)	Defines the lapse of time between each retry during a given Retry Cycle. The default is 15 seconds. For example, if your system performs five 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	The number of retries that the system performs during a retry cycle. The default is 20 retries.
Retry cycle Interval (min).	The lapse of time between retry cycles (in minutes). The default is 10 minutes.

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

Field	Action/Description
Trunk failure thresh. (sec)	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).
Trunk restoration thresh. (sec)	The default value for this field is 15 seconds. The purpose for this field is to avoid unnecessary losses in service that result if restoration is attempted on a primary trunk that is cycling between the up and down states. A primary trunk is only considered available for restoration by the switch if it remains in the link-up state for a minimum amount of time as defined by this threshold.
Switch Name	Displays the name of the Cascade switch on either side of the trunk line.
LPort Name	Displays the name of the logical port for each side of the trunk.
LPort Type	Displays the configured type of the selected logical port.
Slot ID	Indicates the physical slot number where the I/O module which contains the selected port is installed.
PPort ID	Displays the ID number of the physical port for which the selected logical port is configured.

Reviewing the Status of Circuits

The Show All Circuits function displays the current configuration, status, and routing information for all circuits defined in the network map.

To display the circuit status information, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show Circuits, then select one of the following options:

   All on Map — Displays a list of all the circuits configured for the current map. Choose the circuit for which you want to display status information.

   All on Switch — Select a switch on the current map, then use this option to display a list of all the circuits configured for this switch. Choose the circuit for which you want to display status information.

   All by Name — Use this option to enter a specific circuit name for which you want to display status information. You can use any of the following wildcard characters to find a specific circuit name:

   - Use an * to match any number of characters
   - Use a ? to match a single character
   - To match the * character, type **
   - To match the ? character, type \?
   - To match the \ character, type \\

   *Using only the * character can result in a lengthy search.*

   Circuit names are case-sensitive.

   All on Switch and by Name — Select a switch on the current map, then use this option to enter the name of a specific circuit in the switch for which you want to display status information. You can also use the wildcard characters noted under the **All by Name** field.

   After you select an option, the Show All PVCs on Map dialog box appears as shown in Figure 2-2.

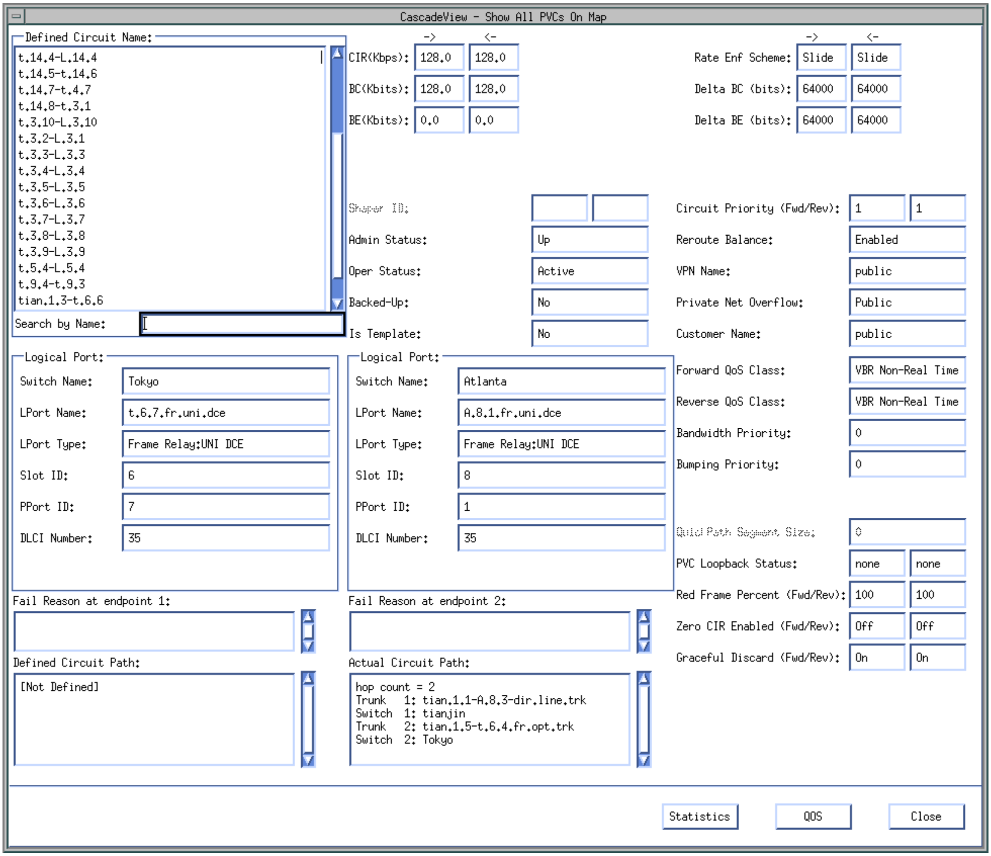


Figure 2-2. Show All PVCs on Map Dialog Box

> *This dialog box displays the circuit names and circuit attributes as configured in the NMS; whereas the Status, Path, and Fail Reasons are extracted directly from the switch.*

2. Select the name of the circuit for which you want to retrieve status information. You can use the Search by Name field to use wildcard characters.

- You can use the *Statistics* command to display the summary statistics for the selected circuit. For more information about summary statistics, refer to "Trunk and Circuit Statistics" on page 8-1.
- You can use the *QOS* command to display the quality of service/class of service statistics for the selected circuit. For more information about these statistics, refer to Chapter 8, "Trunk and Circuit Statistics".
- The **Fail Reason at endpoint 1** field displays the reason a selected circuit failed (if any) for a given endpoint.
- The **Fail Reason at endpoint 2** field displays the reason a selected circuit failed (if any) for a given endpoint.
- When you finish reviewing status information, choose Close to exit the dialog box and return to the network map.

Table 2-2 briefly describes all the possible fields that may appear on the Show All PVCs dialog box:

Table 2-2. Show All PVCs Fields

Field	Action/Description
Defined Circuit Name	Displays a listing of the circuits configured in the network.
Search by Name	You can use a wildcard search to find a specific circuit name. Use an * to match any number of characters Use a ? to match a single character To match the * character, type ** To match the ? character, type \? To match the \ character, type \\\\
Logical Port Fields	
Switch Name	Displays the name of the switch at each endpoint of the circuit.
LPort Name	Displays the name of the logical port at each endpoint of the circuit.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
LPort Type	Displays the configured type of the selected logical port.
Slot ID	Indicates the physical slot number where the I/O module that contains the selected port is installed.
PPort ID	Displays the ID number of the physical port for which the selected logical port is configured.
VPI# (*ATM only*)	Displays a number between 0 and 15 to identify the 4-bit virtual path for the ATM logical port. 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.
VCI# (*ATM only*)	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 that the system displays for this field is equivalent to the VCI value in the ATM cell header. If this is a logical port on a frame-based I/O module, the value should be a number from 32 to 63. If this is a logical port on an ATM-based I/O module (such as the ATM DS3 module), the value should be a number from 32 to 255.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
DLCI Number (Frame Relay only)	Displays the Data Link Connection Identifier number configured for the circuit endpoint. Refer to the *Network Configuration Guide for B-STDX/STDX* for a complete description of this field and its use
Circuit Attribute Fields	
Admin Status	Displays a value of *Up* or *Down* to indicate the administrative setting of the circuit.
Oper Status	The operational status of the PVC. There are four possible values: *Active* – Indicates that the PVC is operational between the two endpoints. *Inactive* – Indicates that the PVC is not operational between the two endpoints. *Invalid* – Indicates that the PVC configuration is not contained within the calling node. *Unknown* – Indicates that the calling node did not respond to the NMS request for the status of this PVC.
Backed Up	Specifies *Yes* or *No*. Yes indicates that there is a redundant PVC for this PVC. No indicates there is no redundant PVC.
Is Template	Displays *Yes* if this circuit connection was defined as a template. Displays *No* if this connection is not a template.
Circuit Priority	Displays the value used to control the priority of green frames traveling over the circuit. The highest priority is 1 and the lowest priority is 3.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
Reroute Balance	When *Enabled* (the default), switch tuning parameters take effect. When disabled, switch tuning parameters are ignored for the circuit.
VPN Name	Displays a virtual private network name. Refer to "VPN Overview" on page 2-33 for more information.
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 only other private trunks during overflow or trunk failure. For more details, refer to "Private Net Overflow" on page 2-33.
Customer Name	The name of the customer assigned to the VPN.
Forward QoS Class	The Quality of Service class for forward traffic. Cascade currently supports only the *VBR non-real time* Class of Service value for non-real time applications. This option enables the circuit to transfer large amounts of data over a long period of time using a pre-established ATM connection. Class of service values enable you to prioritize circuit traffic.
Reverse QoS Class	The Quality of Service class for reverse traffic. Cascade currently supports only the *VBR non-real time* Class of Service value for non-real time applications. This option enables the circuit to transfer large amounts of data over a long period of time using a pre-established ATM connection. Class of service values enable you to prioritize circuit traffic.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
Bumping Priority	A number from 0 through 7 where 0 is the default and indicates that the circuit **will not be bumped**. The combination of the value of the bandwidth priority and the bumping priority indicates the importance, or priority, of the circuit. Lower values, specify a higher priority, therefore, 1 is the highest bumping priority and 7 is the lowest. This value determines the circuit that is allowed to use a low-cost trunk when two circuits attempt to use the trunk at the same time and have the same bandwidth priority. The purpose of the field is to prioritize which circuit will use the trunk with the least cost. Refer to the *Network Configuration Guide for B-STDX/STDX* for a complete description of Circuit Priority Routing.
Bandwidth Priority	A value from 0 through 3 where 0 is the default and indicates the highest priority. The combination of the Bumping Priority and the Bandwidth Priority values enable the system to prioritize the circuit that can use the path with the lowest cost. If two circuits have the same bandwidth priority, the system checks the value of the bumping priority. If you do not override the defaults (a bandwidth priority of 0 and a bumping priority of 0), all circuits are defined at the highest priority (0,0). A network of circuits that are all defined with a 0,0 routing priority operates as though all circuits are given the same priority. Refer to the *Network Configuration Guide for B-STDX/STDX* for a complete description of Circuit Priority Routing.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
PVC Loopback Status	The loopback status of each endpoint. Possible settings are *None*, *Local*, *Remote*, or *Both*. Refer to Chapter 4, "Loopbacks".
Red Frame Percent	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.
Graceful Discard	Indicates 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 (Be).
Fail Reason	Displays the reason code for a circuit with an Inactive Operational status. See Table 2-3 for details.
Actual Circuit Path	Displays the actual path that OSPF selected for this circuit.
Defined Circuit Path	Displays a predefined path (if a path was specified at the time of circuit configuration).
Rate Enf Scheme	Displays *simple* or *jump*. *Simple* indicates time (Tc) as measured in periodic intervals. The configurable rate enforcement scheme provides more flexibility, increased rate enforcement accuracy, and improved switch performance. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
Delta BC (bits)	This value indicates 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. Set the number of Delta Bc bits for this circuit between 0 - 53535. The default is 53535.
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. Set the number of Delta Be bits for this circuit between 0 - 53535. The default is 53535.
Frame Relay Only Fields	*The following three fields appear when at least one endpoint of the circuit is defined as Frame Relay (either FR to FR or FR to ATM). The Display Circuit information is for both directions: LPort1 to LPort2 (→) and LPort2 to LPort1 (←).*
Committed Information Rate (Kbps)	Displays 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.
Committed Burst Size (Bc) (Kbits)	Displays the maximum amount of bits during time interval T that the network agrees to accept under normal conditions. Bc is defined for each circuit.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
Excess Burst Size (Be) (Kbits)	Displays 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.
Translation Option	Displays the translation method used for an ATM protocol (1490 or 1483), where the logical ports are defined as ATM UNI DCE/DTE. This field only appears if one endpoint of the circuit is configured as an ATM logical port and the other endpoint is Frame Relay.
Zero CIR Enabled	This value can be set to On or Off. If set to On, this value indicates that 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.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
ATM Only	The following four fields appear when at least one endpoint of the circuit is configured as an ATM logical port.
Sustainable Cell Rate (SCR)	Displays the Sustainable Cell Rate (SCR). SCR is the average cell transmission rate, measured in cells-per-second. SCR is usually some fraction of the PCR and its value must be greater than or equal to 1/64 of the PCR. ***Note:*** *Cells are transmitted at the peak cell rate only if there are available "credits". One credit is consumed for each cell transmitted. If all the credits are used up, the transmission rate is lowered to the SCR. Credits are accumulated only if there is not traffic. MBS governs the maximum amount of credits. If traffic remains constant, no credits are accumulated and the SCR becomes the cell transmission rate.*
Peak Cell Rate (PCR)	Peak Cell Rate (PCR) is the maximum transmission rate at which cells are transmitted for a selected PCR queue. It defines the shortest time period between cells. You can configure up to 8 PCR Queues, with the first 4 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, refer to the *Network Configuration Guide for B-STDX/STDX*.

Table 2-2. Show All PVCs Fields (Continued)

Field	Action/Description
Maximum Burst Size (MBS)	Displays the maximum number of cells that can be transmitted at peak cell rate. The default value for this field is 32 cells. The MBS value is specified in multiples of 32. For example, if the system displays a value of 2, the MBS is calculated: **2 X 32=64**. The MBS equals 64. MBS determines the maximum number of cells that an ATM DS3/E3 module can transmit at the peak cell rate. Once the port delivers the maximum number of cells, the transmission rate drops to the sustainable cell rate.
OAM Alarms (*ATM CS and IWU modules only*)	Choose *Enable* to allow this circuit to generate OAM alarms to indicate whether the circuit is up or down. These alarms send a signal to the logical port whenever the circuit goes down or comes back up.

Table 2-3. Inactive 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 Cascade Technical Response Center.
Not enough bandwidth on trunk at [*node*]	One of the trunks in the circuit path does not have enough bandwidth to accommodate the CIR of this circuit.	Reconfigure the circuit to a lower CIR or increase the physical or virtual bandwidth of the trunk that is causing the shortage. You can also add more parallel trunks. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information about how to perform these tasks.
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.
Cascade 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 this error to the Cascade Technical Response Center.
OPTimum path flow is blocked at [*node*]	Data flow through the Public Data Frame Relay network is temporarily blocked due to the flow control mechanism.	This condition should correct itself. If the problem persists, check for congestion problems in the OPTimum path.

Table 2-3. Inactive Operational Status Codes (Continued)

Fail Reason	Description	Solution
UNI/NNI is down at [*node*, *Lport*]	The UNI or NNI is down at the node/interface number (ifnum). The port is physically connected, but the LMI is down or the PPP Link Protocol or physical port is down.	Make sure the switch connects to the user device. Display traffic in and out of the port by generating Summary Statistics. (Refer to Chapter 6, "Logical and Physical Port Statistics".) Make sure that you configure the LMI properly and/or troubleshoot the LMI problem.
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 stating that it cannot receive data.	A trunk line in the path of the circuit 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 path for this circuit. Once the defined path is re-established, the circuit will be routed back to the defined path within 20 seconds of availability.

Reviewing 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 over the member circuits.

To display all configured Multicast DLCIs, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Multicast DLCIs. The Show All Multicast DLCIs dialog box appears as shown in Figure 2-3.

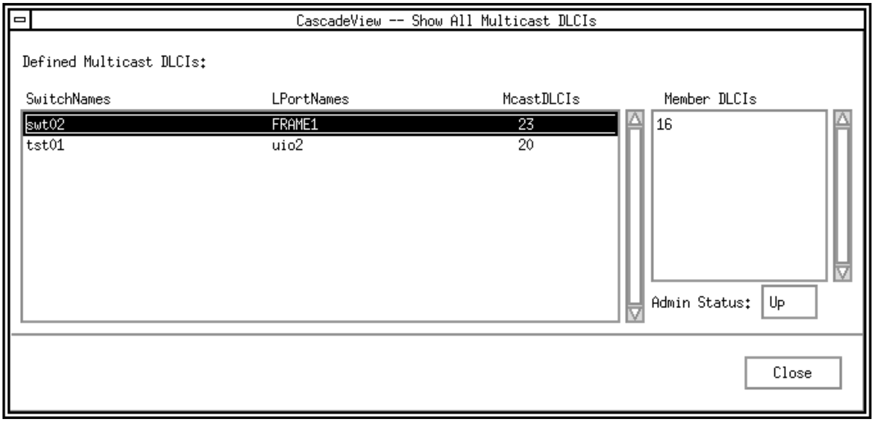


Figure 2-3. Show All Multicast DLCIs Dialog Box

When you finish reviewing the status information, choose Close to return to the network map. Table 2-4 describes the Show All Multicast DLCIs dialog box fields.

Table 2-4. Show All Multicast DLCIs Fields

Field	Action/Description
Switch Names	Displays the name of the switch for which the Multicast DLCI is configured.
LPort Names	Displays the name of the logical port for which the DLCI is configured.
Mcast DLCIs	Displays the number that uniquely identifies the Mulitcast DLCI configured for this switch.
Member DLCIs	Displays a DLCI for each member of the DLCI Multicast group.
Admin Status	Displays whether the Multicast DLCI is administratively *up* or *down*.

Reviewing 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 Cascade 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 Cascade network. For more information about how to configure a Management DLCI, refer to the *Network Configuration Guide for B-STDX/STDX*.

To display all configured Management DLCIs, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Management DLCIs. The Show All Management DLCIs dialog box appears (Figure 2-4).

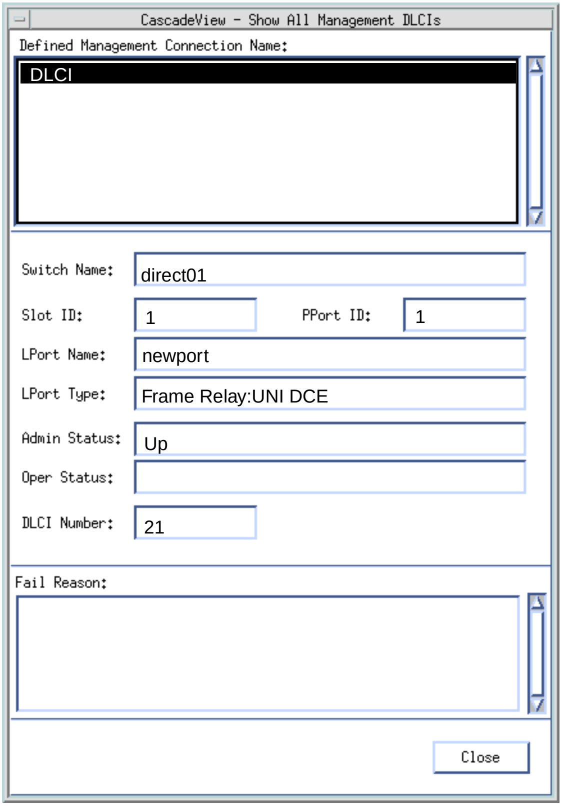


Figure 2-4. Show All Management DLCIs Dialog Box

2. When you finish reviewing the status information, choose Close to return to the network map.

Table 2-5 describes the Show All Management DLCIs dialog box fields:

Table 2-5. Show All Management DLCIs Fields

Field	Action/Description
Defined Management Connection Name	Displays the name configured for the Management DLCI.
Switch Name	Displays 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	Displays the ID number of the physical port for which the selected logical port is configured.
LPort Name	Displays the name of the logical port on the switch.
LPort Type	Displays the type of port configured for this logical port.
DLCI Number	Displays the number that uniquely identifies this Management DLCI configuration.
Admin Status	Displays a value of *Up* or *Down* to indicate whether the Management DLCI configuration is administratively *Up* or *Down.*
Oper Status	Displays the operational status of the Management DLCI. Possible values include: *Active, Inactive, Unknown, Invalid.*
Fail Reason	Displays a reason code if the Operator Status is Inactive.

Reviewing the Status of Management VPI/VCIs

The Show All Management VPI/VCIs function displays the status of all ATM Network Interworking connections. This type of connection enables an ATM broadband circuit to interconnect two Frame Relay networks. Each connection listed on this dialog box has an associated Virtual Path ID (VPI) and also a Virtual Channel ID (VCI).

To display all configured Management VPI/VCIs, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Management VPI/VCIs. The Show All Management VPI/VCIs dialog box appears, displaying a list of all ATM Network Interworking connections.

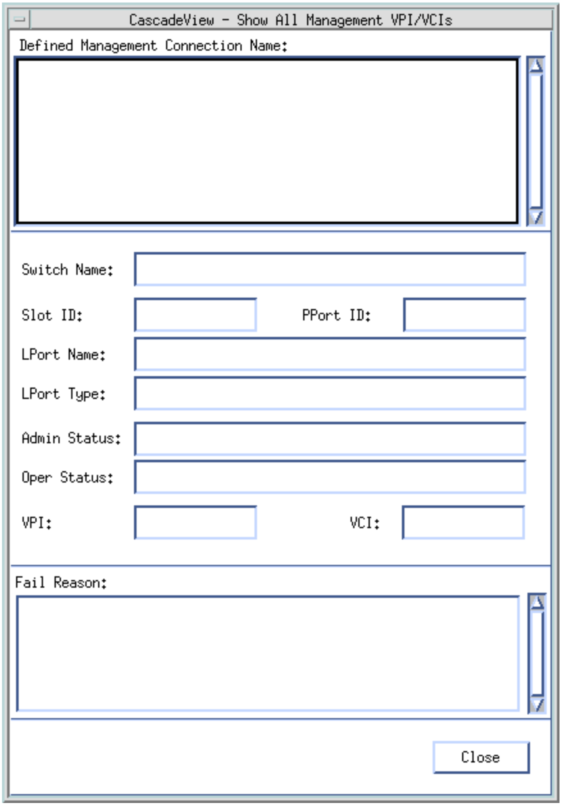


Figure 2-5. Show All Management VPI/VCIs Dialog Box

2. Select a defined management connection name for the retrieval of configuration information.

3. When you finish reviewing the information, choose Close.

   Table 2-6 describes the Show All Management VPI/VCIs dialog box fields.

Table 2-6. Show All Management VPI/VCIs Fields

Field	Action/Description
Defined Management Connection Name	Displays the name configured for the connection.
Switch Name	Displays the name of the switch associated with this connection.
Slot ID	Indicates the physical slot number where the I/O module that contains the selected port is installed.
PPort ID	Displays the ID number of the physical port for which the selected logical port is configured.
LPort Name	Displays the name of the logical port for this connection.
LPort Type	Displays the type of port configured for this logical port.
VPI	Displays a number between 0 and 15 to identify the 4-bit virtual path for the ATM logical port. 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.

Table 2-6. Show All Management VPI/VCIs Fields (Continued)

Field	Action/Description
VCI	Identifies the virtual channel. 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 that the system displays for this field is equivalent to the VCI value in the ATM cell header. • If this is a logical port on a frame-based I/O module, the value should be a number from 32 to 63. • If this is a logical port on an ATM-based I/O module (such as the ATM DS3 module), the value should be a number from 32 to 255. **Note:** The VPI and VCI are used only for establishing connections between two ATM entities, not the end-to-end connection.
Admin Status	Displays a value of *Up* or *Down* to indicate whether the configuration is administratively *Up* or *Down.*
Oper Status	Displays the operational status of the Management connection. Possible values include: *Active, Inactive, Unknown, Invalid.*
Fail Reason	Displays a reason code if the Operator Status is *Inactive.*

Reviewing the Status of SMDS Management Addresses

The Show All Management Addresses function displays the SMDS In-Band Management Address connections that are defined for a switch network. An SMDS In-Band Management Address allows the NMS to connect remotely to the Cascade network using SMDS services to transport the SNMP/UDP/IP protocol packets. For more information about how to configure an SMDS Management Address, refer to the *Network Configuration Guide for B-STDX/STDX*.

To display all configured SMDS Management Addresses, complete the following steps:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Management Addresses. The Show All SMDS Management Address dialog box appears as shown in Figure 2-6.

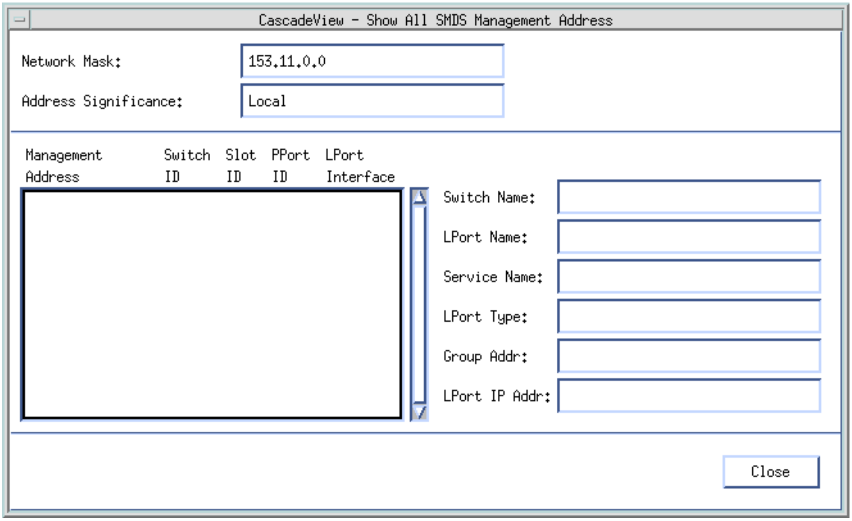


Figure 2-6. Show All SMDS Management Address Dialog Box

Table 2-7. Show All SMDS Management Addresses Fields

Field	Action/Description
Network Mask	Displays the Internet switch IP Network Number that was specified at the time of installation.
Address Significance	Displays a default of Local.
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	Displays the switch ID associated with this connection.
Slot ID	Indicates the back panel physical slot number where the I/O module that contains the selected logical port is installed.
PPort ID	Displays the port number.
LPort Interface	Displays the logical port interface number.
Switch Name	Displays the name of the switch associated with this connection.
LPort Name	Displays the name of the Lport associated with this connection.
Service Name	Displays SMDS as the type of service.
LPort Type	Displays 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.

Reviewing Customer/VPN Parameters

VPN Overview

Virtual Private Networks (VPNs) enable network providers to have dedicated network resources for those customers who require guaranteed performance, reliability, and privacy. When you add a trunk, you can dedicate trunks to specific customers and, if desired, allow customers to monitor their own networks. However, control and configuration of the switches stays with you as the network provider.

A VPN provides a dedicated bandwidth to the network customer; however, the management of the network is done by the provider.

To give a customer the ability 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.

Private Net Overflow

The Private Net Overflow parameters determine whether circuits originating from an logical port will be restricted to trunks of their own VPN or use public (shared) trunks during overflow conditions. You configure the Private Net Overflow parameters when you add a trunk (refer to the *Network Configuration Guide for B-STDX/STDX*).You can set the Private Net Overflow parameters to two modes:

Public (default) – Trunks are dedicated to the customer, however, in the event of outages the customer's traffic is allowed to run over common trunks (shared by a variety of different customers).

Restrict – Trunks are dedicated to the customer, and the customer's traffic is restricted to these trunks only. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.

Monitoring Customer/VPN Parameters

You can use either one of the following functions to monitor VPN information:

- Show All Customers. For more information about this function refer to "Monitoring VPN Networks" on page 2-36.
- Show All Virtual Private Networks. For more information about this function, refer to "Monitoring VPN Customers" on page 2-38.

You can also use the VPN/Customer View function to monitor logical ports, PVCs, or trunks for a specific VPN or customer. The following section describes this function.

Using the VPN/Customer View Function

When you need to monitor logical ports, PVCs, or trunks for a specific VPN or customer, use the Select Customer/VPN function. This function allows you to first select a VPN or customer name. Then, when you monitor these objects, the dialog box only displays the information for the VPN or customer name you select.

For example, if you select a VPN name, the Show All PVCs dialog box only displays the PVCs configured for the VPN name you select; same for Show All logical ports and Show All Trunks dialog boxes.

To use VPN/Customer view:

1. From the Administer menu, select Cascade Object:Select Customer/VPN. The following dialog box appears.

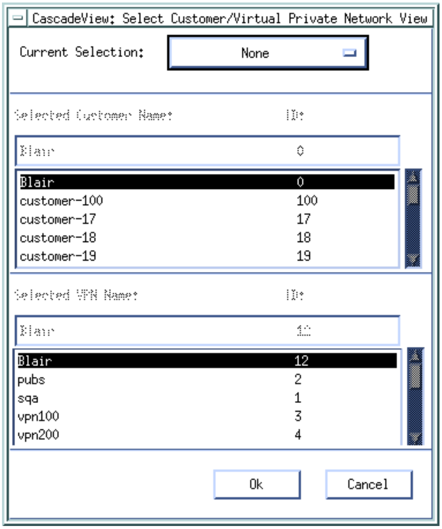


Figure 2-7. Select Customer/Virtual Private Network Dialog Box

2. Use the Current Selection button to select either Customer or VPN.

3. Depending on the option you select, review either the Selected Customer Name or Selected VPN Name list.

4. Select the Customer or VPN name.

5. Choose OK.

Monitoring VPN Networks

You can use the Show All Customer/VPN function to display all customers who are using a virtual private network and also to display all virtual private networks defined on a map.

To display all customers who have a VPN:

1. Select Show All Customer/VPN ... _ Show All Customers from the Monitor menu. The dialog box appears as shown in Figure 2-8.

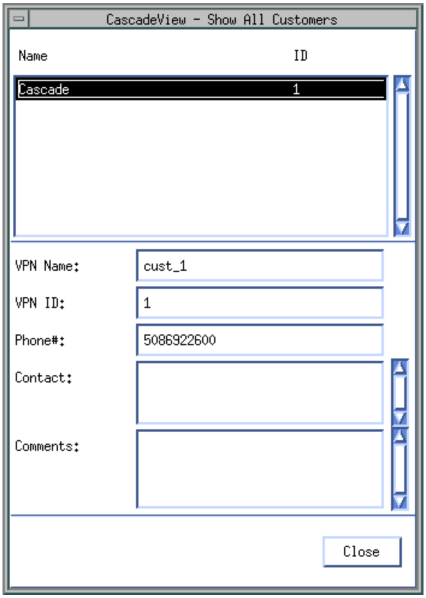


Figure 2-8. Show All Customers Dialog Box

2. From the list at the top of the dialog box, select the Customer Name. Table 2-8 describes each of the fields on the Show All Customers dialog box.

3. Choose Close to return to the network map.

Table 2-8. Show All Customers Fields

Field	Action/Description
Name	Displays the name of the customer using the VPN.
ID	Displays the ID associated with each customer.
VPN Name	Displays the name of the virtual private network (VPN) assigned to this customer.
VPN ID	Displays the ID of the VPN assigned to this customer.
Phone #	Displays the phone number of the contact person at the customer site.
Contact	Displays the name of the contact person at the customer site.
Comments	Displays any applicable comments.

Monitoring VPN Customers

You can use the Show All VPN function to display all virtual private networks defined on a map.

To display all virtual private networks:

1. Select Show All Customer/VPN ... _ Show All Virtual Private Network from the Monitor menu. The Show All Virtual Private Networks dialog box shown in Figure 2-9 appears.

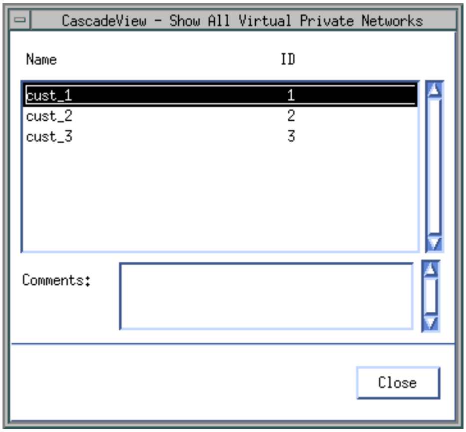


Figure 2-9. Show All Virtual Private Networks Dialog Box

2. From the list at the top of the dialog box, select the VPN name. Table 2-9 describes each of the fields on the Show All Virtual Private Networks dialog box.

3. Choose Close to return to the network map.

Table 2-9. Show All Virtual Private Networks Fields

Field	Action/Description
Name	Displays the name of the virtual private network (VPN).
ID	Displays the ID associated with each VPN.
Comments	Displays any applicable comments.

Reviewing the Status of SMDS Routes

The Show All SMDS Routes function displays all of the destination switches and whether or not a route is defined and the hop count for each route.

To display all SMDS routes:

1. From the Monitor menu, select Cascade Objects ⇒ Show Smds Routes.... The Show Smds Routes dialog box (Figure 2-10) appears, displaying a list of destination switch names along with a hop count if a route is defined.

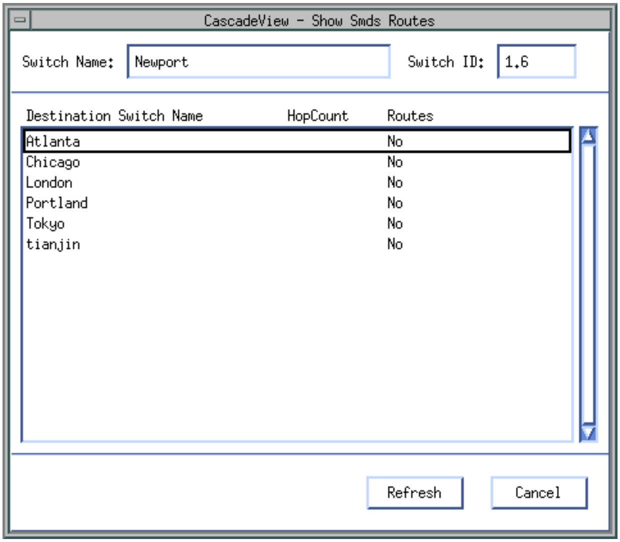


Figure 2-10. Show SMDS Routes Dialog Box

2. Choose Refresh to update the display.

3. Choose Cancel when you finish reviewing the information.

Table 2-10 describes the Show SMDS Routes dialog box fields.

Table 2-10. Show SMDS Routes Fields

Field	Action/Description
Switch Name	Displays the name of the currently selected switch.
Switch ID	Displays the ID for the selected switch.
Destination Switch Name	Displays the name of a destination switch.
HopCount	Displays the hop count for an SMDS route.
Routes	Displays either *Yes* or *No* to indicate if an SMDS route is defined.

3

Running Diagnostics

This chapter describes how to obtain node-level diagnostic information for a selected switch, as well as how to obtain Physical or Logical port-level diagnostic information. CascadeView/UX provides two different types of diagnostic programs:

Background Diagnostics — Background diagnostic programs constantly run in the background to monitor the network switches for potential failures or problems. Background diagnostics execute automatically and do not interfere with switch operations.

Foreground Diagnostics — Foreground diagnostic programs are user-initiated tests that enable you to perform a variety of loopback tests to verify the integrity of the physical and logical ports.

Background Diagnostics

The background diagnostics run continuously in background and provide a current status for all active switches. Background diagnostics are non-obtrusive, since the switch is completely functional while they run.

What Problems Can Background Diagnostics Detect?

The Background Diagnostics can alert you to the following types of problems on an active switch:

- Corruption of different data structures
- Corruption of code space
- Corruption of registers

The 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. Fatal errors that are not user-initiated should be documented and reported to the Technical Response Center by calling one of the following numbers:

In the United States and Canada
1-800-DIAL-WAN (1-800-342-5296)

Outside the U.S., Canada, and the United Kingdom
1-978-952-7299

In the United Kingdom
0-800-96-2229

You cannot resolve most fatal errors using the instructions in this manual. Report any fatal error (with the exception of Error Number 136) to the Technical Response Center.

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 traps alarms that you can view through the Events Browser. Refer to Chapter 10, “Trap Alarm Conditions” for more information about trap alarms.

Use the Background Diagnostics dialog box to display the Background Diagnostics information. The following section describes how to access the Background Diagnostics dialog box.

Accessing the Background Diagnostics Dialog Box

To access Background Diagnostics:

For an STDX 3000/6000

1. On the network map, select the switch icon for which you want to view diagnostic information.
2. From the Diagnose menu, select Cascade Objects: Background Diagnostics. The Background Diagnostics dialog box shown in Figure 3-2 appears.

For a B-STDX 8000/9000

1. On the network map, select the switch icon for which you want to view diagnostic information. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears. (Refer to Figure 1-6 on page 1-12 for an illustration of the Switch Back Panel dialog box.)
2. Select the I/O module, port, or control processor card for which you want to obtain background diagnostic information.
3. Choose Diagnose. The Select Card Diagnostic dialog box shown in Figure 3-1 appears.

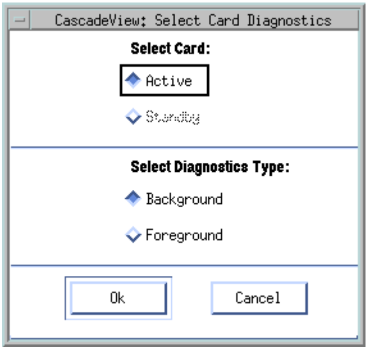


Figure 3-1. Select Card Diagnostic Dialog Box

4. Select either the Active or Standby card.

5. Select Background Diagnostics as the Diagnostics Type. The Background Diagnostics dialog box shown in Figure 3-2 appears.

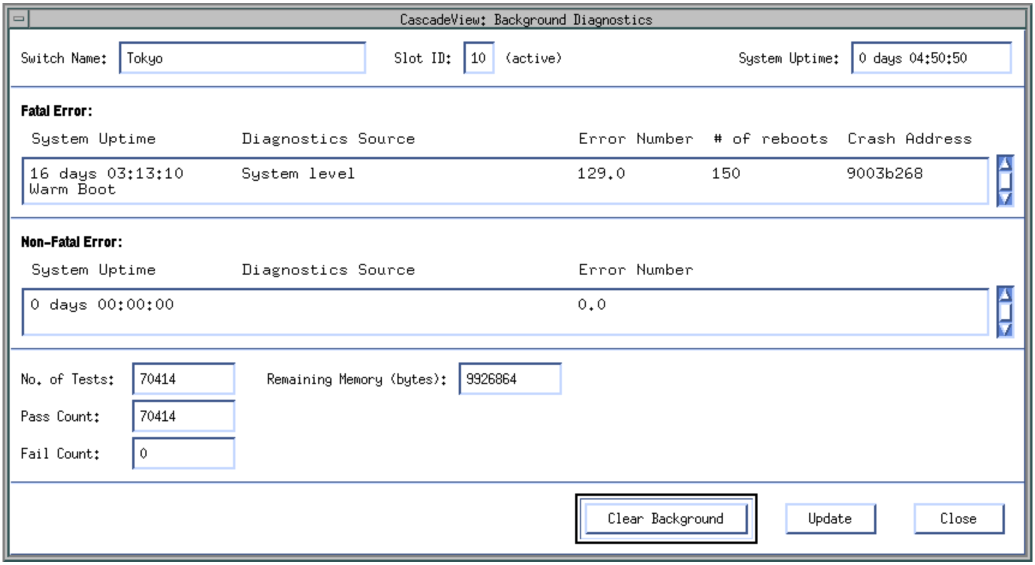


Figure 3-2. The CascadeView: Background Diagnostics Dialog Box

The Background Diagnostics dialog box displays both fatal and non-fatal errors. Table 3-1 describes the Background Diagnostics dialog box fields.

Table 3-1. Background Diagnostics Fields

Field	Action/Description
Switch Name	Displays the name of the switch for which you are viewing the diagnostic information.
Slot ID	Displays the I/O module slot ID and specifies whether the diagnostics are for the active or standby card.
System Uptime	Displays the amount of time, since the last reboot, that the switch has been active.
No. of Tests	Displays the number of tests that have occurred on the selected switch.
Pass Count	Displays the number of background diagnostic tests that have passed without error.
Fail Count	Displays 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)	Displays the amount of available heap memory on the selected card.

Table 3-1. Background Diagnostics Fields (Continued)

Field	Action/Description
Fatal Error	Displays the following information about those conditions that cause the switch to fail and reboot. *System Uptime* – Displays the SysUpTime value at the time that the error occurred. *Diagnostics Source* – Displays the source from which CascadeView/UX collected the error condition. Possible values include: • System level (Packet Processor/Control Processor) • Redundancy Manager • BD Heap (memory) • Power-on diagnostics • Background diagnostics • Fault *Error Number* – Displays the error number containing the major and minor error codes, in the format of X.Y (X being the major error number and Y is the minor error number). For example, error number 129.0 would indicate a major error code of 129 and a minor error code of 0. Table 3-2 lists and describes each of the error codes. *# of Reboots* – Displays the number of times that this switch experienced a reboot condition since the last logged fatal error. If the value in this field is greater than three, the information displayed in the Background Diagnostics dialog box is outdated. *Crash Address* – Displays a crash address that the Technical Response Center uses for debugging purposes. If the background diagnostics indicate a crash address, make a note of the address and contact the Technical Response Center.

Table 3-1. Background Diagnostics Fields (Continued)

Field	Action/Description
Non-Fatal Error	Displays the following information about those conditions that strain system resources. This information is the same as that described for a Fatal Error and includes the following: *System Uptime* – Displays the SysUpTime value at the time that the error occurred. *Diagnostic Source* – Displays the source from which CascadeView/UX collected the error condition. Possible values include: • System level (Packet Processor/Control Processor) • Redundancy Manager • BD Heap (memory) • Power-on diagnostics • Background diagnostics • Fault *Error Number* – Displays the error number containing the major and minor error codes, in the format of X.Y (X being the major error number and Y is the minor error number). For example, error number 144.0 would indicate a major error code of 144 and a minor error code of 0. Table 3-2 lists and describes each of the error codes.

6. Optionally, choose Clear Background to clear the information in the Background Diagnostics log. The system does not clear the screen after you choose the Clear Background option. However, the next time that you display the Background Diagnostics dialog box, a new set of Background Diagnostics displays. The Clear Background option is useful if you want to monitor certain Non-Fatal errors to verify whether or not the error is a persistent condition.

7. Choose Close to return to the network map.

Reboots that Do Not Update the Background Diagnostics Dialog Box

Although the *# of Reboots* counter increments with each reboot, there are instances where the hardware reboots or resets, but the information on this dialog is not updated. These instances include the following conditions:

- The switch is powered off and on.
- The hardware is reset. This could be a case where you have used the latch to reset a B-STDX 8000/9000.
- The CP card continuously polls I/O cards for status. If a card does not respond, the CP resets this card.

Summary of Error Codes

Use Table 3-2 as an error code reference. In this table an asterisk (*) shown after the Major Error Number indicates that additional information about the error is included in the 960 trace area. If any of these errors occur on your system, contact the Technical Response Center at one of the following numbers:

In the United States and Canada
1-800-DIAL-WAN (1-800-342-5296) 0

Outside the U.S., Canada, and the United Kingdom
1-978-952-7299

In the United Kingdom
0-800-96-2229

Table 3-2 also specifies those error numbers that indicate fatal error conditions. If you see an error code that indicates a fatal error condition, call the Technical Response Center. You cannot resolve fatal error conditions by using the instructions in this manual.

Table 3-2. Summary of Error Codes

Major Error	Minor Error	Error Type	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 control processor (CP). To **resolve,** configure the I/O slot and reinitialize the switch. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information about how to perform these tasks.
2 - 16	See Explanation	Non-Fatal	Link stall detection. Transmit completions stalled. This error occurs when the switch cannot transmit a frame 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. Specify the clock configuration if there is no clock present. Refer to the Network Configuration Guide for B-STDX/STDX for more information about how to perform these tasks.
3.2	0	Fatal	This error only occurs on a CP card and indicates a warm boot. Although this is a fatal message, no intervention is required.
4	0	Fatal	Chain corruption in a memory block. This is a fatal error that you cannot resolve without assistance. Call the Technical Response Center.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
5	0	Fatal	Fatal error. Call the Technical Response Center.
11	0	Fatal	The hardware has detected an error on the bus. Call the Technical Response Center.
17	See Explanation	Non-Fatal	Received checksum errors over the bus on control data. Checksum errors are cell level errors that test the software. The **minor error** number indicates the total number of errors. For example, an error code of 17.205 indicates that the system detected 205 checksum errors. It is possible that the insertion of a card could cause this condition. **To resolve,** monitor the problem to see if this condition persists. If it does, contact the Technical Response Center. The error may need to be isolated in order to determine if hardware replacement of some component is necessary.
18	See Explanation	Non-Fatal	Received parity errors on bus receive. Parity errors are byte level errors that test the hardware. The **minor error number** indicates the total number of errors. For example, an error code of 18.150 indicates that the system detected 150 parity errors. **To resolve**, monitor the problem to see if this condition persists. If it does, contact the Technical Response Center. The error may need to be isolated in order to determine if hardware replacement of some component is necessary.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
20*	0	Fatal	Interrupt vectors corrupted. Call the Technical Response Center.
21*	See Explanation	Fatal	960 SRAM corrupted. The **minor error number** is the pointer to the bad SRAM location. Call the Technical Response Center.
22*	0	Fatal	Fault table corrupted. Call the Technical Response Center.
23	0	Fatal	Interrupts disabled. Call the Technical Response Center.
24	1	Fatal	Processor kernel *force bad parity* bit is on. Call the Technical Response Center.
24	2	Fatal	IOP *force bad parity* bit is on. Call the Technical Response Center.
25	0	Fatal	OS counter/timer is disabled. Call the Technical Response Center.
26*	See Explanation	Fatal	Stack overflowed. The **minor error number** specifies the ID of the corrupted stack. Call the Technical Response Center.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
27	1	Non-Fatal	Bus transmits stalled – no transmits sent in the last 90 seconds. This condition occurs if the queue has not advanced over the last 90 seconds (therefore, no data was transmitted in the last 90 seconds). This condition can occur if the CP is pulled from the system or if clocking on the bus has stopped. **To resolve,** use the foreground diagnostics to perform a loopback to determine the cause of the problem. Refer to Chapter 4, "Loopbacks" for more information.
27	2	Non-Fatal	Bus transmits full – hardware owns all of the bus transmit descriptors. This condition occurs if the CP is pulled from the system or if the hardware overflow queue fills up and is wrapped around. The yellow indicator light for the card will be lit for 90 seconds and then the operational green indicator light will be lit. **To resolve**, call the Technical Response Center.
30*	2	Fatal	Heap error — an invalid heap header occurred when freeing a block of memory. Call the Technical Response Center.
30*	3	Fatal	Heap error — out of memory on allocate. Call the Technical Response Center.
30	4	Fatal	Heap error — heap memory corrupted. Call the Technical Response Center.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
31	1	Non-Fatal	PRAM initialized. This error is caused by resetting the PRAM. **To resolve**, resynchronize the PRAM in the card. Refer to the Network Configuration Guide for B-STDX/STDX for more information.
31	2	Non-Fatal	PRAM corrupted — header. **To resolve**, resynchronize the PRAM in the card. Refer to the Network Configuration Guide for B-STDX/STDX for more information.
31	3	Non-Fatal	The PRAM is corrupted in bank 0. **To resolve**, resynchronize the PRAM in the card. Refer to the Network Configuration Guide for B-STDX/STDX for more information.
31	4	Non-Fatal	The PRAM is corrupted in bank 1. **To resolve**, resynchronize the PRAM in the card. Refer to the Network Configuration Guide for B-STDX/STDX for more information.
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. Refer to the Network Configuration Guide for B-STDX/STDX for more information.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
32	0	Fatal	SRAM code space corrupted. Call the Technical Response Center.
33	0	Fatal	IRAM code space corrupted. Call the Technical Response Center.
34*	0	Fatal	960 fault 0. Call the Technical Response Center.
35*	0	Fatal	960 fault 1. Call the Technical Response Center.
36*	0	Fatal	960 fault 2. Call the Technical Response Center.
37*	0	Fatal	960 fault 3. Call the Technical Response Center.
38*	0	Fatal	960 fault 4. Call the Technical Response Center.
39*	0	Fatal	960 fault 5. Call the Technical Response Center.
40*	0	Fatal	960 fault 6. Call the Technical Response Center.
41*	0	Fatal	960 fault 7. Call the Technical Response Center.
42*	0	Fatal	960 fault 8. Call the Technical Response Center.
43*	0	Fatal	960 fault 9. Call the Technical Response Center.
44*	0	Fatal	960 fault 10. Call the Technical Response Center.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
45*	0	Fatal	Bus Error (3000/6000). Call the Technical Response Center.
46	0	Fatal	Parity Error — IRAM (3000/6000). Call the Technical Response Center.
47	0	Fatal	Parity Error — FMEM (3000/6000). Call the Technical Response Center.
48	0	Fatal	FMEM self test failure. Call the Technical Response Center.
49	0	Fatal	Initialization Error — device tables (3000/6000). Call the Technical Response Center.
50	0	Fatal	Initialization Error — bd out heap (3000/6000). Call the Technical Response Center.
51	0	Fatal	Initialization Error — bd in heap (3000/6000). Call the Technical Response Center.
52	0	Fatal	Initialization Error — bd initialization (3000/6000). Call the Technical Response Center.
55	0	Fatal	Ethernet Driver Error. Call the Technical Response Center.
56	0	Fatal	Obsolete
57	0	Fatal	Obsolete
58	0	Fatal	Circular virtual circuit list on the rate enforcement queue. Call the Technical Response Center.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
59	0	Fatal	Obsolete
128	0	Fatal	Cannot download bus. Call the Technical Response Center.
129	0	Fatal	Warm boot. Call the Technical Response Center.
130	0	Fatal	Cold boot. Call the Technical Response Center.
131	0	Fatal	Cannot download T1 xlinx. Call the Technical Response Center.
132	0	Fatal	The passive side of a redundant card pair is shooting the active side. Call the Technical Response Center.
133	0	Non-Fatal	The PRAM is in conflict; PRAM is configured for another node. Each node has a unique ID. A card that was configured for one switch is now in use in a different switch. **To resolve**, resynchronize the PRAM in the card. Refer to the Network Configuration Guide for B-STDX/STDX for more information.
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**, you can reactivate the card by setting the Admin Status field to Up. The Admin Status field can be set on the Modify Logical Port dialog box.
135	0	Non-Fatal	Unused.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
136	0	Fatal	NMS caused a redundant switchover. This is a normal procedure that the NMS calls for.
137	See Explanation	Fatal	Illegal interrupt vector. This condition could be caused by either a software or hardware anomaly. The **minor error number** specifies the vector code. Call the Technical Response Center.
138	0	Fatal	Proxy message from the wrong card. Call the Technical Response Center.
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 interruption in service. However, if you have to switch to the standby card, the older software revision may not support some features that you are using on the active card. **To resolve**, update the standby card with the new software at your earliest convenience.
145	0	Fatal	IOP configured for MULTI. Call the Technical Response Center.
146	0	Fatal	Card service change. Call the Technical Response Center.
147	0	Fatal	Some I/O to PRAM failed. Call the Technical Response Center.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
148	0	Fatal	One of the CPs in a redundant pair of CPs is incapable of the requested admin capability. Call the Technical Response Center.
149	0	Non-Fatal	A standby CP card type is incapable of a requested admin capability. This error code indicates that the standby CP type does not match the active CP type. This is a warning condition and will not cause an interruption in service. However, if you have to switch to the standby CP type, the older version may not support some features that you are using on the active CP type. **To resolve**, replace the standby CP card type so that it matches the active CP type at your earliest convenience.
149	1	Non-Fatal	A standby CP card type is incapable of a requested admin capability, however, the system allowed the admin change to be made. This is a warning condition and will not cause an interrupt in service. However, if you have to switch to the standby CP card type, the older version may not support some features that you are using on the active card type. **To resolve**, replace the standby CP card type so that it matches the active CP type at your earliest convenience.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
149	2	Non-Fatal	A standby CP 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 interruption in service. However, if you have to switch to the standby CP card type, the older version may not support some features that you are using on the active card type. **To resolve**, replace the standby CP card type so that it matches the active CP type at your earliest convenience.
149	3	Non-Fatal	The active IOP card 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 card with the correct card type.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
149	4	Non-Fatal	The standby IOP card cannot perform a requested operation capability. For example, an SMDS request could have been made for a card that is for Frame Relay only. This condition is a warning condition and will not cause an interruption in service. However, if you have to switch to the standby IOP card, the older version may not support some features that you are using on the active card. **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 Technical Response Center.
150	2	Fatal	OSPF error — No LSA in the age bin. Call the Technical Response Center.
150	3	Fatal	OSPF error — Link State (LS) database is corrupted. Call the Technical Response Center.
150	4	Fatal	OSPF error — Bad LSA in NBR queue. Call the Technical Response Center.
150	5	Fatal	OSPF error — Bad LSA in NBR2 queue. Call the Technical Response Center.
150	6	Fatal	OSPF error — LSA not found. Call the Technical Response Center.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
150	7	Fatal	OSPF error — NBR not found. Call the Technical Response Center.
150	8	Fatal	OSPF error — Error in timer queue. Call the Technical Response Center.
150	9	Fatal	OSPF error — Bad LSA in send Link State Uppath (LSU). Call the Technical Response Center.
150	10	Fatal	OSPF error — Duplicate Autonomous System Entry (ASE). Call the Technical Response Center.
150	11	Fatal	OSPF error — No areas. Call the Technical Response Center.
150	12	Fatal	OSPF error — Bad VL. Call the Technical Response Center.
150	13	Fatal	OSPF error — No BB Ifs. Call the Technical Response Center.
150	14	Fatal	OSPF error — No BB. Call the Technical Response Center.
150	15	Fatal	OSPF error — No memory. Call the Technical Response Center.
150	16	Fatal	OSPF error — Bad receive packet. Call the Technical Response Center.
151	1	Fatal	OSPF error — Console logging errors. Call the Technical Response Center.
152	0	Fatal	Permanent Virtual Circuit (PVC) manager errors. Call the Technical Response Center.

Table 3-2. Summary of Error Codes (Continued)

Major Error	Minor Error	Error Type	Explanation
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. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information about how to configure PVCs.

Foreground Diagnostics

Foreground diagnostics enable you to perform a variety of different loopback tests on an I/O card, a physical port, a T1 or E1 logical port, or a channel on a Channelized DS3 module. You use foreground diagnostics to verify that new equipment functions properly, or to test equipment that is not providing optimal performance.

What Problems Can Foreground Diagnostics Detect

Foreground diagnostics provide non-fatal error information and enable you to:

- Verify whether or not an I/O card, physical port, T1 or E1 logical port, or DS3 channel is transmitting data properly at the physical level
- Isolate the cause of a transmission stall error (error codes 27.1 and 27.2)

The following foreground diagnostic test options are available depending on the component that you are testing:

Internal — Tests the I/O card hardware only. You can use this test on all cards. The purpose of the test is to check the internal hardware of a specific physical port. The port must have the Admin Status set to down before you can perform an internal test.

External — Performs an external test that enables you to direct signals back towards the source along a communications path to test the ability of the port to send and receive data. This test requires an external loopback connector, which you install on the physical port that you are testing.

> *The following three tests are for HSSI ports only. These loopbacks are initiated by the DTE through the HSSI LA/LB interface signals. The 9000 HSSI drives these signals when you initiate the loopback from the NMS.*

External **Local DTE** (HSSI ports only) — Sends a signal to the DSU to indicate that the DTE (9000) is performing a loopack test on the HSSI interface.

External Local Line (HSSI ports only) — Sends a signal to the DSU to indicate that the DTE (9000) is performing a loopback test on the DSU DS3 interface.

External Remote Line (HSSI ports only) — Sends a signal to the DSU to indicate that the DTE (9000) is performing a loopback test on the DSU DS3 interface.

DS0 Near End Loopback — Tests the following B-STDX 8000/9000 logical ports: **Channelized T1, 4-port ISDN PRI, 4-port DSX**. This test enables you to test the physical path for data transmission, by looping back traffic from the OCU, CSU, or DSU in one or both directions. You can initiate a DS0 loopback over one or more contiguous DS0 channels of a logical port.

DS0 Far End Loopback — Tests the following B-STDX 8000/9000 logical ports: **Channelized T1, 4-port ISDN PRI, 4-port DSX**. Use the DS0 Far End Loopback option to test the physical path for data transmission by looping traffic from the switch to the OCU, CSU, or DSU and back to the originating switch.

Near End Line Loopback — Tests the following B-STDX 8000/9000 physical ports: **4-port T1, 10-port DSX, channelized DS3**. This type of test enables you to initiate a near-end line loopback and display the current status of each DS1 near-end line loopback. Refer to Chapter 4, "Loopbacks" for detailed information about loopback tests.

DS3 Far End Loopback — For ATM DS3 physical ports only. Enables you to initiate a DS3 far-end loopback test for a single-port ATM DS3 module. Refer to Chapter 4, "Loopbacks" for detailed information.

DS1 Far End Loopback — For Channelized DS3 physical ports only. Enables you to initiate a DS1 far-end loopback. Refer to Chapter 4, "Loopbacks" for detailed information.

DS1 Near End Diag Loopback — For Channelized DS3 modules only. Enables you to display the current status of each DS1 near-end diagnostic loopback. Refer to Chapter 4, "Loopbacks" for detailed information.

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

Displaying Foreground Diagnostics

The process of displaying Foreground Diagnostics is a two-step procedure in which you must:

1. Disable the card, physical port, or logical port by setting the Admin Status to Down.

2. Display the Foreground diagnostics dialog box.

The following sections describe these two procedures.

Setting the Admin Status to Down

The instructions for setting the Admin Status to Down differ depending on whether you are using the foreground diagnostics to test an I/O card, physical port, T1 or E1 logical port, or a channel. The following section describes the steps for each component.

Changing a Physical Port's Admin Status

1. From the Administer menu, choose Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears (Figure 1-6 on page 1-12).

2. Double-click on the specific port you need to modify. The Set Physical Port Attributes dialog box appears as shown in the example in Figure 3-3.

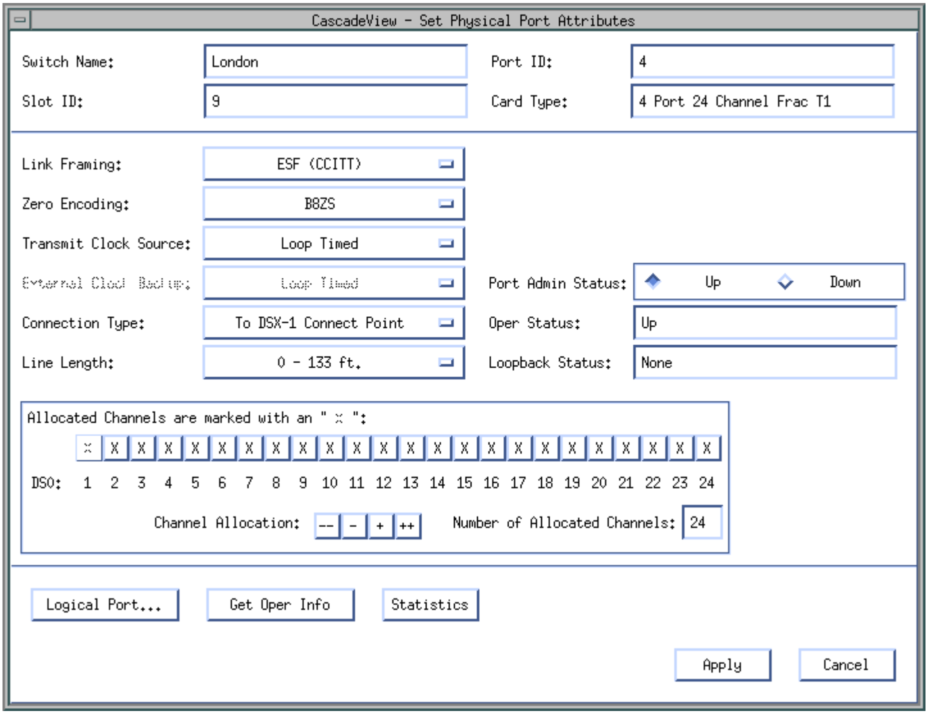


Figure 3-3. Set Physical Port Attributes Dialog Box

3. Change the Admin Status to Down.

4. If the Clock Source Selection on the Set Physical Port Attributes dialog box is set to DTE, change this field temporarily to DCE. If the Clock Source Selection is set to Loop Timed, change this field temporarily to Internal.

> *The Foreground Diagnostic tests require that the physical port provide clocking. Make sure that this field is* ***not*** *set to DTE or Loop Timed.*

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, choose Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears (Figure 1-6 on page 1-12).
2. Double-click on the specific logical port you need to modify. The Set Physical Port Attributes dialog box appears (Figure 3-3).
3. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears (Figure 3-4).

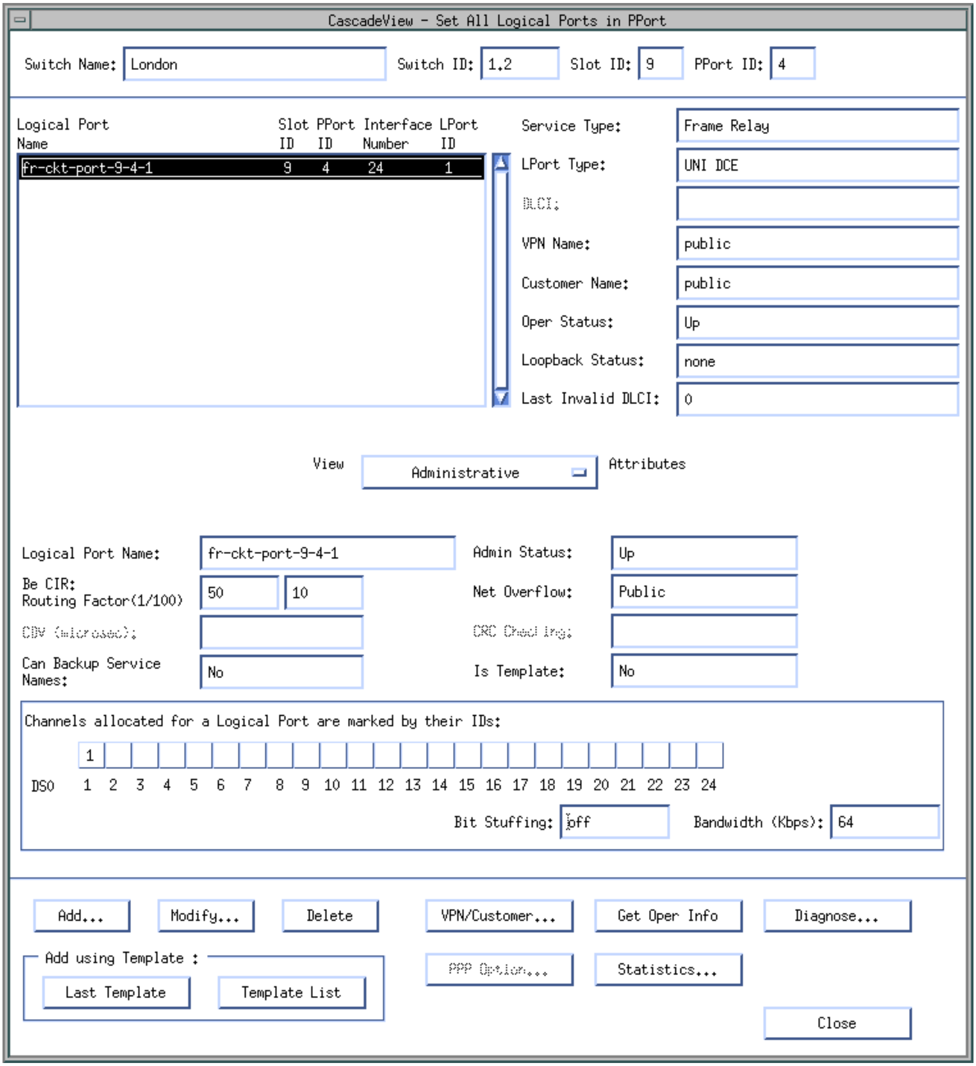


Figure 3-4. Set all Logical Ports in PPort Dialog Box

4. Select a logical port and choose Modify. The system then displays the first of two Modify Logical Port dialog boxes.

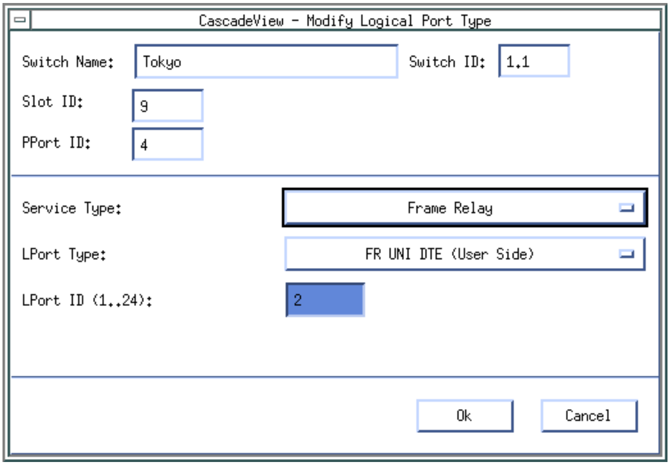


Figure 3-5. Modify Logical Port - Screen 1

5. Choose OK. The system displays the second Modify Logical Port dialog box (Figure 3-6).

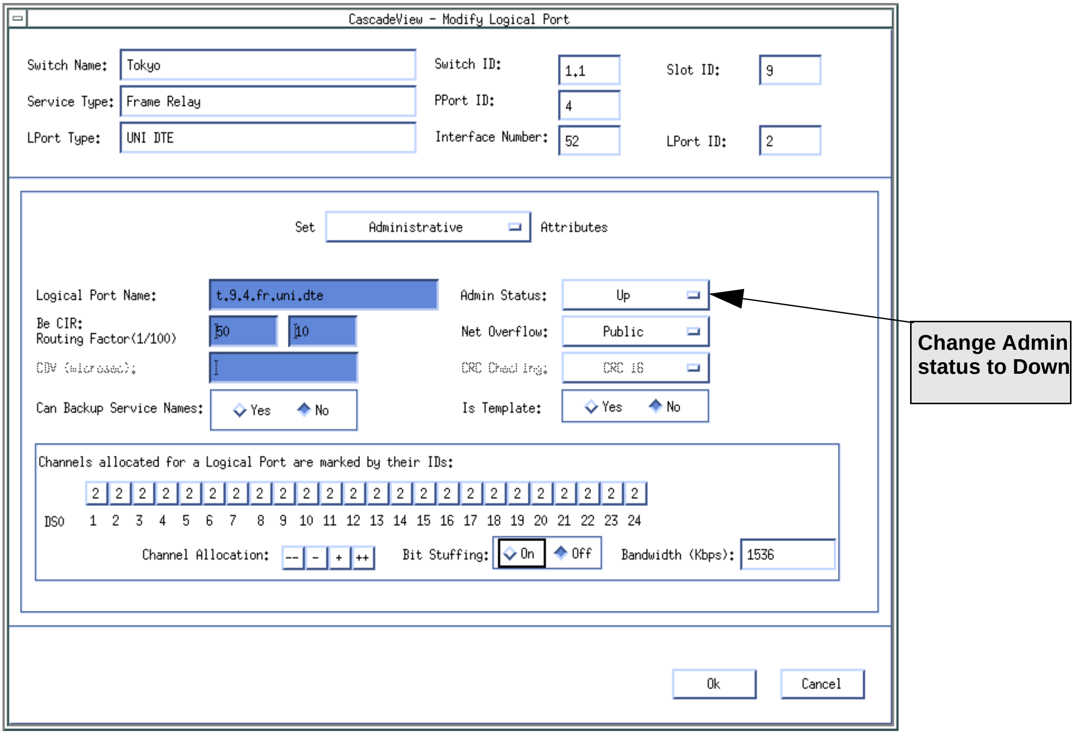


Figure 3-6. Modify Logical Port Dialog Box - Screen 2

6. Change the value in the Admin Status field from Up to Down to disable the logical port.
7. Choose OK. The system then displays a confirmation message.
8. Choose OK to save your changes. The system returns to the Set All Logical Ports in PPort dialog box.

Changing a Channel's Admin Status

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

2. Double-click on the specific port you need to disable. The Set Physical Port Attributes dialog box appears as shown in Figure 3-3 on page 3-27.

3. Double-click the channel that you need to disable. The Set Channel Attributes dialog box appears as shown in Figure 3-7.

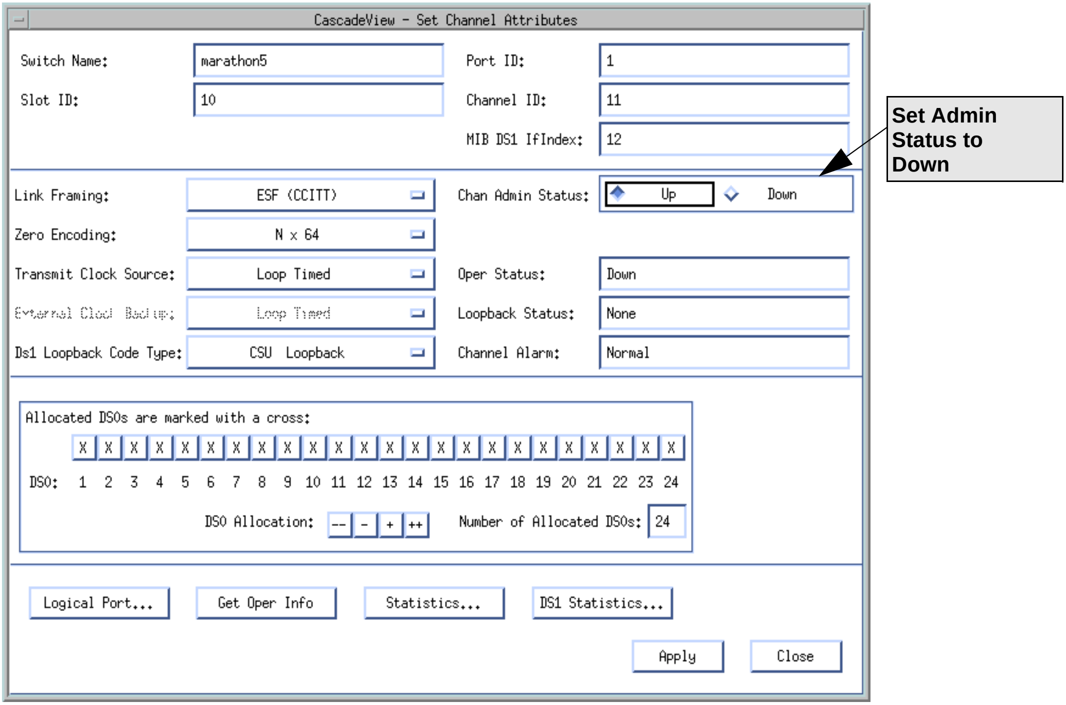


Figure 3-7. Set Channel Attributes Dialog Box

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 an I/O Card's Admin Status

1. From the Administer menu, choose Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears as shown in Figure 1-6 on page 1-12.
2. Change the Admin Status for all physical ports to Down. Refer to "Changing a Physical Port's Admin Status" on page 3-26 for more information.
3. Change the Admin Status for all logical ports to Down. Refer to "Changing a Logical Port's Admin Status" on page 3-28 for more information.
4. Select the card from the Switch Back Panel dialog box. The system then displays the Set Card Attributes dialog box.
5. Change the value in the Admin Status field from Up to Down to disable the card.
6. Choose OK. The system displays a confirmation message.
7. Choose OK to save your changes. The system returns to the Switch Back Panel dialog box.

Displaying the Foreground Diagnostics Dialog Box

After you set the Admin Status of the card, physical port, logical port, or channel to down, you can display foreground diagnostics.

To run foreground diagnostics:

1. On the network map, select the switch from which you want to obtain physical and logical port diagnostic information.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears as shown in Figure 1-6 on page 1-12.
3. Select the I/O card, physical port, logical port, or channel you want to test. Follow the instructions in the following sections according to the type of test you need to use.

Testing an I/O Module

1. Click the mouse once on the specific I/O module, then choose Diagnose from the Switch Back Panel dialog box. The Select Card Diagnostic dialog box appears (*B-STDX 8000/9000 only*), enabling you to select either the active or standby card.
2. Choose Foreground Diagnostics. The Perform Foreground Diagnostic Test dialog box appears as shown in Figure 3-8.

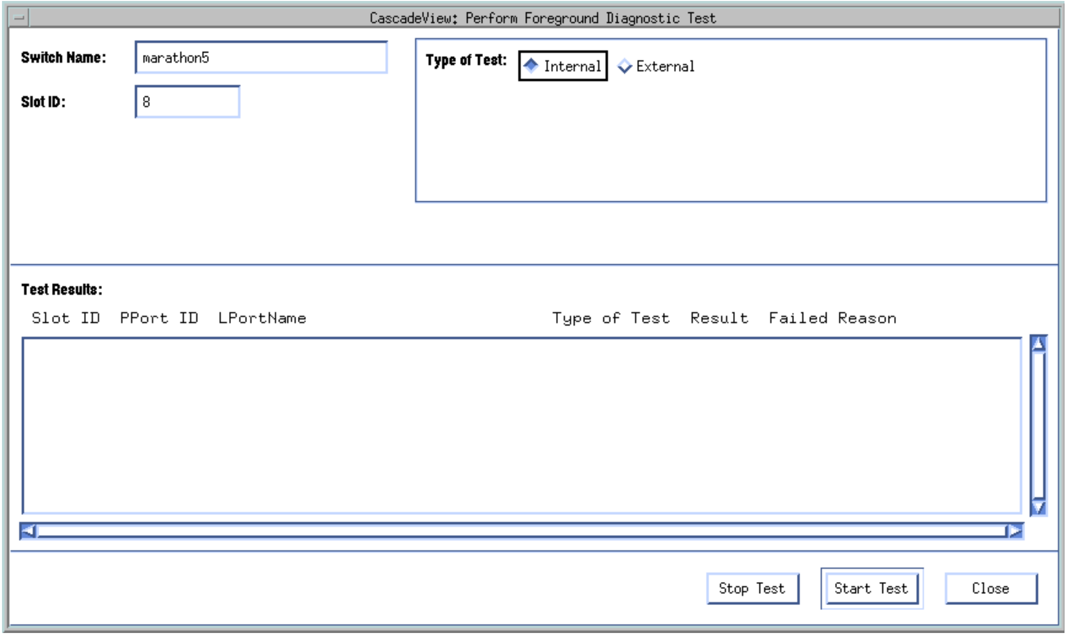


Figure 3-8. Perform Foreground Diagnostic Test (I/O Module) Dialog Box

3. Select the type of test you want to perform. The options that the system displays are dependent on the type of physical port that you are testing. You can perform any one of the following types of tests:

   Internal — Tests the I/O card hardware only. You can use this test on all cards. The purpose of the test is to check the internal hardware of a specific physical port. The internal test does not require an external loopback connector, however, the port's Admin Status must be set to Down.

   External — Tests the physical port's ability to send and receive data.

4. Choose Start Test to start a test traffic pattern. Test results appear in the Test Results portion of the dialog box.

5. Choose Stop Test to stop test pattern generation.

6. Choose Close to return to the Switch Back Panel window.

Testing a Physical Port

To perform a foreground diagnostic test on a physical port:

1. Click the mouse once on the specific physical port and then choose Diagnose. The Perform Foreground Diagnostic Test dialog box appears (Figure 3-9).

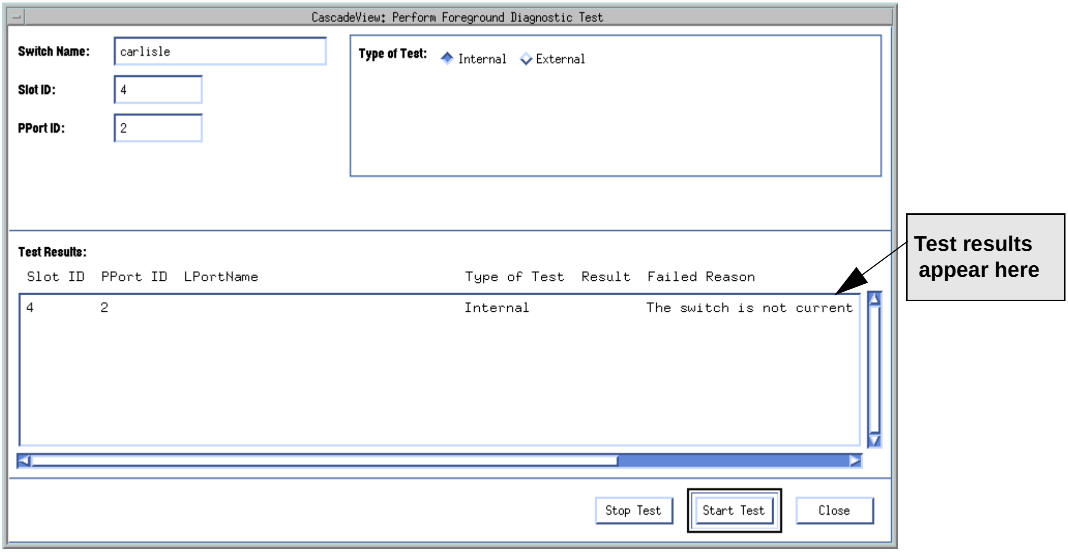


Figure 3-9. Perform Foreground Diagnostic Test (Physical Port) Dialog Box

2. Select the type of test you want to perform. The options that the system displays are dependent on the type of physical port that you are testing. You can perform any one of the following types of tests:

   Internal — Tests the I/O card hardware only. You can use this test on all cards. The purpose of the test is to check the internal hardware of a specific physical port. The internal test does not require an external loopback connector; however, the port's Admin Status must be set to Down.

   External — This option 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 you are testing.

Loopback — A variety of different loopback tests are available depending on the type of physical port you are testing. Refer to Chapter 4, "Loopbacks" for details.

3. Choose Start Test to start a test traffic pattern. Test results appear in the Test Results portion of the dialog box.

4. Choose Stop Test to stop test pattern generation.

5. Choose Close to return to the Switch Back Panel window.

Testing a Logical Port

To perform a foreground diagnostic test on a physical port.

1. Click the mouse once on the physical port. The Set All Physical Port Attributes dialog box appears.

2. Choose Logical Port. The Set Logical Ports dialog box appears.

3. Choose Diagnose. The Perform Foreground Diagnostic dialog box appears for the logical port.

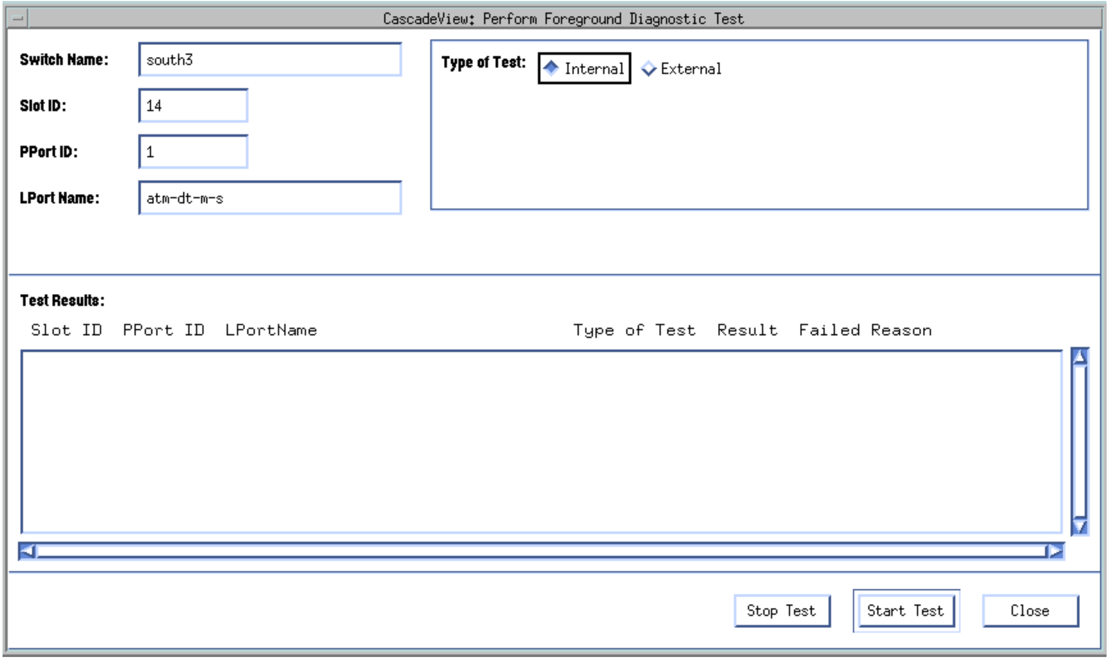


Figure 3-10. Perform Foreground Diagnostics Test (Logical Port) Dialog Box

4. Select the type of test you want to perform. The options that the system displays are dependent on the type of logical port that you are testing.

You can perform any one of the following types of tests:

Internal — Performs an external test on channelized T1 and E1 logical ports. This option 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 you are testing.

> *You can also install the external loopback connector on an external device such as a DSU or router.*

External — This option 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 you are testing.

Loopback — A variety of different loopback tests are available. Refer to Chapter 4, "Loopbacks" for details.

5. Choose Start Test to start a test traffic pattern.
6. Choose Stop Test button stop test pattern generation.

Testing a Channel

To perform a channel foreground diagnostic test on a Channelized DS3 module:

1. Select Set Attr from the Switch Back Panel dialog box (see Figure 1-6 on page 1-12). The Set Physical Port Attributes dialog box appears.

2. Click the mouse once on the specific channel and choose Diagnose. The Perform Foreground Channel Diagnostic Test dialog box appears as shown in Figure 3-11. Select one of the following channel diagnostic tests:

   - DS1 Near End Loopback

   - DS1 Far End Loopback

   - BERT

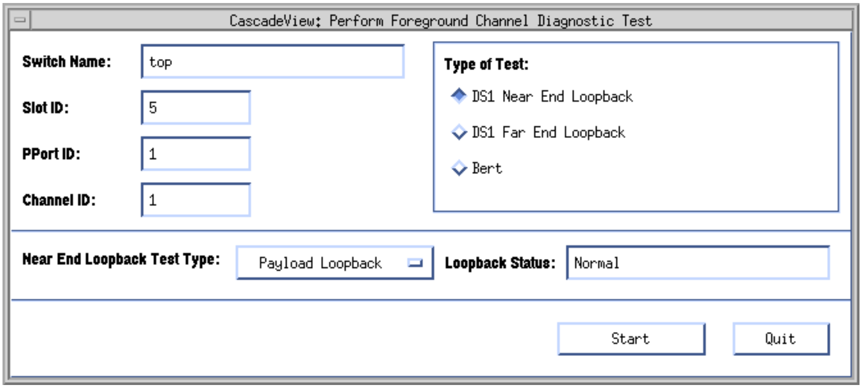


Figure 3-11. Perform Foreground Channel Diagnostic Test Dialog Box

Refer to Chapter 4, “Loopbacks” for more information on loopback testing.

4

Loopbacks

Loopback is an off-line maintenance function that enables you to:

- Measure the difference between a send and a receive signal
- Verify data across a PVC, logical port, or channel by looping back all data frames to a specified endpoint.
- Collect statistics for a physical port link over an extended period of time.

This chapter describes how to set and monitor the following loopback tests:

DS1 loopbacks for 4-port T1 and 10-port DSX — Tests the transmission path of an entire DS1 of a physical port.

DS1 loopbacks for Channelized DS3 — Tests the transmission path of a specific DS1 channel.

DS3 loopbacks for ATM DS3 and Channelized DS3 — Tests the DS3 physical port.

DS0 loopbacks for Channelized T1, 4-port ISDN PRI, and 4-port DSX — Tests the transmission path of a logical port.

PVC loopbacks — Tests the transmission path of a circuit.

DS1 Loopback for 4-Port T1 and 10-Port DSX

When you initiate a DS1 line or payload loopback for a 4-port T1 or 10-port DSX module, the entire DS1 of the physical port is put into the loopback from the near-end. When you initiate a DS1 Framed Line, Unframed Line, ESF FDL Line, or ESF FDL Payload loopback, the entire DS1 of the physical port is put into the loopback from the far-end.

You can generate and receive the following types of loopback code from the physical port of a 4-port T1 or 10-port DSX module:

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.

Line — A near-end loopback that operates upon receipt of specific framed pulse patterns. The line loopback pulse codes and functions are either Activate or Deactivate.

Framed inband line — A far-end loopback that sets/clears line loopback code at the far-end DS1 interface by sending loopback code via T1 frames.

Unframed inband line — A far-end loopback that sets/clears line loopback code at a far-end DS1 interface by sending loopback code via unframed bit code.

ESF FDL line (ANSI) — A far-end loopback that transmits the loopback signal by using ESF data-link messages (out-of-band).

ESF FDL payload (ANSI) — When an ESF FDL payload loopback is activated, the received information bits are transmitted in the outgoing direction (out-of-band).

DS1 Loopback Traps

The NMS generates a trap when a DS1 interface changes its loopback state. For more information about the type of trap that the NMS generates refer to Chapter 10, “Trap Alarm Conditions”.

Network Response to a DS1 Loopback

The following list outlines the network’s response to a DS1 loopback.

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

1. The DS1 port receives a line or payload DS1 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 a status of Down.
5. A trap is issued to the NMS indicating the change in loopback status.
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 DS1 Loopback

To activate and end a DS1 loopback on a 4-port T1 or 10-port DSX module:

1. On the network map, select the switch from which you want to obtain physical port diagnostic information. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears.
2. 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.
3. Disable the physical port for use during the loopback. Use the following steps to do this:
    a. Change the Port Admin Status value from Up to Down.
    b. Choose Apply. The system then prompts you to confirm the Port Admin Status value change.
    c. Choose OK.
    d. Choose Close. The system then redisplays the Set Switch Back Panel dialog box.
4. Choose Diagnose. The Perform Foreground Diagnostic Test dialog box appears as shown in Figure 4-1.

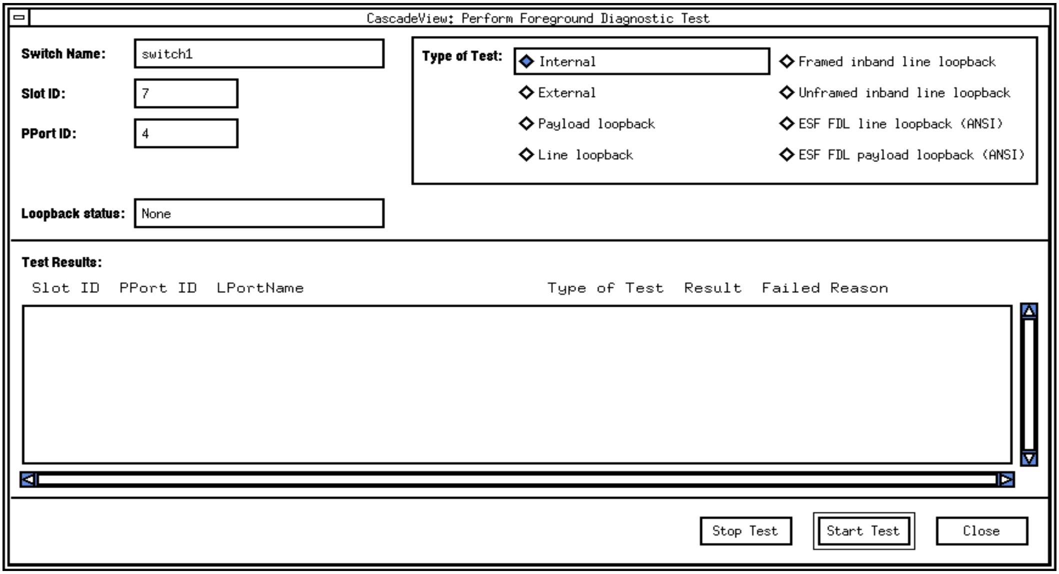


Figure 4-1. Setting a DS1 Loopback

5. Select one of the following values to indicate the type of loopback test that you want to generate:
   - Payload loopback
   - Line loopback
   - Framed inband line loopback
   - Unframed inband line loopback
   - ESF FDL line loopback (ANSI)
   - ESF FDL payload loopback (ANSI)

6. Choose Start Test to start a selected DS1 loopback test. The system displays the test results at the bottom of the Perform Foreground Diagnostic Test dialog box.

> *If you are performing a framed inband line loopback or an unframed inband line loopback, you can test the loopback by selecting External as the Type of Test after you choose Start Test (Step 6). You should then press Start Test again to display the test results at the bottom of the Perform Foreground Diagnostic Test dialog box. Choose Stop Test to disable the External Test.*

7. Choose Stop Test to disable the selected DS1 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.*

DS1 Loopback Tests for Channelized DS3

The DS1 loopback option for channelized DS3 modules enables you to test the transmission path of a specific DS1 channel. You can generate the following types of loopback tests:

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

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

Near-end Loopback Tests

The 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 and does not require a CSU/DSU. Figure 4-3 illustrates a DS1 near-end diag loopback.

Figure 4-2 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.

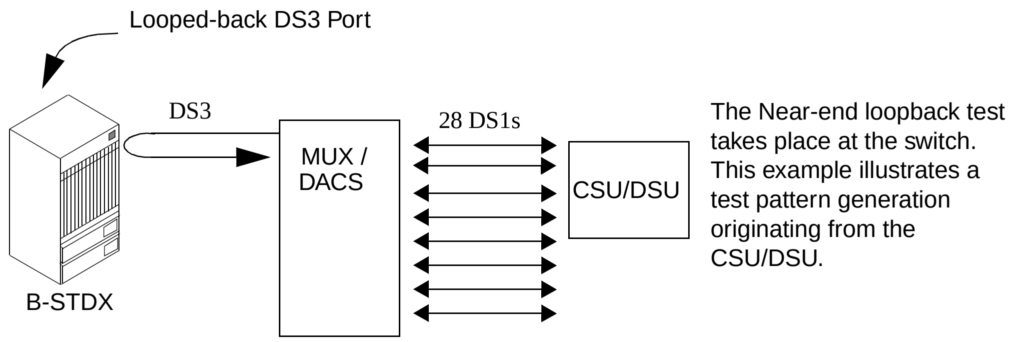


Figure 4-2. Near-end Loopback

Figure 4-3 illustrates a 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.

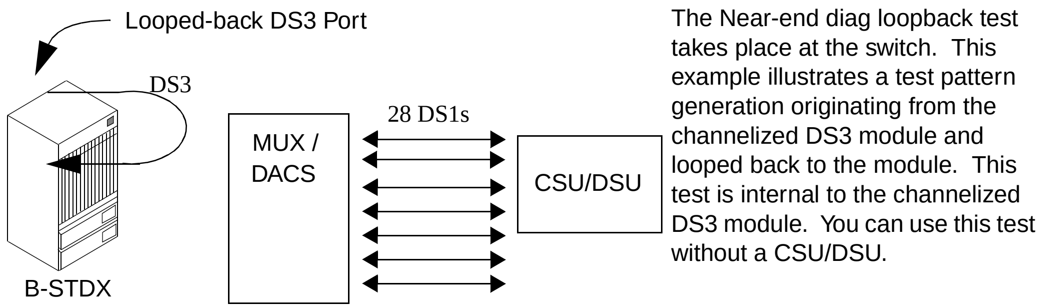


Figure 4-3. Near-end Diag Loopback

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 4-1 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 4-1. Far-end Loopback Tests

Loopback Test	Function/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 Network Interface (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 Network Interface (NI); returns information to the switch on the receive line.

Table 4-1. Far-end Loopback Tests (Continued)

Loopback Test	Function/Description
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 4-4 illustrates a far-end CSU/DSU loopback that takes place at the CSU/DSU.

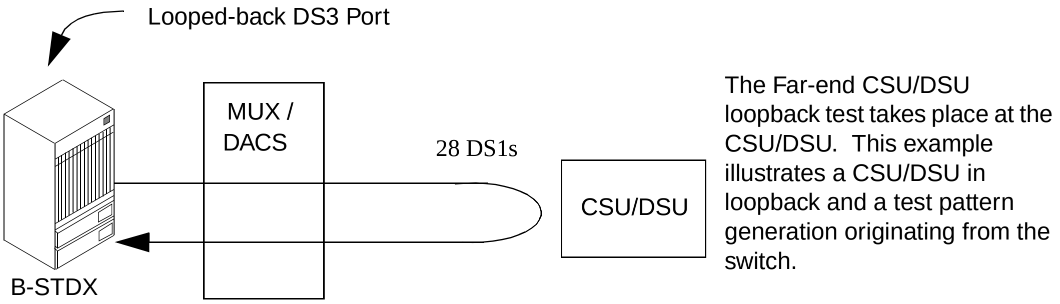


Figure 4-4. DS1 Far-end CSU / DSU Loopback

Figure 4-5 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.

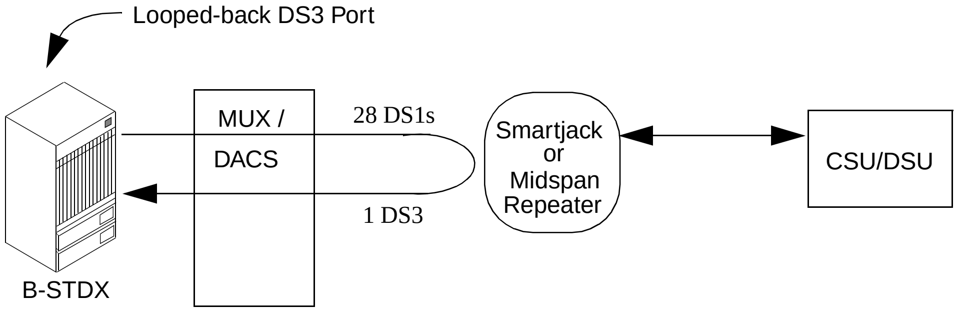


Figure 4-5. DS1 Far-end NI Loopback

Starting and Ending a DS1 Loopback Test

To start and end a DS1 loopback on a channelized DS3 module:

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

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

3. Select the physical port that you want to test by double-clicking on the physical port. The Set Physical Port Attributes dialog box appears as shown in Figure 4-6.

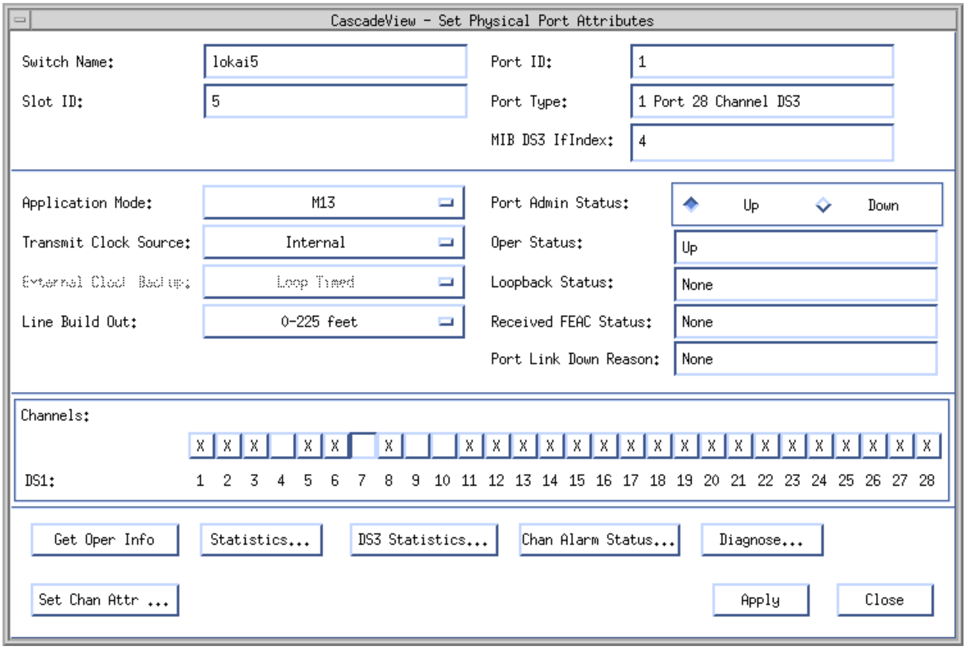


Figure 4-6. Set Physical Port Attributes Dialog Box

4. Select a DS1 channel that you want to test by clicking twice on the channel button ID or select a channel and choose Set Chan Attr. The Set Channel Attributes dialog box appears.

5. Disable the channel for use during the loopback test by changing the Channel Admin Status value from Up to Down.

6. Choose Apply.

7. Choose Close.

   The system then redisplays the Set Physical Port Attributes dialog box (see Figure 4-6).

8. Verify the channel you want to test is highlighted.

9. Choose Diagnose. The Perform Foreground Channel Diagnostic Test dialog box appears as shown in Figure 4-7.

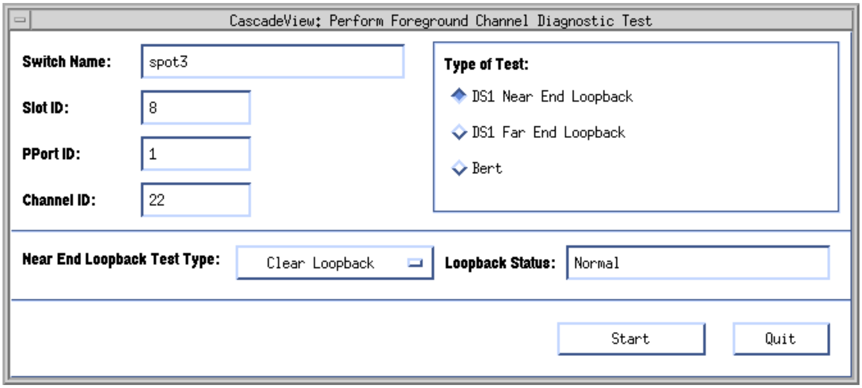


Figure 4-7. Perform Foreground Channel Diagnostic Test Dialog Box

Table 4-2 describes the Perform Foreground Channel Diagnostic Test dialog box fields.

Table 4-2. Perform Foreground Channel Diagnostic Test Dialog Box Fields

Field	Description
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 Status	Channel’s current loopback status.

10. Follow the instructions in the next section according to the type of test you want to generate. Select DS1 Near-end Loopback or DS1 Far-End Loopback for the type of test. For instructions on BERT testing, refer to “DS1 BERT Testing for Channelized DS3” on page 4-17.

Generating a DS1 Near-End Loopback

Use the instructions in this section to generate a DS1 near-end loopback test. For more information about test types, refer to “Near-end Loopback Tests” on page 4-7.

1. Select *DS1 Near-End Loopback* for the Type of Test (as shown in Figure 4-8).
2. Select a Near-End Loopback Test Type. Options include Payload Loopback, Line Loopback, and Diagnostic Loopback.
3. Choose Start to begin the test. The loopback test takes approximately 15 seconds to complete. Tests results display in the Loopback Status field as shown in Figure 4-8.

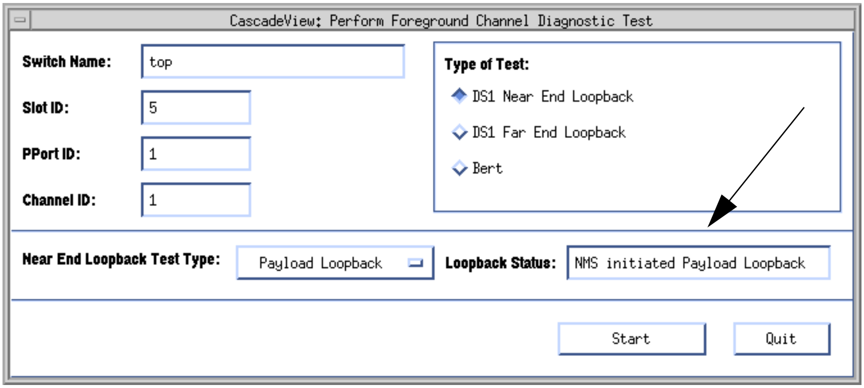


Figure 4-8. DS1 Near-End Loopback Dialog Box

4. Optionally, select Bert for the Type of Test and inject a bit error. (Refer to "Starting and Ending a BERT Test" on page 4-18 for instructions.)

5. To stop the test, select Clear Loopback for the Near-End Loopback Test Type 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.*

Generating a DS1 Far-End Loopback

Use the instructions in this section to generate a DS1 far-end loopback test. For more information about test types, refer to "Far-end Loopback Tests" on page 4-9.

1. On the Perform Foreground Channel Diagnostic Test dialog box, select *DS1 Far-End Loopback* for the type of test.

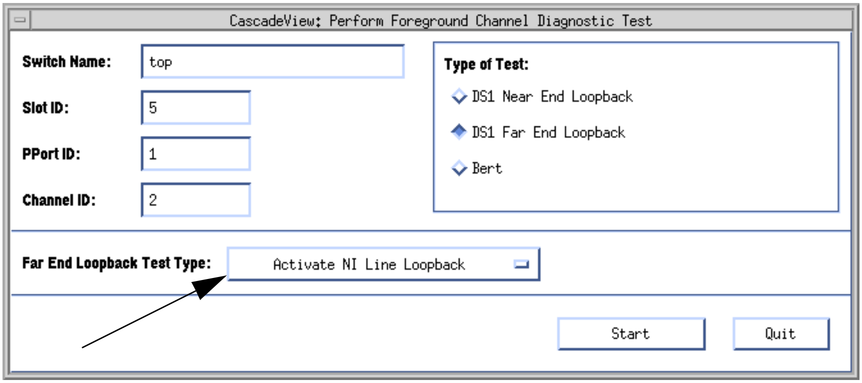


Figure 4-9. DS1 Far-End Loopback Dialog Box

2. Select a Far-End Loopback Test Type (see Figure 4-9). Options include the following:
   - 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
3. Choose Start to begin the test. The loopback test takes approximately 15 seconds to complete.
4. Optionally, select Bert for the Type of Test and inject a Bit Error Rate. (Refer to “Starting and Ending a BERT Test” on page 4-18 for instructions.)

5. To stop the test, select Release [*Test Type*] Loopback for the Test Type and choose Start.

> *If you choose Quit before releasing the test, the test will continue to run and the channel admin status will remain Down. To stop the test, select* ***Release [Test Type] Loopback*** *for the Test Type and choose Start.*

6. To exit the Perform Foreground Channel Diagnostic Test dialog box for this test, choose Quit.

7. To exit the Perform Foreground Diagnostic Test dialog box, choose Close.

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. The generation and monitoring functions are independent, and may 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 4-3 lists and describes the types of Bert Patterns you can generate and receive from the DS1 channel.

Table 4-3. BERT Test Patterns

BERT Test Pattern	Description	Example
All Zeros	Generates and expects data in zeros	0X00
All Ones	Generates and expects data in ones	0XFF
One Zero	Alternate ones and zeros	0XAA
One One Zero Zero	Alternates between two (1s) and two (0s)	0XCC
One Of Eight	Each byte is “10000000”	0X80

Table 4-3. BERT Test Patterns (Continued)

BERT Test Pattern	Description	Example
Three Of Twenty Four	Generates and expects the Hex pattern	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

1. On the network map, select the switch from which you want to obtain physical port and channel diagnostic information.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears (Figure 1-6 on page 1-12).

3. Select the physical port that you want to test by double-clicking on the physical port. The Set Physical Port Attributes dialog box appears (see Figure 4-6 on page 4-12).

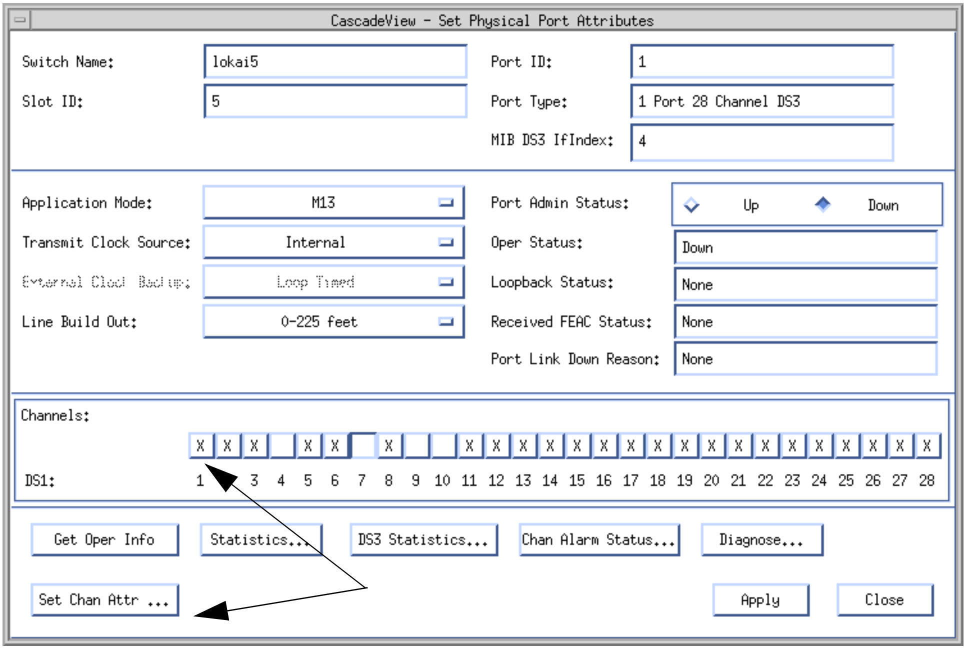


Figure 4-10. Set Physical Port Attributes Dialog Box

4. Select a DS1 channel that you want to test by clicking twice on the channel button ID or select a channel and choose Set Chan Attr (see Figure 4-10).

5. Disable the channel during the loopback test by changing the channel admin status from Up 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 as shown in Figure 4-11.

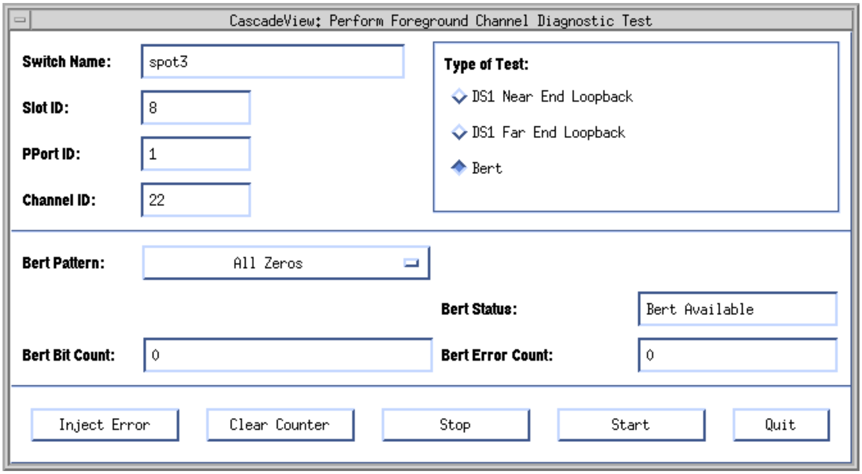


Figure 4-11. Perform Foreground Diagnostics Test (Bert) Dialog Box

9. Select Bert in the Type of Test field as shown in Figure 4-11.

   Table 4-4 describes the fields on the dialog box shown in Figure 4-11.

Table 4-4. Bert Test Fields

Field	Description
Switch Name	Name of the switch in which the module resides.
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.
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. The default Bert Pattern is *All Zeros* (refer to Table 4-3 on page 4-17 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 display in the Bert Status field as shown in Figure 4-12.

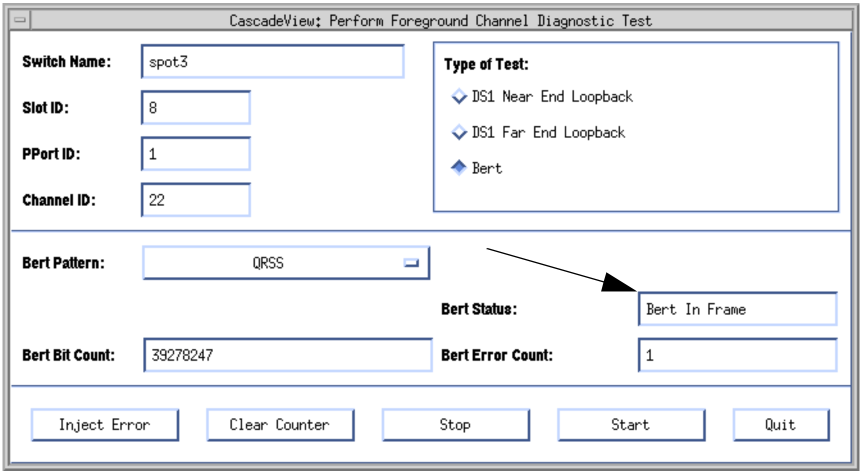


Figure 4-12. Perform Foreground Channel Diagnostic Test Dialog Box

13. Choose Inject Error to inject a bit error and detect a loss of pattern sync. Results display in the Bit Count and Error Count fields. Compare the displayed Bert Error Count to the expected count. (Refer to the example shown in Figure 4-13 for more information.)

14. To exit the Perform Foreground Channel Diagnostic Test dialog box, choose Stop and Quit.

Inject Bit Error Example

Figure 4-13 shows a Bert test using a QRSS pattern. Test results display 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.

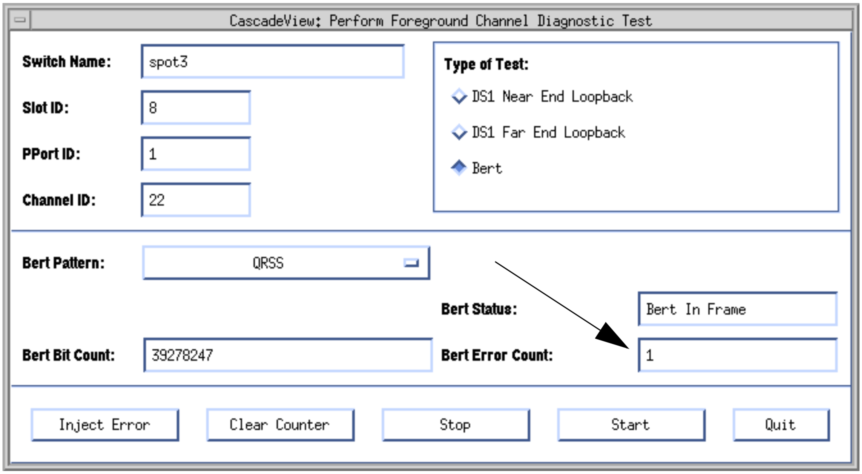


Figure 4-13. Perform Foreground Channel Diagnostic Test Dialog Box

DS3 Loopback

The DS3 option is available only for the following B-STDX 8000/9000 modules:

- Single-port ATM DS3
- Single-port channelized DS3

When you initiate a DS3 Line loopback, the entire DS3 of the physical port is put into the loopback from the near-end. When you initiate a DS3 Far-end loopback, the entire DS3 of the physical port is put into the loopback from the far-end.

Table 4-5. DS3 Loopback Types

Loopback Type	Description	Module
Near-end line	Loops the receiver to the transmitter in order to loop the incoming signal back to the far-end.	ATM DS3 Channelized DS3
Far-end	Sends a code to request the far-end to put itself into loopback.	ATM DS3 Channelized DS3
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.	ATM DS3
Near-end diag	Loops the transmitter to the receiver in order to loop the outgoing signal back to the DS3 port. This test allows the card to test itself.	Channelized DS3

DS3 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 refer to Chapter 10, "Trap Alarm Conditions".

Activating and Ending a DS3 Loopback

1. On the network map, select the switch from which you want to obtain physical port diagnostic information. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box shown in Figure 1-6 appears.
2. 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.
3. Disable the physical port for use during the loopback. Use the following steps to do this:
   a. Change the Port Admin Status value from Up to Down.
   b. Choose Apply. The system then prompts you to confirm the Port Admin Status value change.
   c. Choose OK.
   d. Choose Close. The system then redisplays the Set Switch Back Panel dialog box.
4. Choose Diagnose. The Perform Foreground Diagnostic Test dialog box appears.

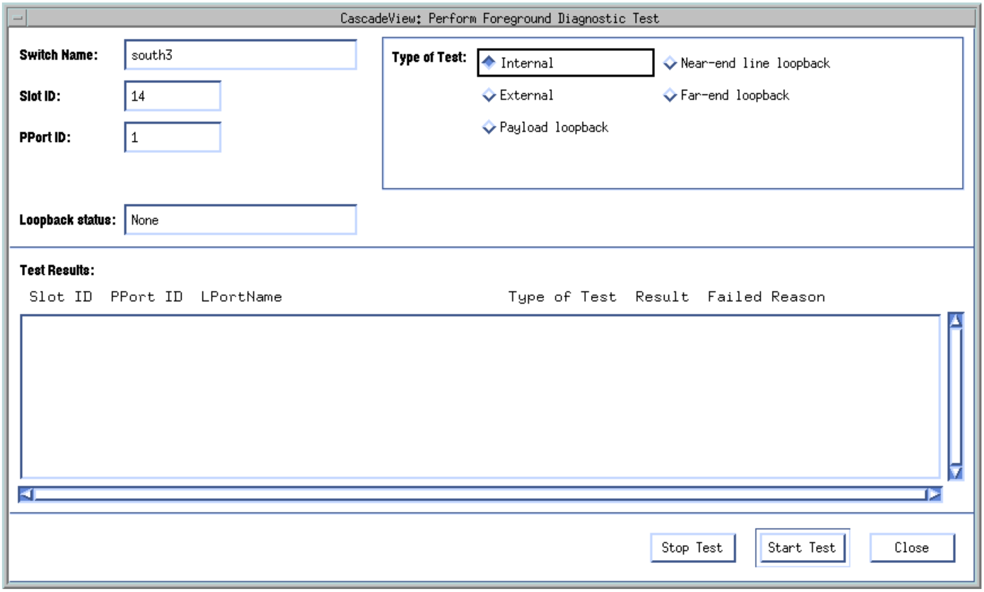


Figure 4-14. Setting a DS3 Loopback (ATM DS3 Module)

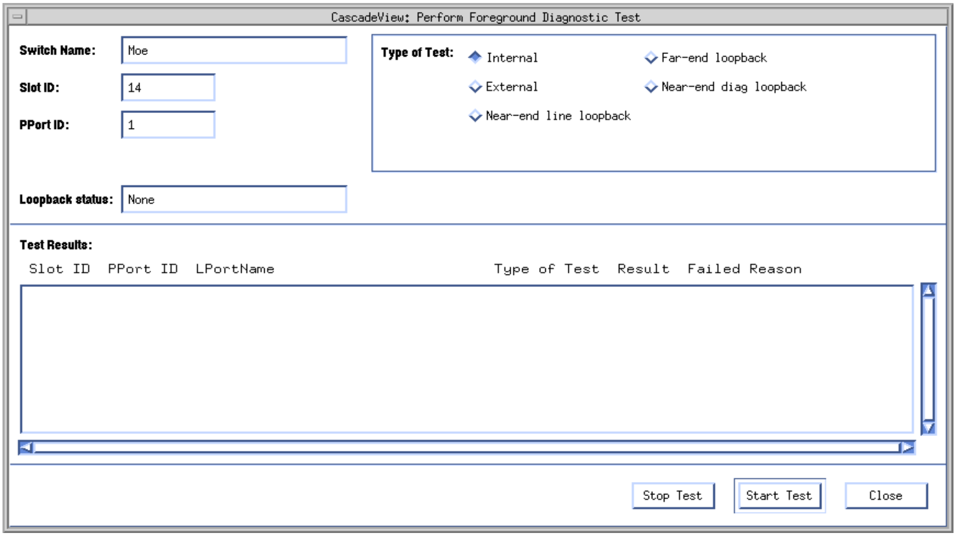


Figure 4-15. Setting a DS3 Loopback (Channelized DS3 Module)

Table 4-6 describes each of the Perform Foreground Diagnostic Test dialog box fields.

Table 4-6. DS3 Perform Foreground Diagnostic Test Dialog Box Fields

Field	Description
Switch Name	Name of the switch in which the module resides
Slot ID	I/O slot number in which the module resides
PPort ID	Port number
Loopback Status	Physical port’s current loopback status

5. 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 4-5 on page 4-23 describes each of these loopback types.
6. Choose Start Test to start the test pattern generation.

   Test results display in the Test Results box at the bottom of the Perform Foreground Diagnostic Test dialog box.
7. Choose Stop Test to return to a normal state.

> *The loopback state is not stored in PRAM. If you reboot the module, the DS3 returns to a normal state.*

8. To exit the dialog box, choose Close. The Set Physical Port Attributes dialog box reappears.
9. Enable the physical port by changing the Admin Status from Down to Up.
10. Choose Apply.
11. Choose Close. The system redisplays the Switch Back Panel dialog box.

DS0 Loopback

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 B-STDX 8000/9000 modules.

- 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 4-16 illustrates a DS0 Near-End Loopback.

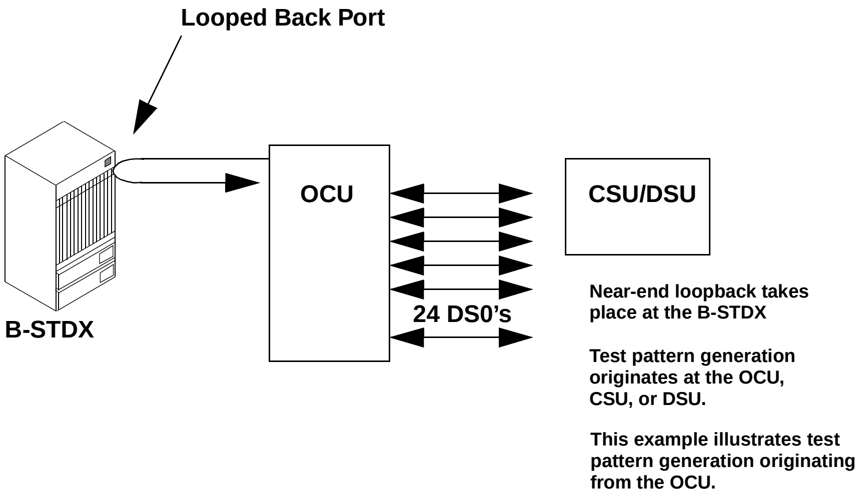


Figure 4-16. DS0 Near-End Loopback

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 4-17 illustrates a DS0 Far-End loopback that takes place at the OCU.

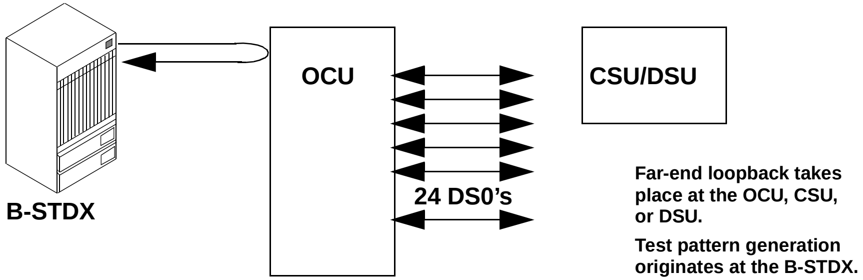


Figure 4-17. DS0 Far-End Loopback

In a Far-End Loopback, there may be up to three midspan repeaters used to boost the signal between the OCU and the CSU/DSU. Figure 4-18 illustrates the use of midspan repeaters in a Far-End Loopback.

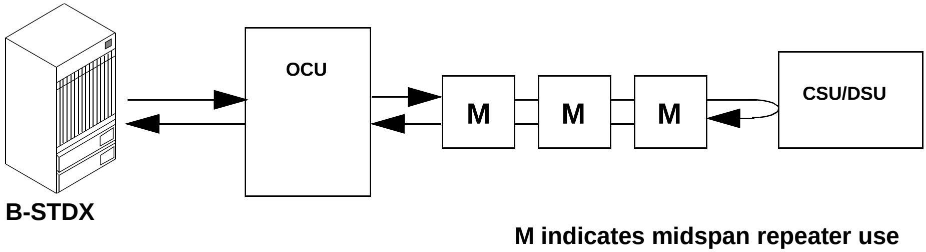


Figure 4-18. Far-End Loopback Using Midspan Repeaters

DS0 Far-End Loopback is a two-step process where you must:

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 card revisions do not support the DS0 loopback feature. If a card does not support the DS0 loopback feature, the DS0 loopback options are grayed out on the Perform Foreground Diagnostic Test dialog box. Refer to the* NMS Software Release Notice *for detailed information about the card revisions that do not support DS0 loopback.*

Activating and Ending a DS0 Near-End Loopback

1. On the network map, select the switch from which you want to obtain physical and logical port diagnostic information. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears.

2. Select the logical port that you want to test.

   To test a logical port — Double-click on the physical port. The Set Physical Ports Attributes dialog box appears. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.

3. Disable the logical port for use during the loopback test. Use the following steps to do this:

   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 from Up to Down to disable the logical port.

4. Choose Diagnose. The Perform Foreground Diagnostic Test dialog box shown in Figure 4-19 appears.

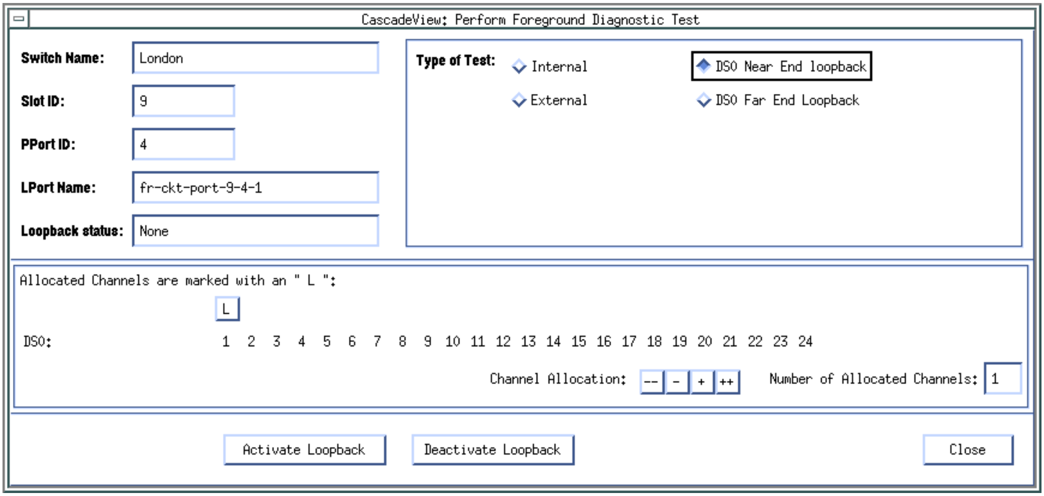


Figure 4-19. Perform Foreground Diagnostic Test Dialog Box

5. Select DS0 Near-End Loopback as the Type of Test. The system then displays all of the logical port channels.

6. 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 manipulation buttons listed in Table 4-7.

Table 4-7. Channel Manipulation Buttons

Button	Action
+	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

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

8. 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.

Activating and Ending a DS0 Far-End Loopback

> *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.*

1. On the network map, select the switch from which you want to obtain physical and logical port diagnostic information. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.

2. Select the logical port that you want to test.

   To test a logical port — Double-click on the physical port. The Set Physical Port Attributes dialog box appears. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.

3. Disable the logical port for use during the loopback. Use the following steps to do this:

   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 then displays the second Modify Logical Port dialog box.

   c. Change the value in the Admin Status field from Up to Down to disable the logical port.

   d. Choose OK. The system then prompts you to confirm the Port Admin Status value change.

   e. Choose OK.

4. Choose Diagnose. The Perform Foreground Diagnostic dialog box appears.

5. Select DS0 Far-End Loopback as the Type of Test. The system then displays all of the logical port channels.

Select the channel on which you want to perform a DS0 Far-End Loopback. 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.*

6. Supply the following field values:

   Far-End Loopback Type — Specifies the Far-End loopback type as one of the following types: OCU, CSU, or DSU.

   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 loopback 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 has an effect on 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 is only applicable for CSU loopbacks.* 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 that your system uses, and you know that there are 3 or less, you can enter a value of 3. Entering a value of 3 will not affect the loopback if you only have 1 or 2 midspan repeaters. However, the loopback will not provide valid data if you have more than 3 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.

7. Select Activate Loopback to activate a DS0 loopback.

8. Select Start Test to start the test pattern generation from the switch that is associated with the selected logical port. The system then displays the DS0 Far-End Loopback statistics. Table 4-8 on page 4-36 lists and describes these statistics.

.

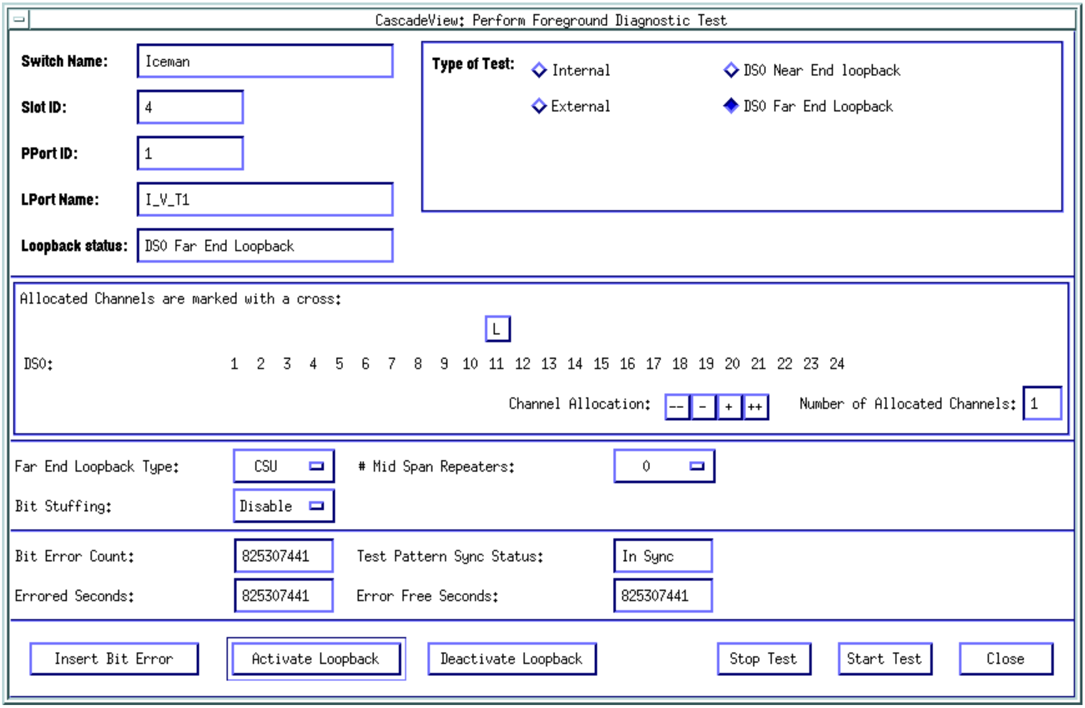


Figure 4-20. Setting a DS0 Far-End Loopback

9. 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 remote equipment connection is operating successfully.

10. Choose Stop Test to stop the test pattern generation.

11. Choose Deactivate Loopback to return to a normal state.

Table 4-8. 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 there is no occurrence of bit errors.

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-Far-Endend 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's. You can also receive the test pattern on the same set of consecutive DS0's.

PVC Loopback

The PVC Loopback option is a diagnostic tool for testing the transmission of data across the 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 frames sent to the PVC could be routed along the entire customer transmission path and be received on either the local or remote endpoint of the PVC.

PVC Loopback Settings

Each PVC endpoint can be configured to one of the following four loopback settings:

- **None** — To indicate that no loopback is in effect.
- **Local** — Indicates that traffic arriving on the logical port from a CPE should be looped back to that CPE on the same logical port. See Figure 4-21 and Figure 4-23 for two examples of local PVC loopbacks. Figure 4-22 and Figure 4-24 illustrate the corresponding Circuit Summary Statistics that result from a local setting on either endpoint A or endpoint B.
- **Remote** — Indicates that traffic arriving from a far-end logical port/CPE should be looped back to that logical port/CPE. See Figure 4-25 and Figure 4-27 for two examples of remote PVC loopbacks. Figure 4-26 and Figure 4-28 illustrate the corresponding Circuit Summary Statistics that result from a remote setting on either endpoint A or endpoint B.
- **Both** — Indicates that both remote and local traffic should loop back.

Figure 4-21 through Figure 4-28 illustrate the direction of the three different PVC loopback settings and the Circuit Summary Statistics that result from each setting. Each figure is followed by a sample summary statistics screen to illustrate the type of statistics that each PVC loopback type will provide.

In all of the figures that illustrate the PVC loopback settings, Router 1 is the endpoint that transmits data over the PVC.

Graceful discard must be set to on in order for the PVC loopback function to operate correctly.

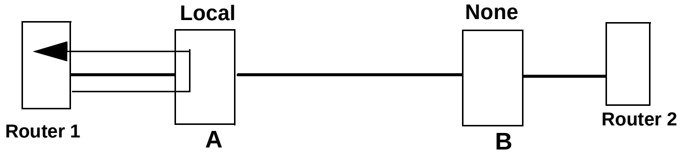
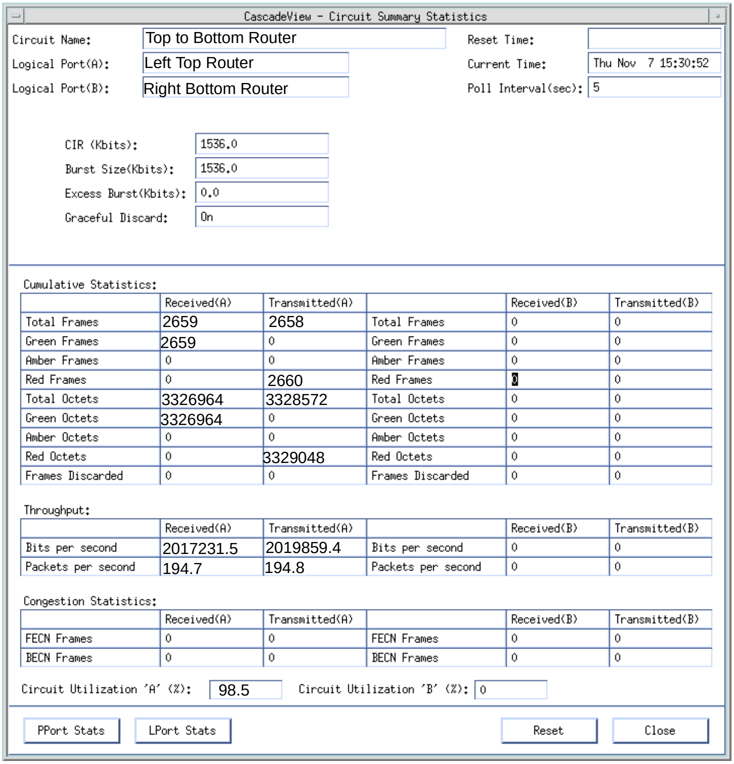


Figure 4-21. PVC Endpoint A Set to Local, Endpoint B Set to None

Figure 4-21 illustrates a PVC loopback that has Endpoint A set to local and Endpoint B set to none. Figure 4-22 illustrates the Circuit Summary Statistics that the system would generate 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.



CascadeView - Circuit Summary Statistics

Circuit Name:	Top to Bottom Router	Reset Time:	
Logical Port(A):	Left Top Router	Current Time:	Thu Nov 7 15:30:52
Logical Port(B):	Right Bottom Router	Poll Interval(sec):	5

CIR (Kbits):	1536.0
Burst Size(Kbits):	1536.0
Excess Burst(Kbits):	0.0
Graceful Discard:	On

Cumulative Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Total Frames	2659	2658	Total Frames	0	0
Green Frames	2659	0	Green Frames	0	0
Amber Frames	0	0	Amber Frames	0	0
Red Frames	0	2660	Red Frames	0	0
Total Octets	3326964	3328572	Total Octets	0	0
Green Octets	3326964	0	Green Octets	0	0
Amber Octets	0	0	Amber Octets	0	0
Red Octets	0	3329048	Red Octets	0	0
Frames Discarded	0	0	Frames Discarded	0	0

Throughput:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Bits per second	2017231.5	2019859.4	Bits per second	0	0
Packets per second	194.7	194.8	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

Circuit Utilization 'A' (%): 98.5 Circuit Utilization 'B' (%): 0

PPort Stats LPort Stats Reset Close

Figure 4-22. Statistics That Result When A is Local and B is None

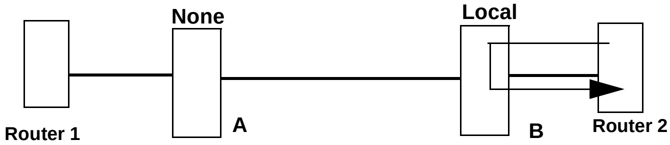
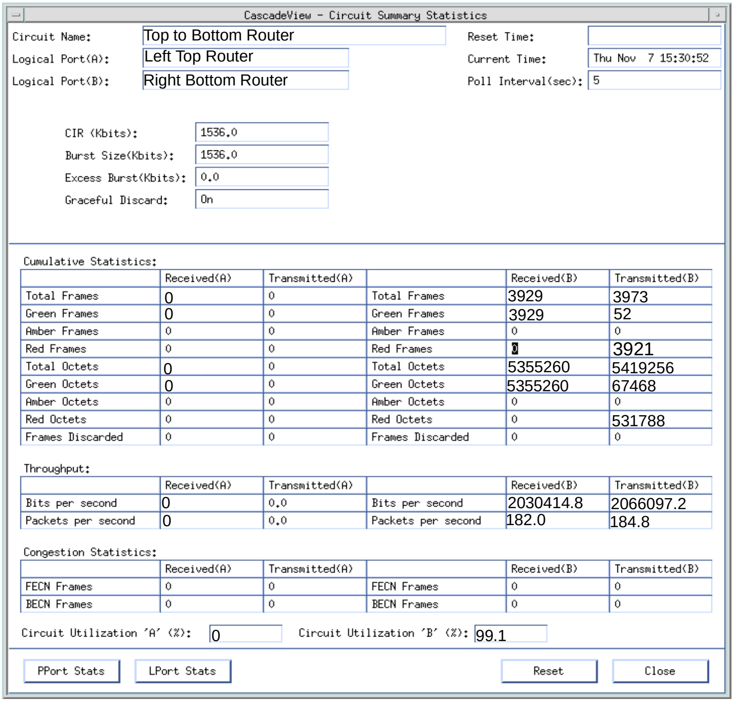


Figure 4-23. PVC Endpoint A Set to None, Endpoint B Set to Local

Figure 4-23 illustrates a PVC loopback that has Endpoint A set to none and Endpoint B set to local. Figure 4-24 illustrates the Circuit Summary Statistics that the system would generate for a local PVC loopback at Endpoint B.



CascadeView - Circuit Summary Statistics

Circuit Name: Top to Bottom Router
Logical Port(A): Left Top Router
Logical Port(B): Right Bottom Router
Reset Time:
Current Time: Thu Nov 7 15:30:52
Poll Interval(sec): 5

CIR (Kbits): 1536.0
Burst Size(Kbits): 1536.0
Excess Burst(Kbits): 0.0
Graceful Discard: On

Cumulative Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Total Frames	0	0	Total Frames	3929	3973
Green Frames	0	0	Green Frames	3929	52
Amber Frames	0	0	Amber Frames	0	0
Red Frames	0	0	Red Frames	0	3921
Total Octets	0	0	Total Octets	5355260	5419256
Green Octets	0	0	Green Octets	5355260	67468
Amber Octets	0	0	Amber Octets	0	0
Red Octets	0	0	Red Octets	0	531788
Frames Discarded	0	0	Frames Discarded	0	0

Throughput:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Bits per second	0	0.0	Bits per second	2030414.8	2066097.2
Packets per second	0	0.0	Packets per second	182.0	184.8

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' (%): 0 Circuit Utilization 'B' (%): 99.1

PPort Stats LPort Stats Reset Close

Figure 4-24. Statistics That Result When A is None and B is Local

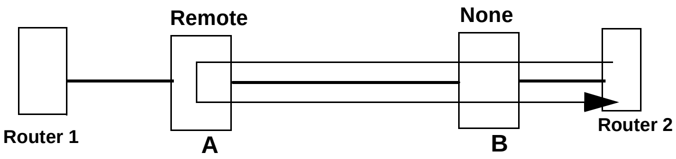


Figure 4-25. PVC Endpoint A Set to Remote, Endpoint B Set to None

Figure 4-25 illustrates a PVC loopback that has Endpoint A set to remote and Endpoint B set to none. Figure 4-26 illustrates the Circuit Summary Statistics that the system would generate for a remote PVC loopback at Endpoint A.

CascadeView - Circuit Summary Statistics

Circuit Name:	Top to Bottom Router	Reset Time:	
Logical Port(A):	Left Top Router	Current Time:	Thu Nov 7 15:30:52
Logical Port(B):	Right Bottom Router	Poll Interval(sec):	5

CIR (Kbits):	1536.0
Burst Size(Kbits):	1536.0
Excess Burst(Kbits):	0.0
Graceful Discard:	On

Cumulative Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Total Frames	0	0	Total Frames	3298	3356
Green Frames	0	0	Green Frames	3298	3356
Amber Frames	0	0	Amber Frames	0	0
Red Frames	0	0	Red Frames	0	0
Total Octets	0	0	Total Octets	4923700	5007620
Green Octets	0	0	Green Octets	4923700	5007620
Amber Octets	0	0	Amber Octets	0	0
Red Octets	0	0	Red Octets	0	0
Frames Discarded	0	0	Frames Discarded	0	0

Throughput:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Bits per second	0.0	0.0	Bits per second	1966657.0	2012518.8
Packets per second	0.0	0.0	Packets per second	163.9	168.3

Congestion Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
FECN Frames	0	0	FECN Frames	0	3357
BECN Frames	0	0	BECN Frames	0	0

Circuit Utilization 'A' (%): 0 Circuit Utilization 'B' (%): 96.0

PPort Stats LPort Stats Reset Close

Figure 4-26. Statistics That Result When A is Remote and B is None

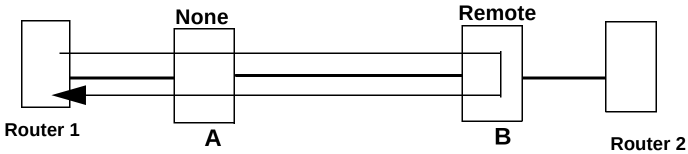
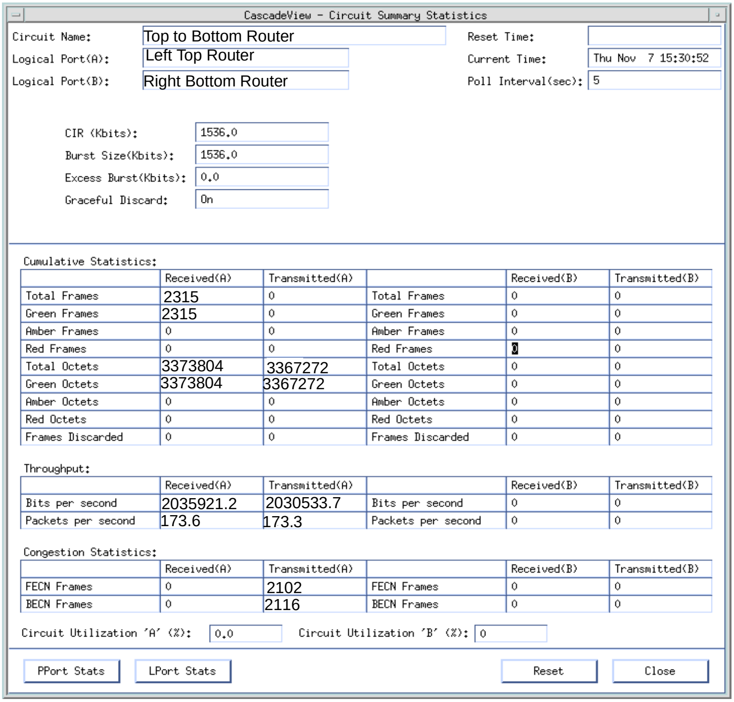


Figure 4-27. PVC Endpoint A Set to None, Endpoint B Set to Remote

Figure 4-27 illustrates a PVC loopback that has Endpoint A set to none and Endpoint B set to remote. Figure 4-28 illustrates the Circuit Summary Statistics that the system would generate if endpoint A is set at None and endpoint B is set at Remote.



CascadeView - Circuit Summary Statistics

Circuit Name:	Top to Bottom Router	Reset Time:	
Logical Port(A):	Left Top Router	Current Time:	Thu Nov 7 15:30:52
Logical Port(B):	Right Bottom Router	Poll Interval(sec):	5

CIR (Kbits):	1536.0
Burst Size(Kbits):	1536.0
Excess Burst(Kbits):	0.0
Graceful Discard:	On

Cumulative Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Total Frames	2315	0	Total Frames	0	0
Green Frames	2315	0	Green Frames	0	0
Amber Frames	0	0	Amber Frames	0	0
Red Frames	0	0	Red Frames	0	0
Total Octets	3373804	3367272	Total Octets	0	0
Green Octets	3373804	3367272	Green Octets	0	0
Amber Octets	0	0	Amber Octets	0	0
Red Octets	0	0	Red Octets	0	0
Frames Discarded	0	0	Frames Discarded	0	0

Throughput:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
Bits per second	2035921.2	2030533.7	Bits per second	0	0
Packets per second	173.6	173.3	Packets per second	0	0

Congestion Statistics:

	Received(A)	Transmitted(A)		Received(B)	Transmitted(B)
FECN Frames	0	2102	FECN Frames	0	0
BECN Frames	0	2116	BECN Frames	0	0

Circuit Utilization 'A' (%): 0.0 Circuit Utilization 'B' (%): 0

PPort Stats LPort Stats Reset Close

Figure 4-28. Statistics That Result When A is None and B is Remote

When to Use PVC Loopback

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

What Problems Can PVC Loopback Detect

PVC loopback enables you to determine the following circuit problems:

- Whether or not 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

Refer to the section that follows for more information about how to set a PVC loopback. Refer to “Monitoring a PVC Loopback” on page 4-46 for more information about how to view the status of a PVC loopback.

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:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits ⇒ Point-to-Point. The Set All PVCs On Map dialog box appears.

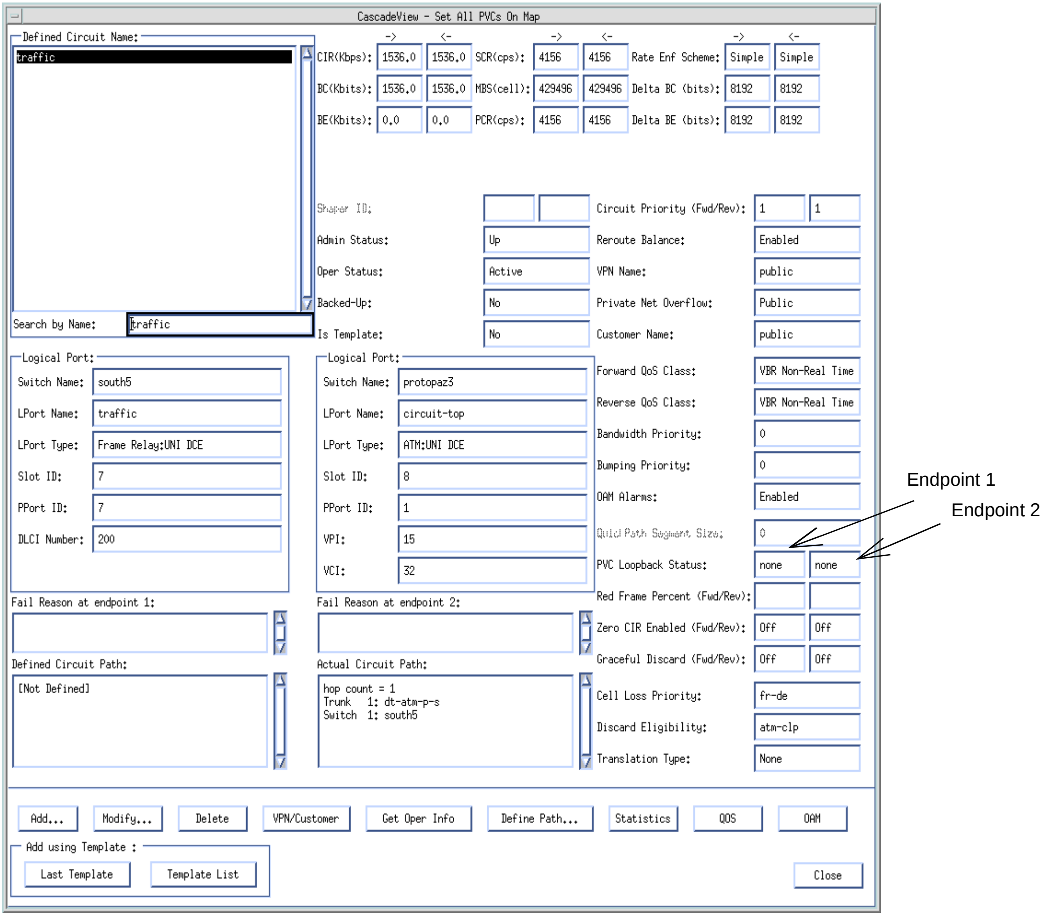


Figure 4-29. Set All Circuits on Map

2. Choose Modify from the Set All Circuits on Map dialog box. The Modify Circuit dialog box appears.

3. Choose the Set User Preference Attributes option. The system then displays the user preference attributes at the bottom of the Modify PVC dialog box (Figure 4-30).

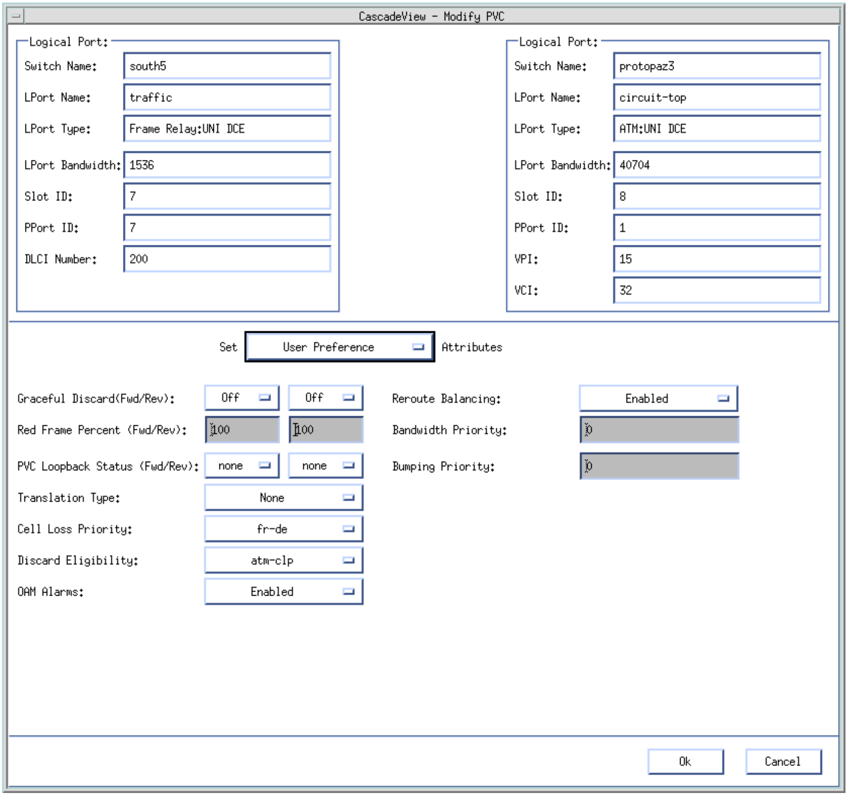


Figure 4-30. Setting a PVC Loopback

4. 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*. Refer to“PVC Loopback Settings” on page 4-37 for a complete description of the PVC loopback settings. Table 4-9 on page 4-45 lists the valid PVC loopback combinations for the endpoint loopback specifications.

Use the Circuit Summary Statistics window to monitor a PVC loopback. Refer to the Monitoring a PVC Loopback section that follows for instructions on accessing the Circuit Summary Statistics 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 4-9.

Table 4-9. 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 on Map dialog box specifies whether or not a PVC loopback status is in effect. Refer to “Reviewing the Status of Circuits” on page 2-10 for more detailed information about how to access the Show All PVCs on Map dialog box.

To view the statistics for a PVC loopback, choose the Statistics button from the Show All PVCs on Map dialog box (Figure 4-31). The system then displays the Circuit Summary Statistics dialog box. See the “Circuit Summary Statistics Example” on page 8-9 for more information about displaying circuit summary statistics.

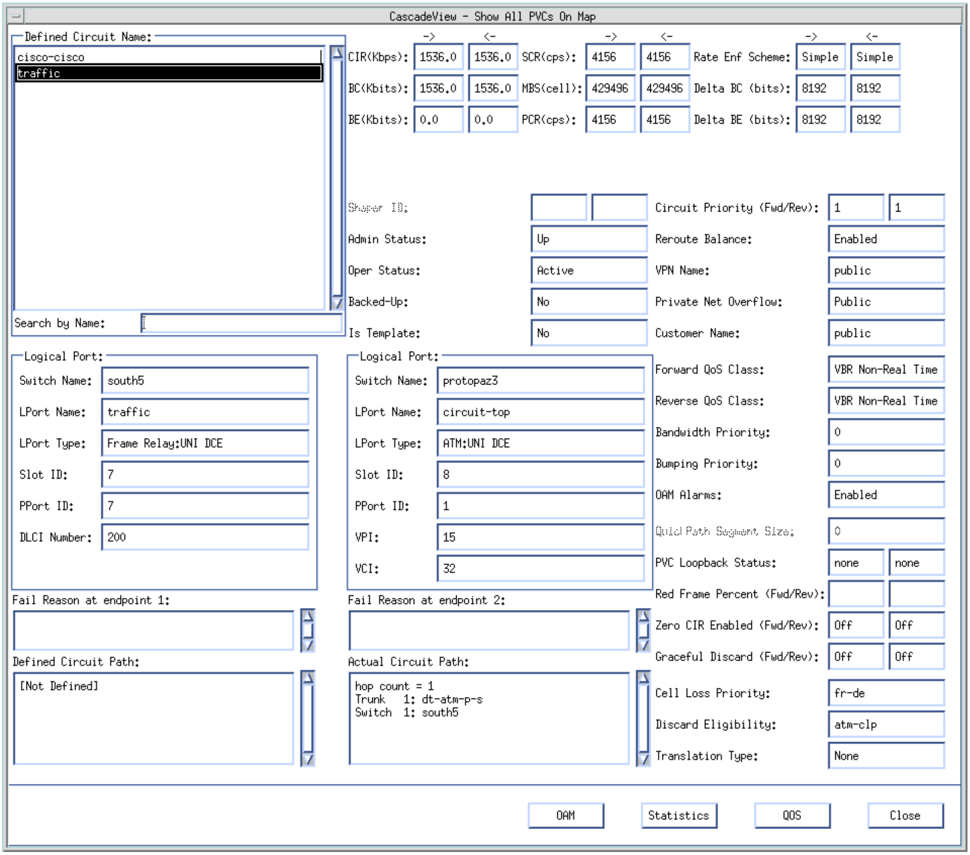


Figure 4-31. Show All PVCs on Map

5

Generating Statistics and Reports

CascadeView/UX generates statistical information for a selected physical port, logical port, circuit, or trunk. This chapter describes how to set the polling interval that is used to retrieve statistical data. In addition, Table 5-1 on page 5-3 lists the chapters in this section that describe how to display real-time statistics that you can use to monitor and troubleshoot the Cascade network. This chapter also describes how to use scripts or the CascadeView/UX NMS to generate network, circuit, node, or trunk reports.

Setting the Polling Interval

The *Polling* function sets the time interval for the collection of all statistical data during the current session of CascadeView/UX.

To reset the time interval for the current session of CascadeView/UX select Misc ⇒ Cascade Time Intervals ⇒ Set Statistics Time Interval.

CascadeView/UX then displays the Change Statistics Polling Interval dialog box shown in Figure 5-1.

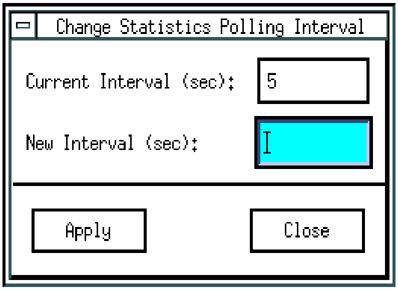


Figure 5-1. Change Statistics Polling Interval Dialog Box

Generating Summary Statistics

Summary statistics display real-time statistical information in a tabular format for various network objects.

Summary Statistics Types

The statistical data that the system retrieves is dependent on your custom selections, as the following list describes:

Physical port — Shows the bits and frames being sent and received over the selected physical port.

Logical port — Shows the error codes that have been received by the selected logical port.

Circuit — Shows the bytes and frames sent and received over the selected circuit.

Trunk — Shows the bi-directional use of the selected trunk at a given point in time.

In addition, the channelized DS3 module enables you to view a number of different summary statistics that are not provided for the other modules.

Summary statistics are displayed but not stored on the NMS. You can use the Bulk Statistics for UNIX product to store statistical data for later use. Refer to the Bulk Statistics Collector for B-STDX/STDX *document for more information about this product.*

Table 5-1 lists the references to each of the different type of summary statistics along with the description of the statistics type.

Table 5-1. Types of Statistics

See	For Information About
Chapter 6, "Logical and Physical Port Statistics"	Physical port summary statistics and Frame Relay and SMDS logical port summary statistics for all modules other than the channelized DS3.
Chapter 7, "Channelized DS3 Statistics"	Channelized DS3 physical and logical port summary statistics.
Chapter 8, "Trunk and Circuit Statistics"	Trunk, circuit, and circuit quality of service statistics.

Generating Reports

Using Scripts to Generate Reports

Table 5-2 describes the scripts that you can run to generate reports at the network, node, circuit, or trunk level.

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 shown in Table 5-2 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 5-2. 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

Using the CascadeView/UX Report Menu to Generate Reports

The CascadeView/UX Report menu contains Generate and View submenus to enable you to generate and view the following types of reports:

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

Table 5-3 describes each of the Generate and View report options. The system generates an error message if you attempt to use the View option to view a nonexistent report before the report has been generated.

Table 5-3. Generate and View Report Options

Report Option	Description
Generate or View Single Node Report	To select this option: • First click the mouse on a node to select the node for use in a report. • Then select the Report menu option. The system 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 input is required. All nodes in the NMS database (specified in cascadeview.cfg) are applied in the report.
Generate or View Network Report	When you select this option the system prompts you for the network number. If you specify the network number, the system generates a report for the one specified network. If you press Enter without specifying a network number, the system generates a report for all networks. The network report is available for viewing until the Generate option is selected to generate another report.
Generate or View Trunk Report	When you select this option the system prompts you for the network number. If you specify the network number, the system generates a trunk report for the one specified network. If you press Enter without specifying a network number, the system generates a trunk report for all networks. The trunk report is available for viewing until the Generate option is selected to generate another report.

Table 5-3. Generate and View Report Options (Continued)

Report Option	Description
Generate or View Circuit Report	When you select this option, the system prompts for the network number. If you specify the network number, the system generates a circuit report for the one specified network. If you press Enter without specifying a network number, the system generates a circuit report for all networks. The circuit report is available for viewing until the Generate option is selected to generate another report.
Transparency	All reports are sent to the */opt/CascadeView.var/cvReport* directory of the user's HOME.

6

Logical and Physical Port Statistics

This chapter describes the following types of summary statistics for modules other than the Channelized DS3 module.

- Physical Port Summary Statistics
- Frame Relay Logical Port Summary Statistics
- SMDS Logical Port Summary Statistics
- ATM IWU Logical Port Summary Statistics

See Chapter 7, "Channelized DS3 Statistics" for information about channelized DS3 statistics.

See the *CBX 500 Network Administrator's Guide* for information about monitoring logical port summary statistics on the CBX 500.

Displaying Physical Port Summary Statistics

Use the following steps to generate Physical Port Summary Statistics:

1. On the network map, select the appropriate switch icon. The selected object appears highlighted.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The system then displays the Switch Back Panel dialog box as shown in Figure 1-6.
3. Select the physical port and choose Get Attributes. The system then displays the Show Physical Port Attributes dialog box.
4. Choose Statistics. The Physical Port Summary Statistics dialog box appears as shown in Figure 6-1 and Figure 6-2. Table 6-1 describes each of the fields on this dialog box.

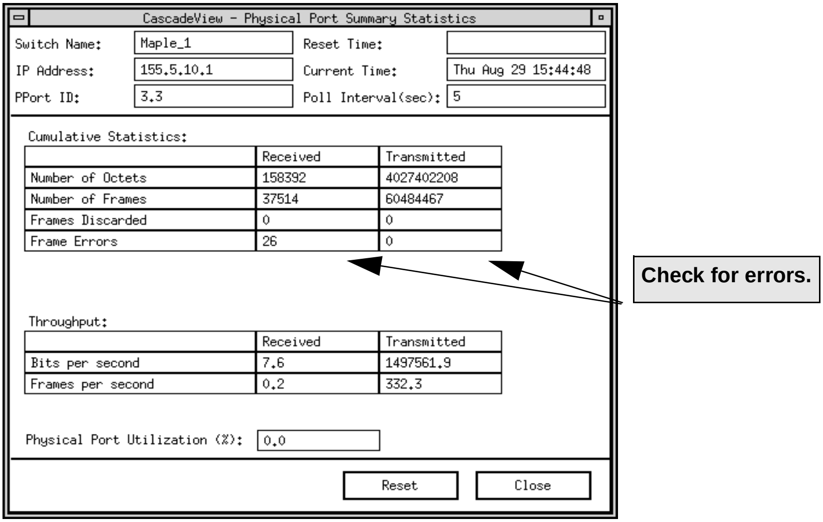


Figure 6-1. Physical Port Summary Statistics, Example 1

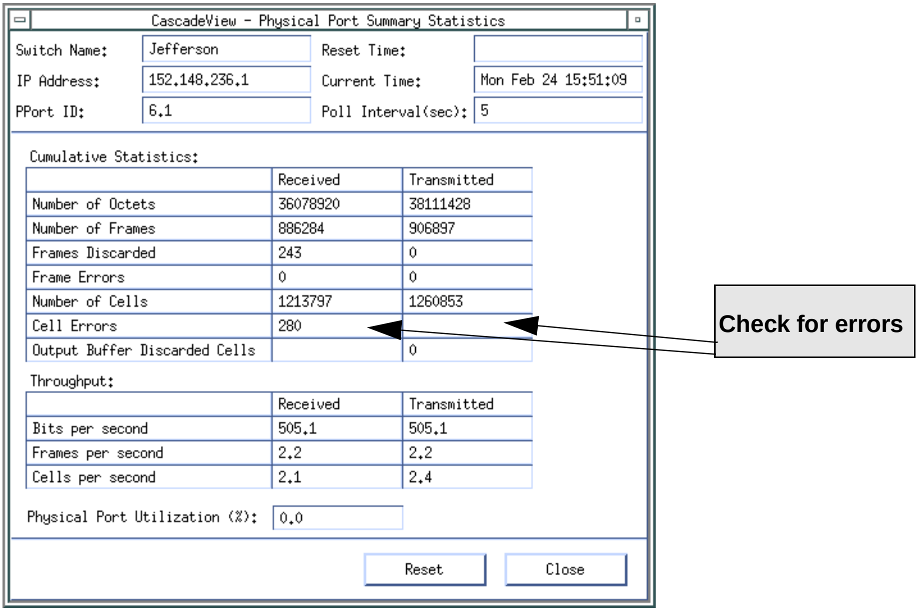


Figure 6-2. Physical Port Summary Statistics, Example 2

> *The physical port utilization field measures the amount of traffic queued for transmission on a physical port as a percentage of the physical port bandwidth. It does not measure the amount of bandwidth of the physical port being used. For this reason the value displayed in the physical port utilization field can exceed 100%.*

> *The fields that the Physical Port Summary Statistics dialog box displays vary depending on the type of card you are currently displaying statistics for. Table 6-1 lists and describes all of the fields that can be displayed in the Physical Port Summary Statistics dialog box.*

Physical Port Summary Statistics Descriptions

The Physical Port Summary Statistics dialog box displays data in separate columns to reflect the transmission and receipt of data on the physical port. **Cumulative Statistics** list the number of each type of cell or frame (received, transmitted, or tagged due to an error). In addition, the **throughput fields** display the bits, frames, or cells per second for the physical port. Table 6-1 lists and describes each physical port summary statistic

A warm boot clears all of the cumulative statistics and resets the counters.

.

Table 6-1. Physical Port Summary Statistics Field Descriptions

Field	Description
Identifying Fields	
Switch Name	Displays the name of the switch for which you are viewing the diagnostic information.
IP Address	The internal IP address of the switch.
PPort	The ID that identifies this physical port.
Reset Time	The time that the Reset command 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. Refer to "Setting the Polling Interval" on page 5-1 for details about how to set this value.
Cumulative Statistics	
Number of Octets	The total number of octets (bytes) received and transmitted since the last reset.

Table 6-1. Physical Port Summary Statistics Field Descriptions (Continued)

Field	Description
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 value 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.
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.

Table 6-1. Physical Port Summary Statistics Field Descriptions (Continued)

Field	Description
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 being used. For this reason, the value displayed in this field can exceed 100%.

Displaying Logical Port Summary Statistics

To display logical port summary statistics:

1. On the network map, select the appropriate switch icon. The selected object appears highlighted.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The system then displays the Switch Back Panel dialog box.
3. Select the physical port. The system then displays the Show Physical Port Attributes dialog box.
4. Choose the Logical Port option. The system then displays the Show All Logical Ports in PPort dialog box. Table 6-2 on page 6-8 describes each of the fields for this dialog box.

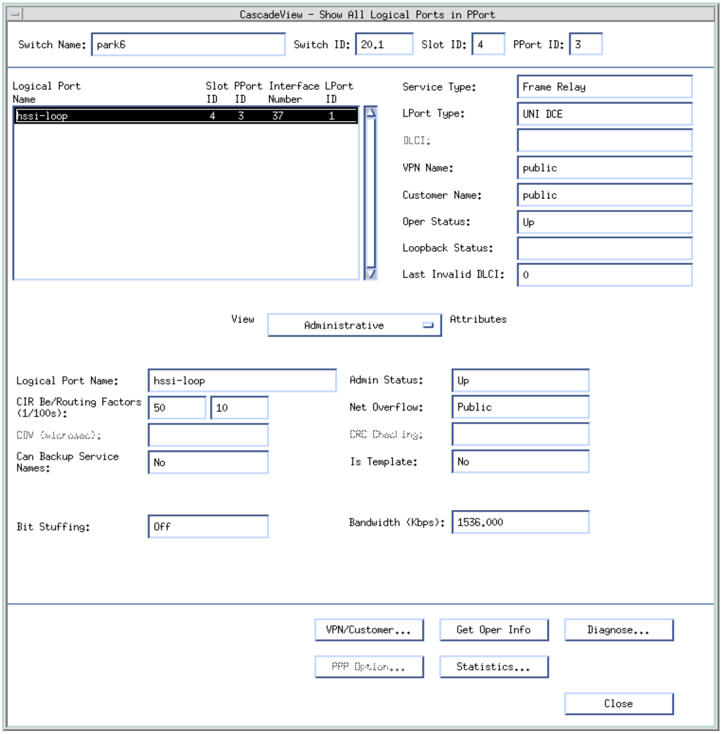


Figure 6-3. Show All Logical Ports in PPort Dialog Box

Table 6-2. Show All Logical Ports in Physical Port Fields

Field	Description
Switch Name	Displays the name of the switch for which you are viewing the diagnostic information.
Switch ID	The ID assigned to this switch.
Slot ID	The back panel physical slot number where the I/O module that contains the selected logical port is installed.
PPort ID	The ID number of the selected physical port.
Logical Port List	The list of logical ports that are defined for the selected physical port.
Lport Type	The logical port configuration type.
VPN Name	A virtual private network (VPN) name. Refer to "VPN Overview" on page 2-33 for details.
Customer Name	The name of the customer using the VPN.
Can Backup Service Name	Displays either Yes or No to specify whether or not this logical port can be backed up to a service name binding.
Admin Status	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 off-line so that diagnostics can be run to test the port. A logical port with an Admin Status of *Down* is not operational.
Loopback Status	*(DS3 only)* The default value for this field is *none*. If you enable diagnostic loopback tests, this field displays the DS3 card's loopback status. A loopback test enables you to test the physical path for data transmission by looping back traffic in one or both directions. For more information about loopbacks, see Chapter 4, "Loopbacks".

Table 6-2. Show All Logical Ports in Physical Port Fields (Continued)

Field	Description
Oper Status	Indicates whether the selected port is operationally Up, Down, or Unknown. Unknown indicates that the NMS is unable to contact the switch to retrieve status.
Is Template	Displays either Yes or No to indicate whether you can use this logical port configuration as a template.
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 only other private trunks during overflow or trunk failure. For more details, see “Private Net Overflow” on page 2-33.

5. Choose Statistics from the Show All Logical Ports in PPort dialog box. The system then displays either the SMDS Logical Port Summary Statistics dialog box shown in Figure 6-4 or the CascadeView Logical Port Summary Statistics (for Frame Relay statistics) shown in Figure 6-6.

For detailed information about the SMDS Logical Port Summary Statistics, see Table 6-3 and Table 6-4.

For detailed information about the Frame Relay Logical Port Summary Statistics, refer to “Frame Relay Logical Port Summary Statistics” on page 6-23.

SMDS Logical Port Summary Statistics Example

Figure 6-4 illustrates the SMDS logical port statistics.

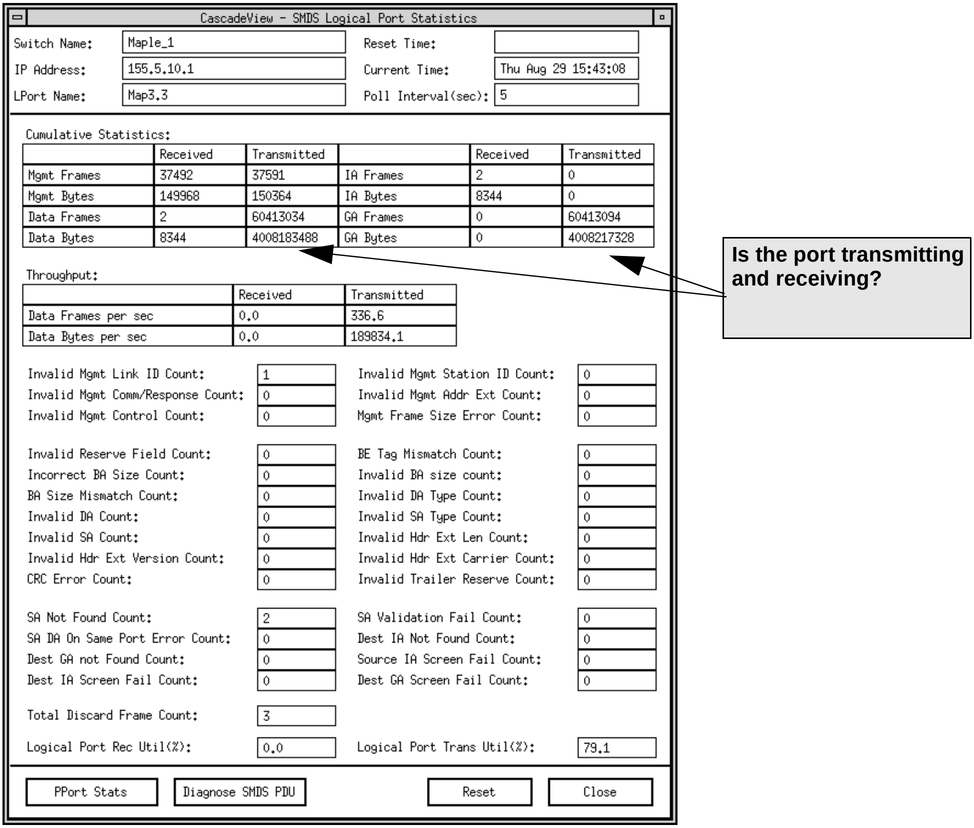


Figure 6-4. SMDS Logical Port Summary Statistics Example

> *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%.*
>
> *The CascadeView/UX NMS does not report values for the IA frame and GA frame counts for pre-4.2 switches.*

Table 6-3 lists and describes all of the identifying, cumulative, and throughput information at the top of the SMDS Logical Port Summary Statistics dialog box. Table 6-4 describes each of the summary statistics shown in Figure 6-4.

Table 6-3. SMDS Identifying, Cumulative, and Throughput Descriptions

Field	Description
Identifying Fields	
Switch Name	Displays the name of the switch for which you are viewing the diagnostic information.
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. Refer to "Setting the Polling Interval" on page 5-1 for details about how to set this value.
Cumulative Statistics	
Number of Management Frames	The total number of management frames received and transmitted since the last reset.
Number of Management Bytes	The total number of management bytes received and transmitted since the last reset.
Number of Data Frames	The total number of data frames received and transmitted since the last reset.
Number of Data Bytes	The total number of data bytes.
Throughput Statistics	
Data Frames per second	The total number of data frames received and transmitted each second.
Data Bytes per second	The total number of data bytes received and transmitted each second.

SMDS Logical Port Summary Statistics

The SMDS Logical Port Summary Statistics dialog box provides three different types of summary statistics about each logical port:

SMDS PDU Violation Statistics (S) — CascadeView/UX increments a counter every time an SMDS Protocol Data Unit (PDU) violation takes place on a logical port. Ten separate counters are provided for each logical port. These counters record the 10 SMDS PDU checks that the system **always** performs during the switching of an SMDS packet.

Protocol Error Checking Statistics (P) — These statistics are recorded only when you set the Protocol Error Checking parameter to on. (This value is set through CascadeView/UX when you add the logical port). If this value is set to *on*, complete protocol error checking occurs. If it is set to *off*, none of these statistics are recorded.

Unsupported Statistics (U) — Statistics that are not used or not currently supported.

Table 6-4 lists and describes each of these statistics. In addition, this table specifies the type of summary statistic in the Type column by indicating an **S** for SMDS PDU Violation Statistics, a **P** for Protocol Error Checking Statistics, and a **U** for Unsupported Statistics.

> *"The number of times" in the Description field refers to the total number of frames counted since the system up time of the card.*

SMDS Logical Port Summary Statistics Description

Table 6-4. SMDS Logical Port Summary Statistics

Type	Statistic	Description
P	BA Size Mismatch Count	The number of times that the SMDS Interface Protocol (SIP) Level 3 PDU Buffer Allocation (BA) size 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.
P	BE Tag Mismatch Count	The number of times that the SMDS Interface Protocol (SIP) Level 3 PDU Beginning and End (BE) tag did not match. A BE tag resides in both the leader and the trailer portions of a frame. The value is incremented by one for each frame that is transmitted from 0-255. After the 255th frame, the counter is reset to 0. The value of the BE tag in the header and trailer should be equal. If not, the BE Tag Mismatch Count increments.
U	CRC Error Count	Not used.
S	Dest GA Not Found Count	The number of times that the Destination Group Address (GA) was not found because the switch configuration did not specify the destination GA.
S	Dest IA Not Found Count	The number of times that the Destination Individual Address (IA) was not found because the switch configuration did not specify the destination IA.

Table 6-4. SMDS Logical Port Summary Statistics (Continued)

Type	Statistic	Description
S	Dest IA Screen Fail Count	The number of times that the Destination Individual Address (IA) screen failed. Each time a packet that is transmitted by a user device enters a Cascade 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.
S	Dest GA Screen Fail Count	The number of times that the Destination Group Address (GA) screen failed. Each time a packet that is transmitted by a user device enters a Cascade 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.
P	Incorrect BA Size Count	The number of times that the SMDS Interface Protocol (SIP) Level 3 PDU Buffer Allocation (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.
P	Invalid BA Size Count	The number of times that the SMDS Interface Protocol (SIP) Level 3 PDU Buffer Allocation (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 considered invalid.
U	Invalid DA Count	Not used.

Table 6-4. SMDS Logical Port Summary Statistics (Continued)

Type	Statistic	Description
P	Invalid DA Type Count	The number of times that the Destination Address (DA) type was invalid. E.164 addresses start with either an *E* or a *C* prefix. An *E* indicates a group address (GA). A *C* indicates an Individual Address (IA). A destination address can start with either a *C* or an *E*. Any other prefix is caught by the counter as an invalid type.
U	Invalid Hdr Ext Carrier Count	Not used.
P	Invalid Hdr Ext Len Count	The number of times that the SMDS Interface Protocol (SIP) Level 3 PDU Header Extension Length (HEL) was invalid. The HEL value resides in the header of the frame. A 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.
U	Invalid Hdr Ext Version Count	Not used.
P	Invalid Mgmt Addr Ext Count	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 and is reserved to be a 1. If this bit is ever a 0, the packet is dropped. Possible causes of this condition are: 1. Routers that are incorrectly configured. 2. It is possible that the AE bit (being the LSB) was squashed by either the line or by a user device (including a Cascade user device).

Table 6-4. SMDS Logical Port Summary Statistics (Continued)

Type	Statistic	Description
P	Invalid Mgmt Comm/Response Count	The number of times that the Data Exchange Interface (DXI) Level 2 PDU command/response field was invalid. This situation occurs if Cascade cannot communicate with the user device or if the user device is dead. If the heartbeat poll option is Yes, and the router doesn't respond after five consecutive fail counts, a trap is sent and the count value increments. Minimally either the Cascade or the user device must have the keep alive option set to on.
P	Invalid Mgmt Control Count	The number of times the Data Exchange Interface (DXI) Level 2 Protocol Data Unit (PDU) control field was invalid. The Level 2 PDU control field is a one-octet field that identifies the frame type. There are two possible frame types, UI and Test. 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 a value of 03 is not found, 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 the 03 nor the F3 value is found, the Invalid Mgmt Control Count increments.
S	Invalid Mgmt Link ID Count	The number of times that the Data Exchange Interface (DXI) Level 2 Protocol Data Unit (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, 1 indicates a management frame (heartbeat poll).

Table 6-4. SMDS Logical Port Summary Statistics (Continued)

Type	Statistic	Description
P	Invalid Mgmt Station ID Count	The number of times that the Data Exchange Interface (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. If this bit is incorrectly set, the frame is dropped.
P	Invalid Reserve Field Count	The number of times that the SMDS Interface Protocol (SIP) Level 3 PDU reserved field in the header was invalid. There is a one-byte reserve 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.
U	Invalid SA count	Not used.
P	Invalid SA Type Count	The number of times that the source address (SA) type was invalid. The only valid SA prefix is the letter *C*. The counter flags any other prefix.
P	Invalid Trailer Reserve Count	The number of times that the SMDS Interface Protocol (SIP) Level 3 PDU reserved field in the trailer was invalid. The reserved field in the trailer is a one-byte field that is populated with 0’s. Any value other than 0 is considered invalid and the frame is dropped.

Table 6-4. SMDS Logical Port Summary Statistics (Continued)

Type	Statistic	Description
S	Mgmt Frame Size Error Count	The number of times that a Data Exchange Interface (DXI) Level 2 PDU frame size error occurred. This statistic checks to see if a frame is greater than a specified minimum of 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. You should also note that *if protocol error checking is set to off*, and this counter is incrementing, the *frames that are in error are data frames*.
S	SA DA on Same Port Error Count	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.
S	SA Not Found Count	The number of times that the Source Address (SA) was not found. The counter increments whenever a Protocol Data Unit (PDU) is received with an E.164 address that is not configured within the SMDS Access Server.
S	SA Validation Fail Count	The number of times that the Source Address (SA) validation failed. This count value increments whenever Cascade receives a PDU with an E.164 address that exists within the SMDS Access Server but is not assigned to the DXI/SNI port that received the PDU.
S	Source IA Screen Fail Count	The number of times that the source Individual Address (IA) screen failed. Each time a user device transmits a packet that enters a Cascade switch, the packet is screened at the Ingress port and at the Egress port. The screening at the Egress port verifies that the packet's source IA is authorized for a particular end-user port.

Viewing SMDS PDU Statistics

To view SMDS PDU statistics, choose Diagnose SMDS PDU from the SMDS Logical Port Statistics listing shown in Figure 6-4 on page 6-10. The system then displays the following SMDS PDU statistics shown in Figure 6-5.

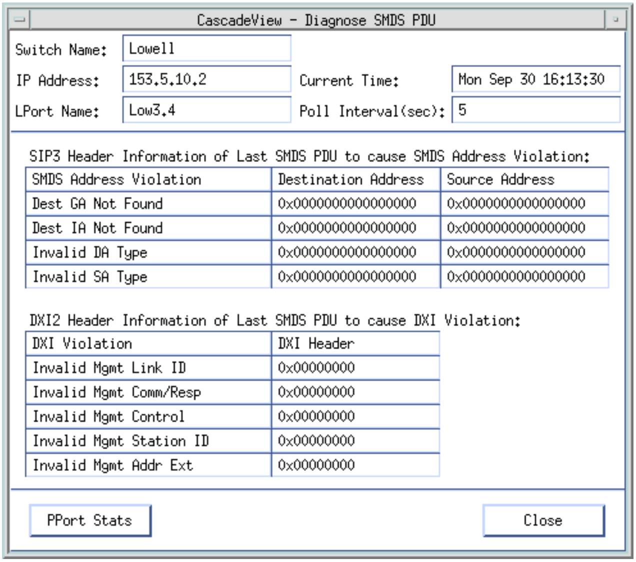


Figure 6-5. Diagnose SMDS PDU Dialog Box

Table 6-5 describes each of the statistics shown in Figure 6-5.

Table 6-5. SMDS PDU Diagnostic Statistics

Violation	Description
SMDS Address Violations	
Dest GA Not Found	The value that was specified for the Destination Group Address (GA).
Dest IA Not Found Count	The value that was specified for the Destination Individual Address (IA).
Invalid DA Type	The value of the SMDS Interface Protocol (SIP) Level 3 PDU Destination Address (DA). E.164 addresses should start with either an *E* or a *C* prefix. An *E* indicates a group address (GA). A *C* indicates an Individual Address (IA). A destination address can start with either a *C* or an *E*. Any other prefix is caught by the counter as an invalid type.
Invalid SA Type	The value of the source address (SA) type. The only valid SA prefix is the letter *C*. The counter flags any other prefix.
DXI Level 2 Header Information	
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 Cascade cannot communicate with the user device of if the user device is dead.

Table 6-5. SMDS PDU Diagnostic Statistics (Continued)

Violation	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. There are two possible frame types, UI and Test. There are two possible frame types, UI and Test. 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 a value of 03 is not found, 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 the 03 nor the 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. If this bit is incorrectly set, 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 reserved to be a 1. If this bit is ever a 0, the packet is dropped. Possible causes of this condition are: 1. Routers that are incorrectly configured. 2. It is possible that the AE bit (being the LSB) was squashed by either the line or by a user device (including a Cascade user device).

Frame Relay Logical Port Summary Statistics Example

Figure 6-6 illustrates the Frame Relay logical port statistics.

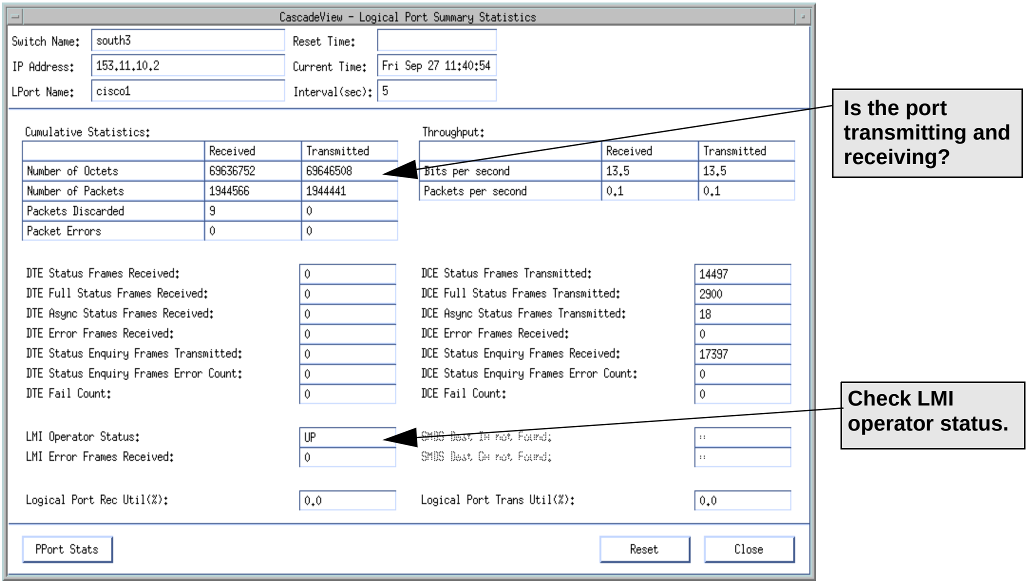


Figure 6-6. Frame Relay Logical Port Summary Statistics Example

> *The Logical Port Utilization field measures the amount of traffic queued for transmission on a logical port as a percentage of the logical port speed. It does not measure the amount of bandwidth of the logical port. For this reason, the value that the system displays in the Logical Port Utilization field can exceed 100%.*
>
> *If the link management interface (LMI) protocol is disabled, the system does not display any DTE or DCE statistics for the logical port. You specify the LMI interface protocol when you define the parameters for a logical port. Refer to the* Network Configuration Guide for B-STDX/STDX *for more information about defining the LMI protocol for a frame relay logical port.*

Frame Relay Logical Port Summary Statistics

Table 6-6 lists and describes the frame relay logical port summary statistics shown in Figure 6-6. Table 6-6 includes DTE as well as DCE statistics. The type of statistics that the system displays for a logical port depend on the type of logical port you are using:

UNI-NNI logical port – the system displays both DTE as well as DCE statistics.

UNI-DCE logical port – the system displays only DCE statistics.

UNI-DTE logical port – the system displays only DTE statistics.

Table 6-6. Frame Relay Logical Port Summary Statistics

Field	Description
Identifying Fields	
Switch Name	The name of the switch associated with the logical port.
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. Refer to "Setting the Polling Interval" on page 5-1 for details about how to set this value.
Cumulative Statistics	
Number of Octets	The total number of octets (bytes) received and transmitted since the last reset.
Number of Packets	The total number of packets (frames) received and transmitted since the last reset.
Packets Discarded	The total number of packets (frames) received and discarded since the last reset. This value is specified in the Received column.

Table 6-6. Frame Relay Logical Port Summary Statistics (Continued)

Field	Description
Packet Errors	The total number of packet (frame) errors received since the last reset. This value is specified in the Received column.
Throughput Statistics	
Bits per second	The total number of bits received and transmitted each second.
Packets per second	The total number of packets (frames) received and transmitted each second.
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). If the system displays any value other than zero for this field it is an indication of a problem.

Table 6-6. Frame Relay Logical Port Summary Statistics (Continued)

Field	Description
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. If the system displays any value other than zero for this field, it is an indication of 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.
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).
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.

Table 6-6. Frame Relay Logical Port Summary Statistics (Continued)

Field	Description
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) wasn't received during a T392 second interval. • 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. If the system displays any value other than zero for this field, it is an indication of 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.

Table 6-6. Frame Relay Logical Port Summary Statistics (Continued)

Field	Description
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. 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.
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.
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). It does not measure the amount of bandwidth of the logical port. For this reason, the value that the system displays in this field can exceed 100%.

Verifying a Problem With a Frame Relay Logical Port

You can use the Frame Relay Logical Port Summary Statistics dialog box (Figure 6-6) to verify whether or not you have a logical port problem.

Use the following steps to check for a logical port problem:

1. Display the Logical Port Summary Statistics dialog box. Refer to "Displaying Logical Port Summary Statistics" on page 6-7 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 6-6 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. If these exist, there is a problem with the logical port.

ATM IWU Logical Port Summary Statistics Example

Figure 6-7 illustrates the logical port summary statistics for ATM IWU modules.

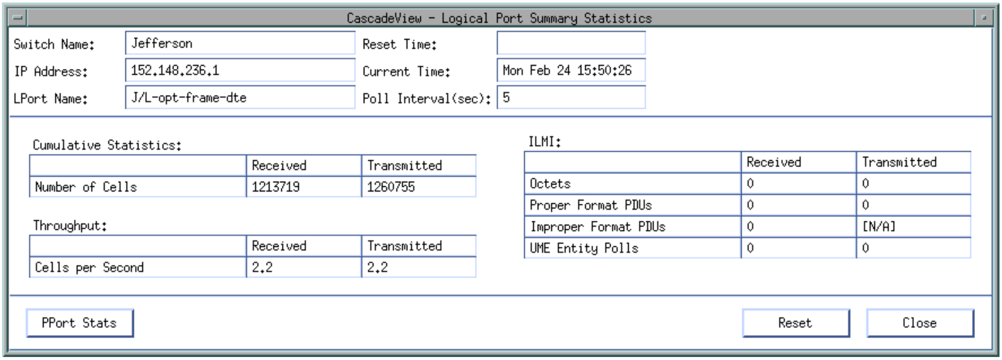


Figure 6-7. ATM IWU Logical Port Summary Statistics

ATM IWU Logical Port Summary Statistics

Table 6-7 lists and describes the ATM IWU logical port summary statistics shown in Figure 6-7.

Table 6-7. ATM IWU Logical Port Summary Statistics

Field	Description
Cumulative Statistic	
Number of Cells	The total number of cells received and transmitted by the port since the last reset.
Throughput Statistic	
Cells per Second	The total number of cells received and transmitted by the port each second.
ILMI Statistics	
Octets	The total number of octets received and transmitted by the port each second.
Proper Format PDUs	The total number of Protocol Data Units (PDUs) that were received with a proper format and transmitted.
Improper Format PDUs	The total number of Protocol Data Units (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.

7

Channelized DS3 Statistics

Channelized DS3 Summary Statistic Options

You can generate the following types of statistics for the channelized DS3 module:

Physical Port Summary Statistics — Shows the octets and frames being sent and received over the selected physical port, and displays DS3 summary statistics.

DS3 Link Performance — Shows the error codes received by the selected physical port and displays cumulative statistics for all 28 T1 ports.

Channel Alarm Status — Shows the bits and frames being sent and received over the selected channel, and displays DS1 summary statistics and the channel alarm status for 28 channels.

Selecting Statistics Options

You select each of the channelized DS3 summary statistic options from the Show Physical Port Attributes dialog box.

Use the following steps to display the Show Physical Port Attributes dialog box for a channelized DS3 module:

1. On the network map, select the appropriate switch icon. The selected object appears highlighted.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The system then displays the Switch Back Panel dialog box.
3. Select the physical port. The system then displays the Show Physical Port Attributes dialog box (Figure 7-1)

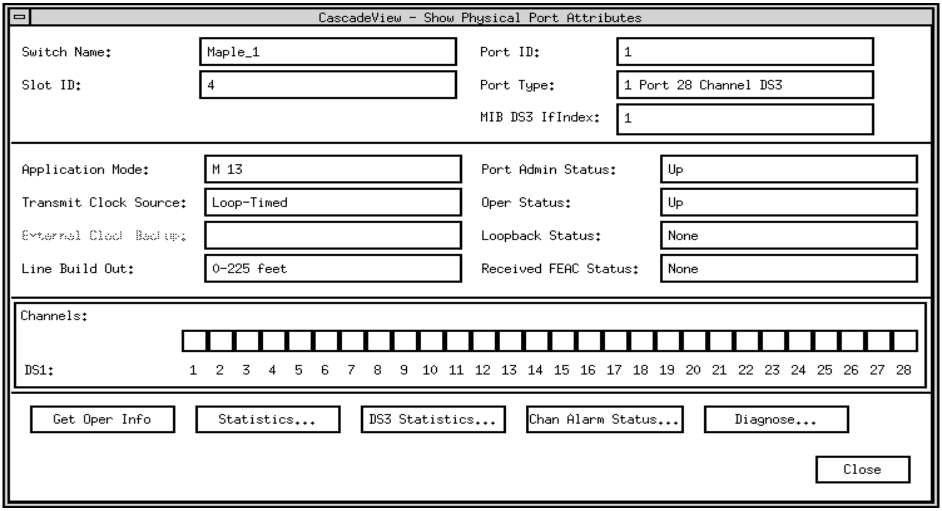


Figure 7-1. Channelized DS3 Show Physical Port Attributes Dialog Box

Table 7-1. Show Physical Port Attributes Fields

Field	Action/Description
Switch Name	The name of the switch associated with the logical port.
Port ID	The number associated with the logical port.
Slot ID	I/O slot number where the module resides.
Port Type	Logical port configuration type.
MIB DS3 IfIndex	Interface number used for link performance statistics.
Application Mode	The DS3 signal is partitioned into M-frames of 4760 bits each. The M-frames are divided into seven M-subframes of 680 bits. The first C-bit in M-subframe 1 is used as an application identification channel (AIC) to identify the specific DS3 M-frame. This determines the mode of operation for a DS3 signal. Options include: *M13 (default)* – Uses C-bits in a frame to indicate the presence or absence of stuffing bits. *C-bit Parity* – Uses the first C-bit in M-subframe 1 to identify the format as C-bit parity.
Transmit Clock Source	The transmit clock source for the channelized DS3 module. The DS3 receive clock is independent from the DS3 transmit clock. 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 a DS1 clock source. This source drives a phased locked loop circuit to provide DS3 clocking. If you select this option, you should also set an external backup clock source.

Table 7-1. Show Physical Port Attributes Fields (Continued)

Field	Action/Description
Line Build Out	The distance measurement from the channelized DS3 module to the network equipment. Options include: 0 - 225 feet (Default) 225 - 450 feet
Port Admin Status	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 off-line so that diagnostics can be run to test the port. A logical port with an Admin Status of *Down* is not operational.
Oper Status	Indicates 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	*(DS3 only)* The default value for this field is *none*. If you enable diagnostic loopback tests, this field displays the DS3 card's loopback status. A loopback test enables you to test the physical path for data transmission by looping back traffic in one or both directions. For more information about loopbacks, see Chapter 4, "Loopbacks".
Received FEAC Status	Displays the FEAC (Far-End Alarm and Control) status received by the physical port, if C-bit parity is enabled. This field indicates the status of the physical port on the other end of the connection. If you are using M13, this field displays *None*.
Channels	Channels are located between the physical port and logical port layers. Each channel supports one user logical port (with the exception of OPTimum trunk logical ports). Each physical port is divided into 28 fractional T1 channels. Each DS1 channel contains 24 DS0 channels.

Displaying Channel Alarm Status

The Channel Alarm Status dialog box displays the alarm status for all 28 DS1 channels. To display the alarm status:

1. From the Show Physical Port Attributes dialog box (see Figure 7-1) choose Chan Alarm Status. The Channel Alarm Status dialog box appears as shown in Figure 7-2.

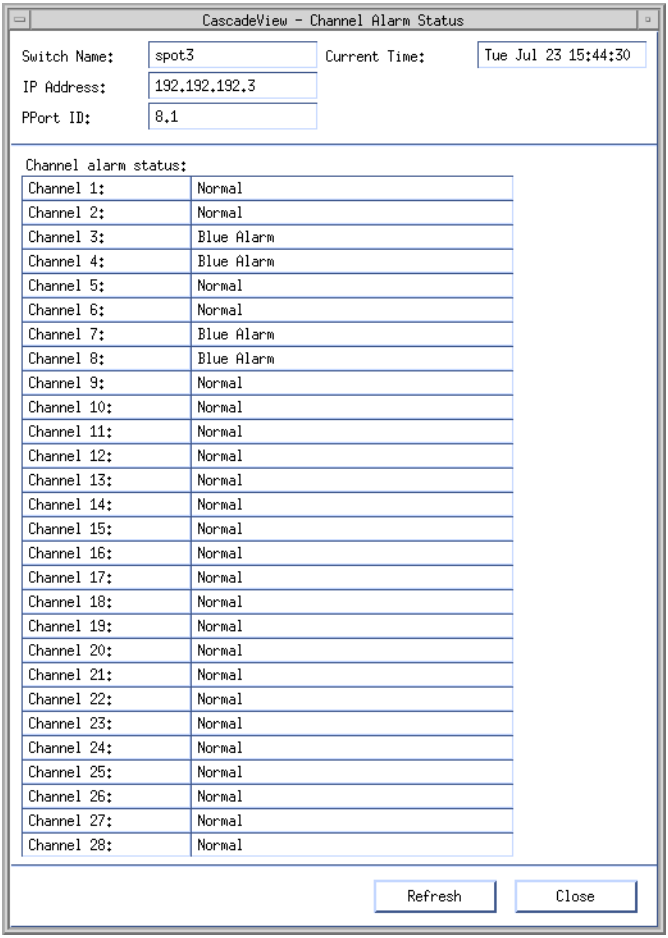


Figure 7-2. Channel Alarm Status Dialog Box

The Channel Alarm Status dialog box also displays the alarm status of the 28 DS1 channels. Table 7-2 lists and describes the alarm states.

Table 7-2. DS1 Channel Alarm States

Alarm State	Description/Indication
Normal	Normal operating state
Red	Loss of frame or loss of signal
Yellow	Far end is in red alarm
Blue	Down stream equipment failure

2. Choose Refresh to clear the alarm status.
3. Choose Close to exit. The Set Physical Port Attributes dialog box reappears.

Displaying DS3 Link Performance Statistics

The DS3 Statistics feature displays link performance statistics on the signal quality of the DS3. Statistics are displayed in 15-minute intervals for up to 24 hours (for a total of 96 intervals). The DS3 Statistics feature provides information such as the number of seconds the link was in error and the number of seconds the link was down.

To display DS3 statistics:

1. From the Show Physical Port Attributes dialog box, select DS3 Statistics (see Figure 7-1 on page 7-2). The DS3 Statistics dialog box appears as shown in Figure 7-3.

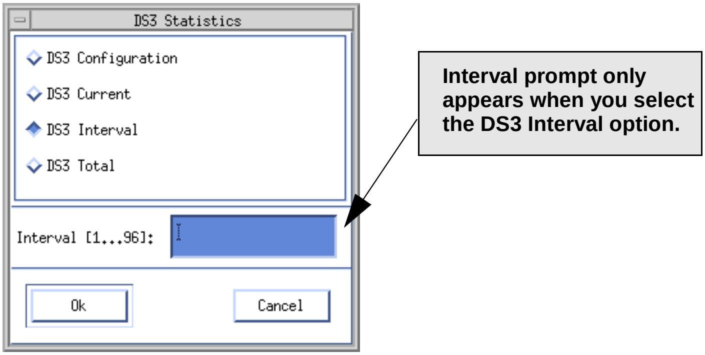


Figure 7-3. DS3 Statistics Dialog Box

2. Select from the following types of statistics and choose OK. A DS3 Statistics dialog box appears, depending on your selection.

   All DS3 Statistics dialog boxes display error and performance information (for a specified time period), based on your selection.

   DS3 Configuration — Displays DS3 MIB table information in the form of configuration statistics. Refer to the next section for more information.

   DS3 Current — Displays statistics accumulating in the present interval. Refer to "DS3 Current Statistics" on page 7-13 for more information.

DS3 Interval — Displays statistics that were collected during a previous 15 minute interval. 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 CascadeView. Specify a number between 1 and 96 in the Interval [1...96] field. (For example, interval 4 displays statistics from the previous hour.) Refer to "DS3 Interval Statistics" on page 7-14 for more information.

DS3 Total — Displays statistics for the *sum* of all intervals and the current interval. Refer to "DS3 Total Statistics" on page 7-15 for more information.

All DS3 Statistics dialog boxes display the following information:

Switch Name — The name of the switch in which the channelized DS3 module resides.

IP Address — IP Address of the switch in which the module resides.

PPort ID — Port number of the selected port.

Current Time — Current time.

DS3 Configuration Statistics

The DS3 Configuration Statistics dialog box lists the error and performance event variables.

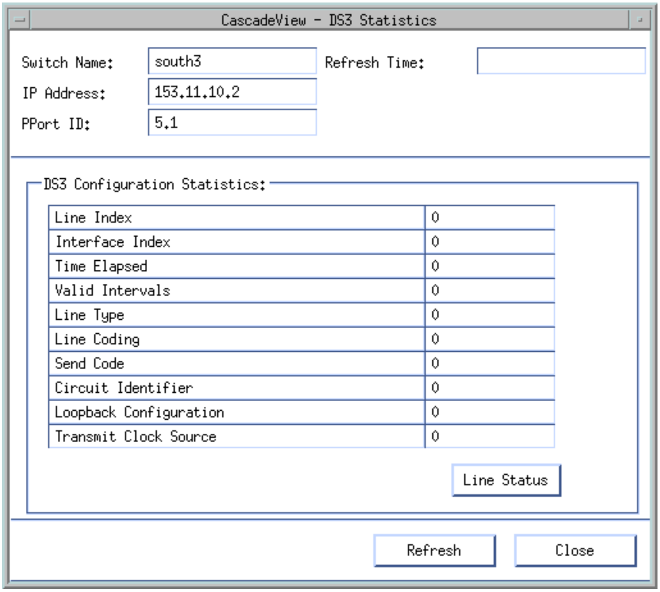


Figure 7-4. DS3 Configuration Statistics

Table 7-3 lists and describes the DS3 configuration statistics and performance event variables.

Table 7-3. DS3 Configuration Statistics and Variables

Variable	Description
Line Index	Displays the line index value for this interface.
Interface Index	The unique interface number for this interface on the switch.
Time Elapsed	Displays the number of elapsed seconds since the beginning of the measurement period.
Valid Intervals	Displays the number of previous near-end intervals for which valid data was collected. The value is 96. (If the interface was brought on-line within the last 24 hours, the value will be the number of complete 15-minute near-end intervals since the interface has been on-line.)
Line Type	Indicates the variety of DS3 C-bit applications implementing this interface. The DS3 rate is 44.736 Mbps. Options include: M23 mode C-bit Parity
Line Coding	Describes the variety of Zero Code Suppression used on this interface (B3ZS).
Send Code	Indicates the type of code the device is sending across the DS3 interface.

Table 7-3. DS3 Configuration Statistics and Variables (Continued)

Variable	Description
Circuit Identifier	Contains the transmission vendor’s circuit identifier (used for troubleshooting).
Loopback Configuration	Represents the DS3 loopback configuration.
Transmit Clock Source	Indicates the source of transmit clock. Transmit clock is derived from the recovered receive clock of another DS3 interface.

3. Choose the Line Status option to display the DS3 Configuration Line Status as shown in Figure 7-5.

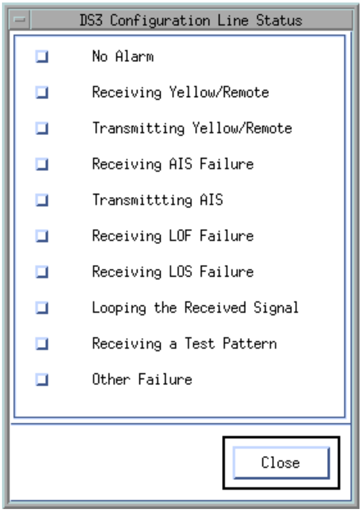


Figure 7-5. DS3 Configuration Line Status

The Channel Alarm Status dialog box also displays the alarm status of the 28 DS1 channels. Table 7-4 lists and describes the DS3 line status values.

Table 7-4. DS1 Channel Alarm States

Line Status Value	Description/Indication
No Alarm	Normal operating state
Receiving Yellow/Remote	The loopback far end is in a red alarm state.
Transmitting Yellow/Remote	The loopback near end is in a red alarm state (due to loss of signal (LOS) or loss of frame (LOF).
Receiving AIS Failure	Receiving Alarm Indication Signal (AIS). The loopback far end is in a local loopback state.
Transmitting AIS	Transmitting Alarm Indication Signal (AIS). The local loopback is enabled, transmitting AIS to the loopback far end.
Receiving LOF Failure	Receiving Loss of Frame (LOF). This is a red alarm condition.
Receiving LOS Failure	Receiving Loss of Signal (LOS). This is a red alarm condition.
Looping the Received Signal	The channel is in a near-end loopback state.
Receiving a Test Pattern	The far end of the channel is in a loopback state and has sent a test pattern. Monitor the channel for line errors.

DS3 Current Statistics

The DS3 Current Statistics dialog box provides up-to-date statistical information for the current 15-minute interval. Refer to Appendix B for more information on DS3 current statistics and variables.

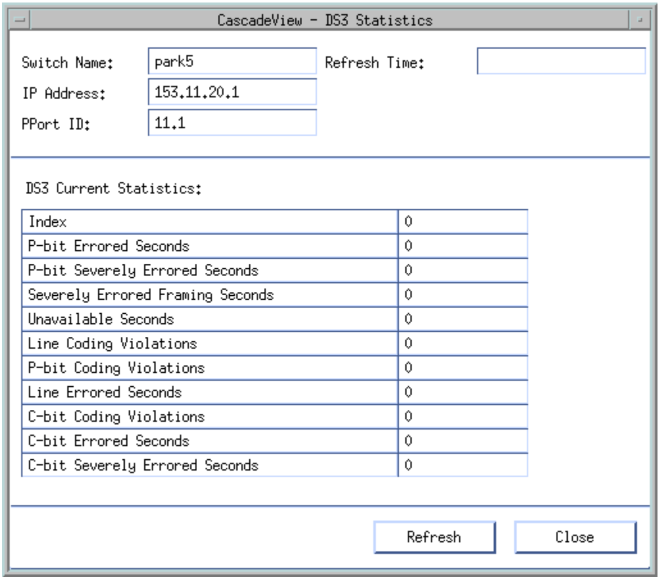


Figure 7-6. DS3 Current Statistics Dialog Box

DS3 Interval Statistics

The DS3 Interval Statistics dialog box provides statistical information on the last 24 hours of operation. The last 24 hours are broken down into 96 completed 15-minute intervals.

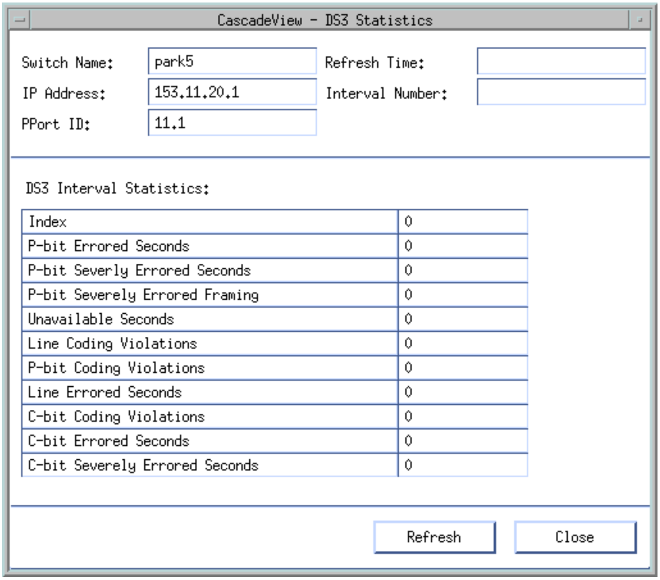


Figure 7-7. DS3 Interval Statistics Dialog Box

DS3 Total Statistics

The DS3 Total Statistics dialog box provides statistical information for the sum of all intervals and the current interval. Refer to Table B-3 for more information on DS3 total statistics and variables.

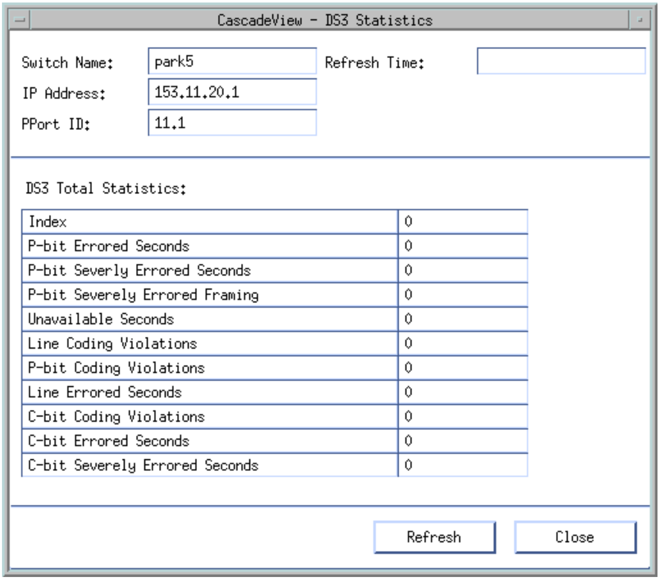


Figure 7-8. DS3 Total Statistics Dialog Box

Displaying Channel Summary Statistics

The Statistics option in the Set Channel Attributes dialog box displays the summary statistics for the selected DS1 channel.

To display channel summary statistics:

1. From the Show Physical Port Attributes dialog box, double-click the channel button ID for which you want to display DS1 summary statistics. The Channel Attributes dialog box appears as shown in Figure 7-9.

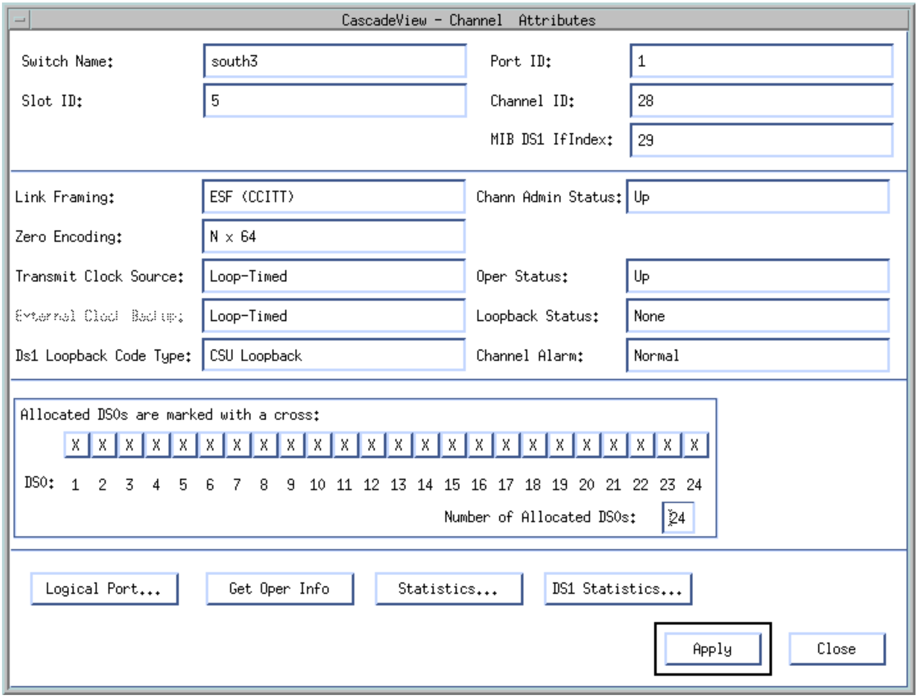


Figure 7-9. Channel Attributes Dialog Box

2. Select Statistics. The Channel Summary Statistics dialog box appears as shown in Figure 7-10.

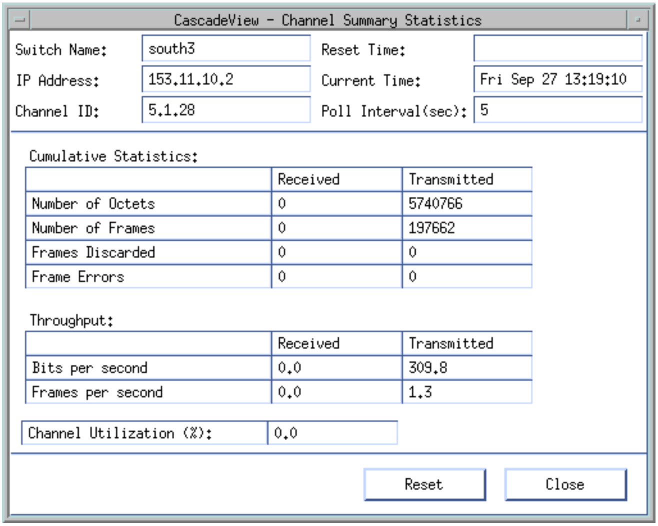


Figure 7-10. Channel Summary Statistics Dialog Box

The Channel Summary Statistics dialog box displays the Cumulative and Throughput statistics. Table 7-5 describes each of the Channel Summary Statistics fields.

Table 7-5. Channel Summary Statistics Fields

Field	Action/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.

Displaying DS1 Link Performance Statistics

The DS1 Statistics command button on the Set Channel Attributes dialog box displays channel summary statistics and link performance statistics on the signal quality of the DS1 channel. Statistics are displayed in 15-minute intervals for up to 24 hours (for a total of 96 intervals). The DS1 Statistics function provides information such as the number of seconds the link was in error and the number of seconds the link was down.

To display DS1 link performance statistics:

1. From the Set Physical Port Attributes dialog box, double-click the channel button ID or select a channel for which you want to display DS1 performance statistics and choose Set Chan Attr. The Channel Attributes dialog box appears as shown in Figure 7-9 on page 7-16.

2. Select DS1 statistics. The DS1 Statistics dialog box appears as shown in Figure 7-11.

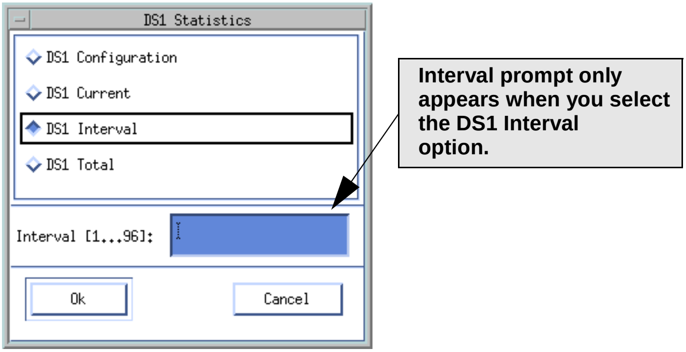


Figure 7-11. DS1 Statistics Dialog Box

3. Select from the following types of statistics and choose OK. A DS1 Statistics dialog box appears depending on your selection.

   All DS1 Statistics dialog boxes display error and performance information (for a specified time period), based on your selection.

   DS1 Configuration — Displays DS1 MIB table information, including error and performance variables. See "DS1 Configuration Statistics" on page 7-21.

DS1 Current — Displays statistics accumulating in the present interval. See "DS1 Current Statistics" on page 7-23.

DS1 Interval — Displays statistics that were collected during a previous 15-minute interval. 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 CascadeView. Specify a number between 1 and 96 in the Interval [1...96] field. (For example, interval 4 displays statistics from the previous hour). Refer to "DS1 Interval Statistics" on page 7-24.

DS1 Total — Displays statistics for the sum of all intervals and the current interval. Refer to "DS1 Total Statistics" on page 7-25.

All DS1 Statistics dialog boxes display the following information. Table 7-6 describes the DS1 Statistics fields.

Table 7-6. DS1 Statistics Fields

Field	Action/Description
Switch Name	Name of the switch in which the channelized DS3 module resides.
IP Address	IP Address of the switch in which the module resides.
Channel ID	Channel number of the selected Channel.
Current Time	Current time.

DS1 Configuration Statistics

The DS1 Configuration Statistics dialog box lists the MIB table definitions including the DS1 configuration error and performance event variables.

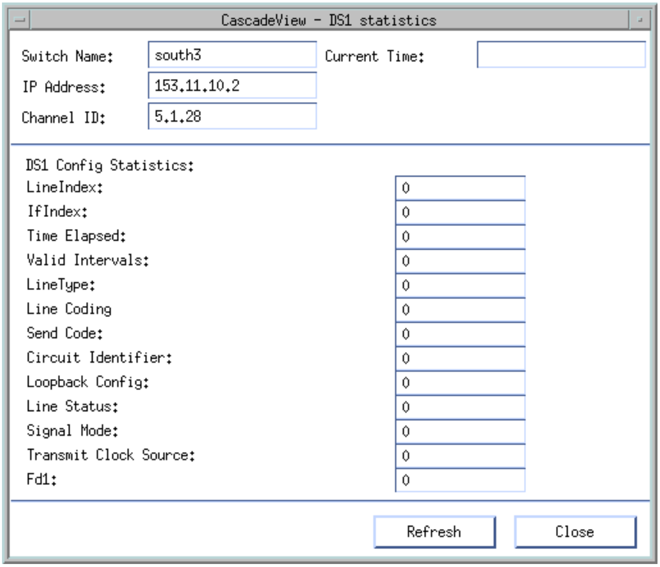


Figure 7-12. DS1 Configuration Statistics Dialog Box

Table 7-7 lists and describes the DS1 Configuration statistics and variables.

Table 7-7. DS1 Configuration Statistics and Variables

Variable	Description
Line Index	Displays the line index value for this interface.
IfIndex	The unique interface number for this interface on the switch.
Time Elapsed	Displays the number of elapsed seconds since the beginning of the current error-measurement period.
Valid Intervals	Displays the number of previous intervals for which valid data was collected.
LineType	Displays the variety of DS1 Line implementing this circuit.
Line Coding	The variety of Zero Code Suppression used on the link.
Send Code	Indicates the type of code the device is sending across the DS1 interface.
Circuit Identifier	Contains the transmission vendor’s circuit identifier (used for troubleshooting).
Loopback Config	Represents the loopback configuration of the DS1 interface.
Line Status	Indicates the interface lines status.
Signal Mode	The signal application mode. Refer to the *Network Configuration Guide for B-STDX/STDX* for details.
Transmit Clock Source	Indicates the source of transmit clock.

DS1 Current Statistics

The DS1 Current Statistics dialog box provides up-to-date statistical information. See Table B-4 on page B-6 for more information on DS1 current statistics and variables.

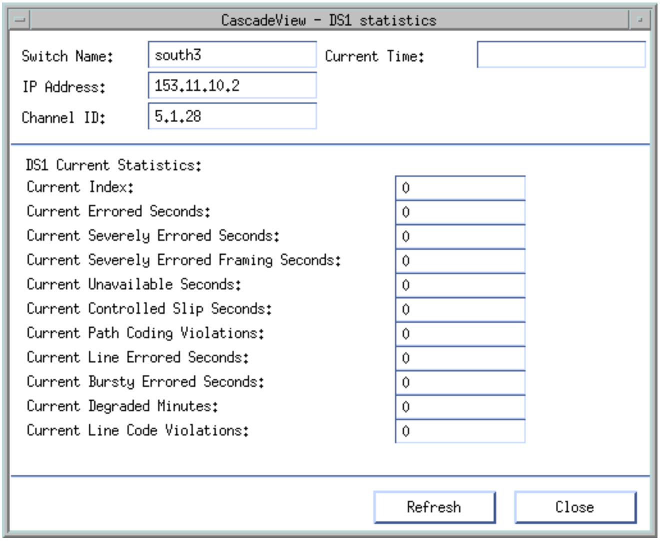


Figure 7-13. DS1 Current Statistics Dialog Box

DS1 Interval Statistics

The DS1 Interval Statistics dialog box provides statistical information on the last 24 hours of operation. The last 24 hours are separated into 96 completed 15-minute intervals. Refer to Table B-5 on page B-8 for more information on DS1 interval statistics and variables.

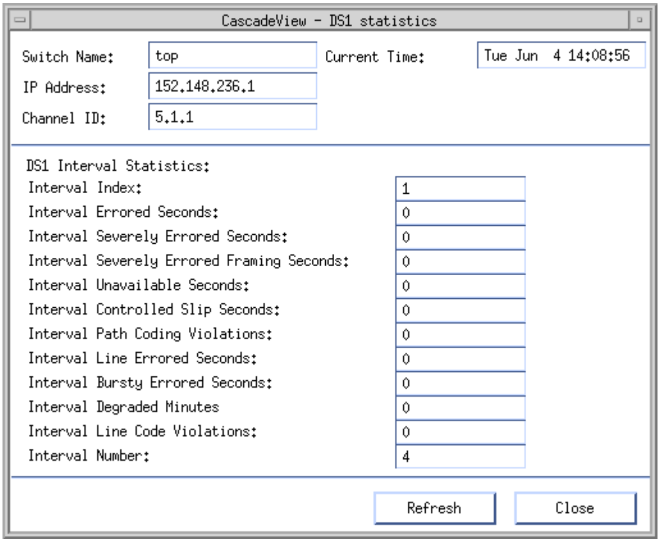


Figure 7-14. DS1 Interval Statistics Dialog Box

DS1 Total Statistics

The DS1 Total Statistics dialog box provides statistical information for the sum of all intervals and the current interval. Refer to Table B-6 on page B-9 for more information on DS1 total statistics and variables.

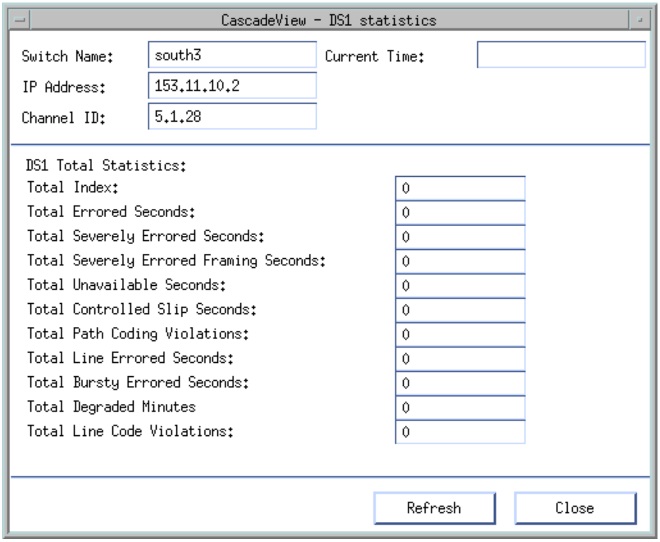


Figure 7-15. DS1 Total Statistics Dialog Box

Error Events

All DS3 and DS1 Statistics dialog boxes display error events. Table 7-8 lists and describes generic error events. For a complete list of current, interval, and total statistics and error events, refer to Appendix B.

Table 7-8. Error Events

Error Event	Description
Line Coding Violation (LCV)	A count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) occurring over the accumulation period.
P-bit Coding Violation (PCV)	A coding violation error event is a P-bit Parity Error event.
Parity Error Event	The occurrence of a received P-bit code on the DS3 M-frame that is not identical to the locally calculated code.
C-bit Coding Violation (CCV)	The number of coding violations reported via the C-bits.

Performance Parameters

All DS3 and DS1 Statistics dialog boxes display performance parameters. Table 7-9 lists and describes generic performance parameters. For a complete list of current, interval, and total statistics and performance parameters, refer to Appendix B.

Table 7-9. Performance Parameters

Performance Parameter	Description
Line Errored Seconds (LES)	A second in which one or more coding violations (CV) or one or more loss of signal (LOS) defects occurred.
P-bit Errored Seconds (PES)	A second with one or more CVs, Out of Frame defects, or a detected incoming Alarm Indication Signal (AIS).
C-bit Errored Seconds (CES)	A second with one or more CCVs, Out of Frame defects or a detected incoming Alarm Indication Signal (AIS).
C-bit Severely Errored Seconds (CSES)	A second with 44 or more CCVs, one or more Out of Frame defects, or a detected incoming Alarm Indication Signal (AIS).
Severely Errored Framing Seconds (SEFS)	A second with one or more Out of Frame defects or a detected incoming Alarm Indication Signal (AIS).
Unavailable Seconds (UAS)	The number of seconds the interface is unavailable.

8

Trunk and Circuit Statistics

This chapter describes the following types of summary statistics:

- Trunk Summary Statistics
- Circuit Summary Statistics
- Circuit Quality of Service (QoS) Statistics

Displaying Trunk Summary Statistics

To display summary statistics for a selected trunk:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Trunks. The system then displays the Show All Trunks dialog box.
2. In the Defined Trunk Names list, select the name of the trunk from which you want to retrieve statistics information and choose the Statistics option. The system then displays the Trunk Summary Statistics dialog box (Figure 8-1).

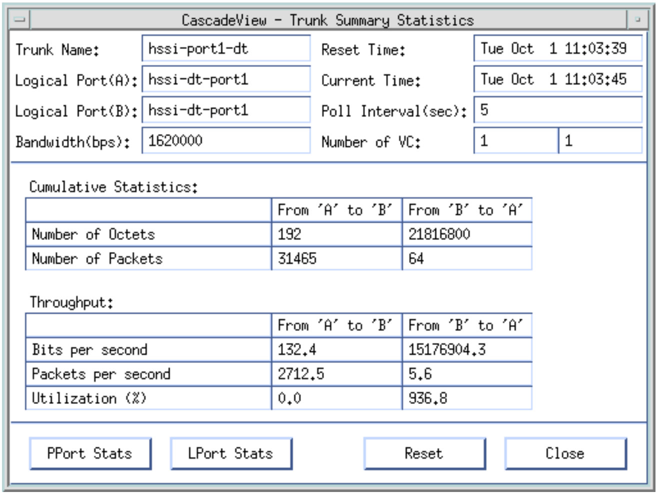


Figure 8-1. Trunk Summary Statistics Dialog Box

Table 8-1 lists and describes each of the Trunk Summary Statistics fields.

3. When you finish reviewing the trunk statistics you can use any one of the following command buttons:

Use	To
PPort Stats	Display the physical port statistics for both ends of the trunk.
LPort Stats	Display the logical port statistics for both ends of the trunk.
Reset	Reset the displayed values to zero.

Table 8-1. Trunk Summary Statistics Fields

Field	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. 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. Refer to “Setting the Polling Interval” on page 5-1 for details about how to set this value.
Cumulative Statistics	
Number of Octets	The total number of octets (bytes) received and transmitted since the last reset.
Number of Packets	The total number of packets (frames) received and transmitted since the last reset.
Throughput Statistics	
Bits per second	The total number of bits received and transmitted each second.
Packets per second	The total number of packets (frames) received and transmitted each second.
Utilization (%)	The utilization is based on the percentage of the logical port buffer space currently used.

Displaying QOS Statistics for ATM Direct Cell Trunks

To display Quality of Service (QOS) statistics for ATM direct cell trunks:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Trunks. The system then displays the Show All Trunks dialog box.

2. Select the trunk name from the Defined Trunk Names group box.

3. Choose View QoS Parameters. The system then displays the Show Logical Port QoS Parameters dialog box shown in Figure 8-2.

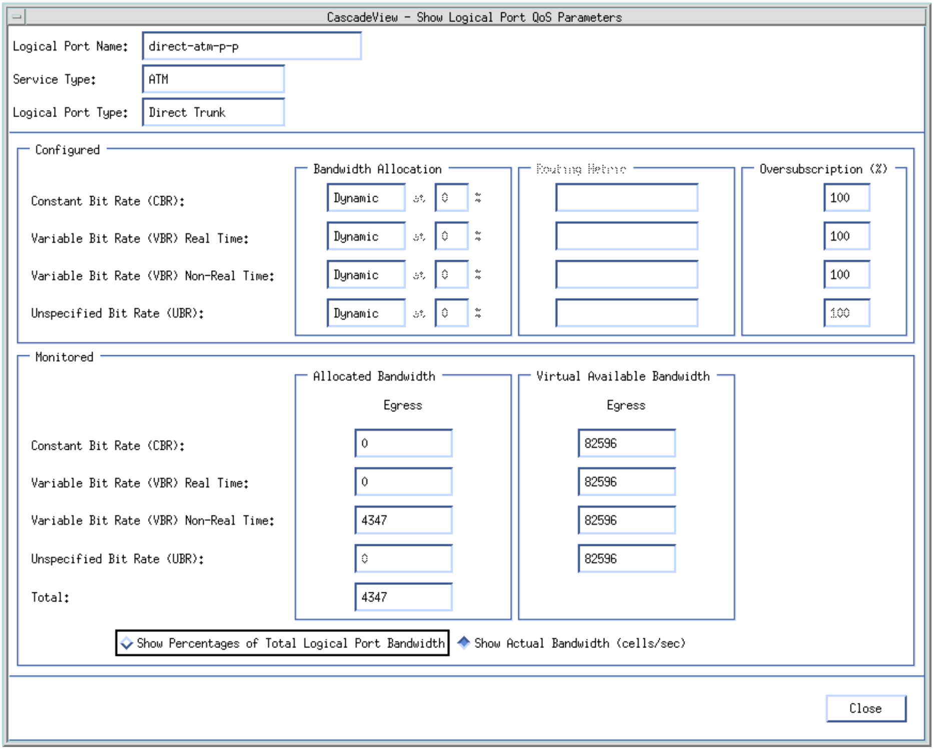


Figure 8-2. Show Logical Port QoS Parameters Dialog Box

Table 8-2 describes each of the fields on the Show Logical Port QoS Parameters dialog box.

Table 8-2. ATM Direct Cell Trunk QoS Statistics

Field	Description
Identification Fields	
Logical Port Name	The name that identifies the logical port.
Service Type	Displays ATM as the service type.
Logical Port Type	Displays Direct Trunk as the logical port type.
Class of Service	
Constant Bit Rate	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	For packaging special delay-sensitive applications, such as packet video, that require low cell delay variation between endpoints.
Variable Bit Rate (VBR) Non-Real Time	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. CBX 500 CPE protocols adjust for any delay or loss incurred through the use of VBR non-real time.
Unspecified Bit Rate (UBR)	Primarily used for LAN traffic. The CBX 500 CPE should compensate for any delay or lost cell traffic.

Table 8-2. ATM Direct Cell Trunk QoS Statistics (Continued)

Field	Description
QoS Parameters	
Bandwidth Allocation	Displays *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. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information about these values.
Oversubscription	Displays 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. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information about oversubscription.

Table 8-2. ATM Direct Cell Trunk QoS Statistics (Continued)

Field	Description
Allocated Bandwidth (Egress)	Displays the allocated bandwidth as a percentage of total logical port bandwidth or as the actual bandwidth (in cells per second) depending on the option that you select at the bottom of the dialog box.
Virtual Available Bandwidth	Displays 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 that you select at the bottom of the dialog box.

Displaying QOS and Summary Statistics for Circuits

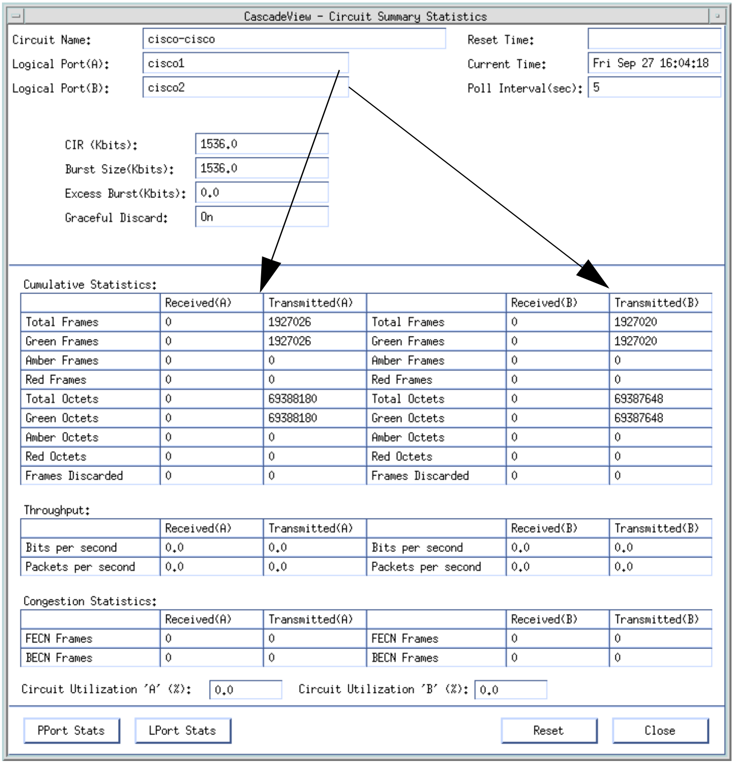
To display Summary Statistics or Quality of Service (QOS) statistics for circuits:

1. From the Monitor menu, select Cascade Objects ⇒ Show Circuits ⇒ All on Map. The system then displays the Show All PVCs on Map dialog box.
2. Select a circuit from the Defined Circuit Name group box. You can 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. Perform one of the following steps:
   a. Choose **Statistics** to display Circuit Summary Statistics. The system then displays the Circuit Summary Statistics dialog box shown in Figure 8-3.

   b. Choose **QOS** to display Quality of Service Statistics. The system then displays the Circuit Quality of Service Statistics dialog box shown in Figure 8-4.

Circuit Summary Statistics Example

Figure 8-3 illustrates the statistics that CascadeView/UX provides for a selected circuit.



Logical Port A is reported as A. Logical Port B is reported as B.

Figure 8-3. Circuit Summary Statistics Dialog Box

> *The circuit utilization fields in the Circuit Summary Statistics dialog box measure the amount of traffic queued for transmission on a circuit as a percentage of the committed information rate (CIR). For this reason the value displayed in circuit utilization 'A' or 'B' can exceed 100%.*

Circuit Summary Statistics Description

The Circuit Summary Statistics dialog box (Figure 8-3) display statistics data in separate columns to reflect the transmission and receipt of data on each side of the circuit. CascadeView/UX stamps the individual frames with a color coding scheme to differentiate the way frames are handled in the event of network congestion. (Refer to the *Cascade Networking Services Technology Overview* for more information about congestion control).

The Circuit Summary Statistics dialog box provides the following three types of statistics:

- **Cumulative statistics** list the number of each type of frame and whether those frames are being transmitted or dropped due to conditions in the network.
- **Throughput statistics** display the frames per second and bits per second for each side of the circuit.
- **Congestion statistics** indicate whether or not the FECN or BECN bit is set on frames being transmitted and received.

Table 8-3 lists and describes the circuit summary identification fields and statistics shown in Figure 8-3.

Table 8-3. Circuit Summary Statistics

Statistic	Description
Cumulative Statistics	
Total Frames	The total number of frames received and transmitted over the specified logical ports since the last reset.
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	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	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	The total number of octets (bytes) received and transmitted over the specified logical ports since the last reset.
Green Octets	Green octets are never discarded by the network, except under extreme circumstances (such as node or link failure).
Amber Octets	Amber octets are eligible for discard if they pass through a congested node.

Table 8-3. Circuit Summary Statistics (Continued)

Statistic	Description
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.
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. Refer to the *Cascade Networking Services Technology Overview* for more information about FECN frames and congestion control.
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. Refer to the *Cascade Networking Services Technology Overview* for more information about FECN frames and congestion control.

Table 8-3. Circuit Summary Statistics (Continued)

Statistic	Description
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%.

Circuit Quality of Service Statistics Example

Figure 8-4 illustrates the Circuit Quality of Service (QOS) Statistics dialog box.

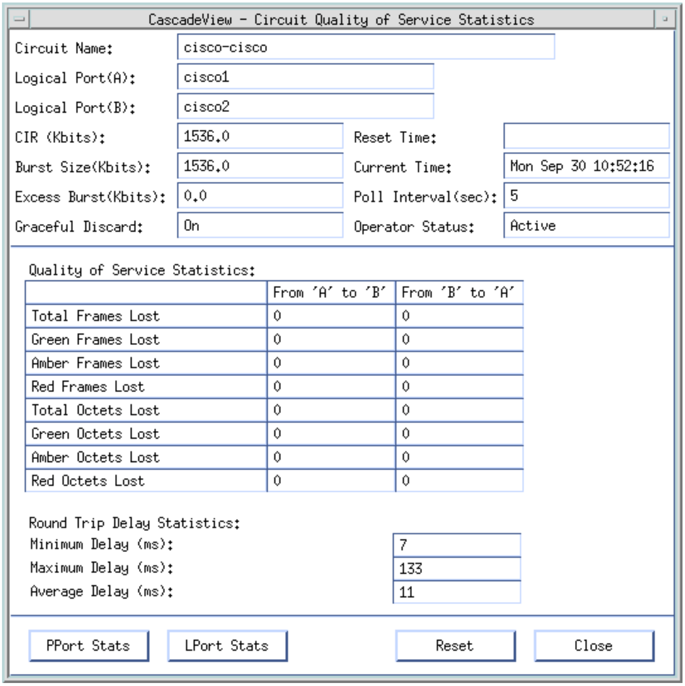


Figure 8-4. Circuit Quality of Service Dialog Box

Circuit Quality of Service Descriptions

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. Table 8-4 describes each of the Circuit Quality of Service Summary Statistics.

Table 8-4. Circuit Quality of Service Statistics

Statistic	Description
Configuration Information	
Circuit Name	The name that identifies the circuit.
Logical Port A	The logical port that is defined as endpoint 1 of the circuit configuration.
Logical Port B	The logical port that is 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. CascadeView/UX manages DE frames according to the Graceful Discard setting.

Table 8-4. Circuit Quality of Service Statistics (Continued)

Statistic	Description
Graceful Discard	Displays either *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. Refer to "Setting the Polling Interval" on page 5-1 for details about how to set this value.
Operator Status	The operational status of the PVC. There are four possible values: *Active* – Indicates that the PVC is operational between the two endpoints. *Inactive* – Indicates that the PVC is not operational between the two endpoints. *Invalid* – Indicates that the PVC configuration is not contained within the calling node. *Unknown* – Indicates that the calling node did not respond to the NMS request for the status of this PVC.

Table 8-4. Circuit Quality of Service Statistics (Continued)

Statistic	Description
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.
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).

Table 8-4. Circuit Quality of Service Statistics (Continued)

Statistic	Description
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) to transfer a packet from point A to point B of a circuit and then back to point A.
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.
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.

The collection of the Circuit QoS statistics is based on a poll timer variable set. This variable affects the frequency at which the NMS polls the switch for QOS statistics. Although the default value is set to 5 seconds, you can change this default by using the Change Statistics Polling Interval dialog box shown in Figure 5-1 on page 5-2.

The NMS polls the switch every 60 seconds for the Round Trip Delay statistics. For this reason, the Round Trip Delay statistics values will not change as often as the other Circuit QOS statistics. You cannot set the polling interval for Round Trip Delay statistics.

9

Monitoring MIB Values

This chapter introduces the Management Information Base (MIB) and describes how to use the Cascade MIB Browser to navigate through the Cascade MIB.

MIB Overview

The MIB is a repository of objects that represent the devices in the network and their internal components. Common MIB objects include:

- Counters of packets sent
- Connections used
- Connections attempted

SNMP Structure of Management Information

The Cascade MIB uses the SNMP Structure of Management Information (SMI) as the set of rules that define the MIB structure. This set of rules specifies that the text format of each object in the MIB should use the following structure:

Object Type — 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}
```

would indicate 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 complete list of Cascade MIB definitions, refer to the *Cascade 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 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 CCITT.

> *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 Cascade 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 would specify the object identifier for the path to the Cascade MIB.

```
1.3.6.1.4.1.277
```

Refer to the *Cascade Enterprise MIB Definitions* for specific information about the OID values for each Cascade variable. The OID string for each variable is always 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.

Cascade MIB

The Cascade MIB is identified by the group name *cascade*. Below cascade (which has an object ID of 277) are the following groups:

Group	Object ID
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

Figure 9-1 on page 9-6 illustrates the Cascade MIB tree hierarchy, which shows the branches through the MIB that are used to access the Cascade MIB.

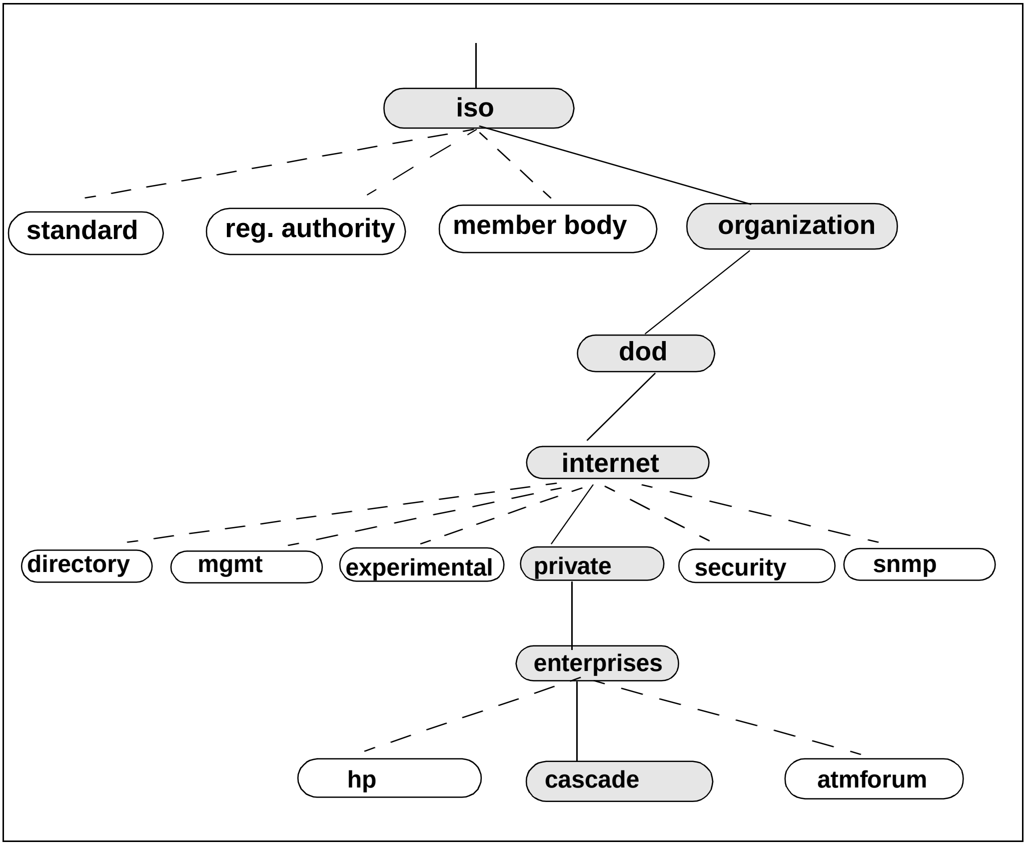


Figure 9-1. Cascade MIB Tree Hierarchy

cascfr Group

The cascfr group contains groups that all protocols share (including Frame Relay, SMDS, ATM, and ISDN). The following groups comprise the cascfr group:

Group	Description
net	Variables that are relevant to a Cascade network.
ase	The OSPF Autonomous System External device and host table for NMS paths.
node	The variables that configure a switch.
card	The variables that configure an intelligent card.
pport	The variables that configure a physical port.
lport	The variables that configure a logical port.
ckt	*(Frame Relay Only)* The variables that configure permanent virtual circuits (PVCs) on a port.
cascds1	The variables that specify DS1 channel information.
svcaddr	The variables that relate to Switched Virtual Circuit addressing (E.164).

Using the Cascade MIB Browser

The Management Information Base (MIB) Browser enables you to:

- Navigate through the CascadeView 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

When you use the MIB Browser, only specify one MIB value at a time. Attempting to retrieve more than one MIB value can cause an interruption in service.

Accessing Information in the Cascade MIB

The first step to using the MIB to access switch information is to determine the type of information that you need. Then you must identify the group that contains the information.

For example, if you wanted to use the MIB to check a card's Admin status you would have to look in the card group.

After you determine the group, the next step is to find the variable that 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 Browse MIB dialog box:

1. From the Misc menu, select SNMP MIB Browser. The system then displays the Browse MIB dialog box (Figure 9-2).

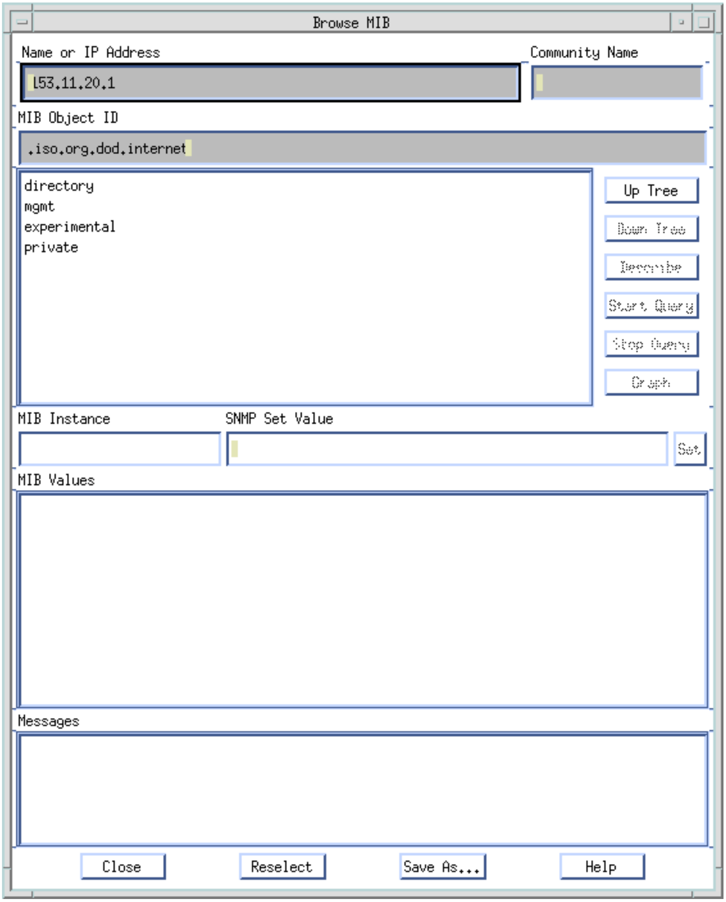


Figure 9-2. Browse MIB Dialog Box

The following list describes each of the options that you can select from the Browse MIB dialog box. Table 9-1 describes each of the Browse MIB fields.

Use	To
Up Tree	Move up the MIB tree to the previous MIB group.
Down Tree	Move down the MIB tree to the selected MIB group.
Describe	Display the Describe MIB Variable dialog box to display descriptive information about the selected object.
Start Query	Start a query on a specified object ID string.
Stop Query	Stop a query on a specified object ID string.
Graph	An HP OpenView function that is not supported.

Table 9-1. Browse MIB Fields

Field	Action/Description
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. Refer to *Cascade STDX and B-STDX MIB Definitions* for more information.
MIB Instance	Specific MIB instance of a selected category.
SNMP Set Value	When you perform a query on the MIB, the Browser displays the current SNMP set value. Reset this value by entering the new SNMP Set value in this field. Use the Describe option to check on the numeric SNMP Set values (You must enter a numeric value; for example, 1 may represent Enable and 2 could represent Disable).
MIB Values	Displays values that result from a query on an object.
Messages	Displays any resulting error or informational messages.

2. Select **private** as the MIB Object ID and choose the Down Tree option.

3. Select **enterprises** as the MIB Object ID and choose the Down Tree option.

4. Select **cascade** as the MIB Object ID and choose the Down Tree option. The system displays all of the possible cascade groups in the Browse MIB dialog box.

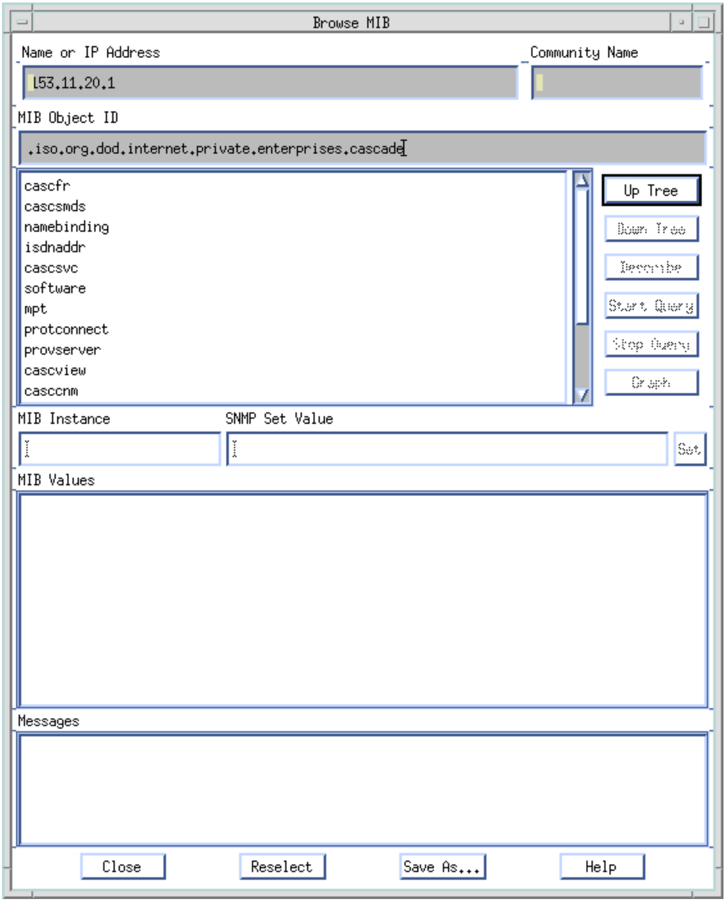


Figure 9-3. Displaying Groups in the Browse MIB Dialog Box

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.

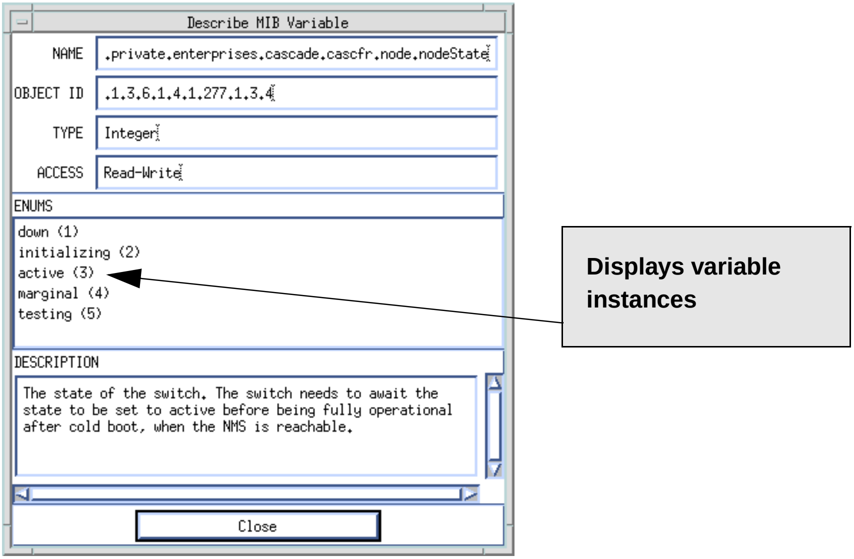


Figure 9-4. Describe MIB Variable Dialog Box

10

Trap Alarm Conditions

Trap alarm conditions notify the operator of events taking place on those switches that are configured to report to the NMS. You can display a list of currently-logged trap alarm conditions at any time by selecting the Cascade Events option from the Event Categories window. This chapter describes how to use the Event Categories window to display or delete events. This chapter also describes how you can add event categories and move events from one category to another. In addition, this chapter lists and describes each of the trap alarm conditions.

The Event Categories Window

The Event Categories window appears each time you run CascadeView/UX and it notifies you of any significant trap alarm conditions. This window has a button corresponding to each of the event categories, including Cascade Events. Figure 10-1 illustrates the Event Categories window.

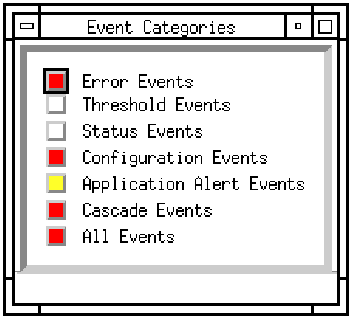


Figure 10-1. Event Categories Window

When a button in the Event Categories window changes color, it indicates that an event occurred on the network that relates to that category. The color of the button indicates the level of severity of the event in the category. Through the Network Node Manager (NNM) internal processes, the event is sent to a predefined category in the Events Browser. You can view the events by displaying the All Events Browser dialog box.

You can customize the Event Categories window by adding categories to the window. For example you may want to add a category that holds all acknowledged events or one that holds all canceled events. See “Adding Event Categories” on page 10-4 for instructions about adding event categories.

For more information about operational states and status colors, select Display Legend from the Help menu.

Accessing the All Events Browser Dialog Box

To access the Cascade All Events Browser, choose Cascade Events from the Event Categories window. The system then displays the All Events Browser dialog box shown in Figure 10-2.

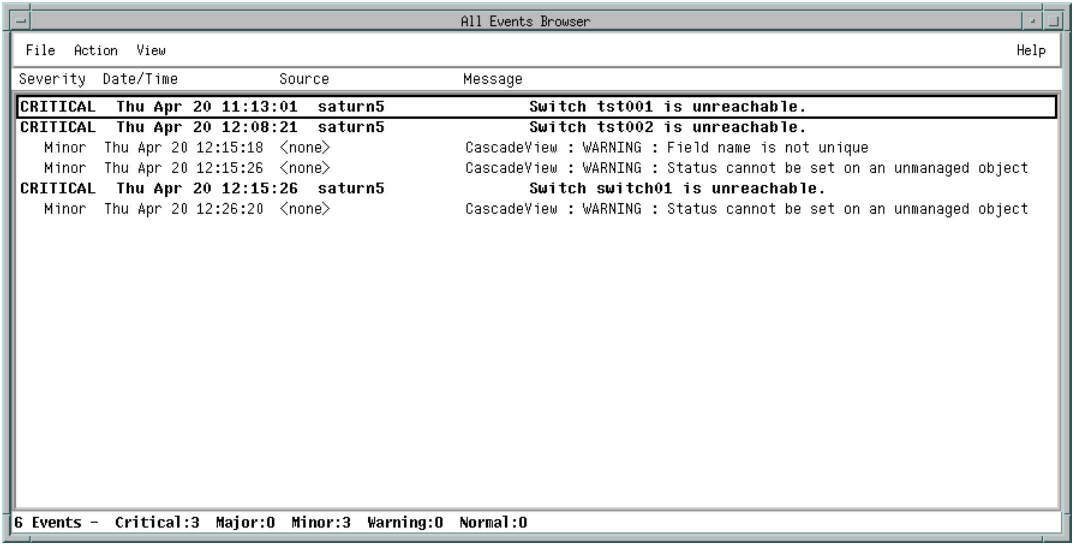


Figure 10-2. All Events Browser Dialog Box

The All Events Browser dialog box lists the following information about each trap alarm condition:

Severity — Displays the trap alarm condition's level of severity. Possible values are: Critical, Major, Minor, Warning, or Normal.

Date/Time — Displays the date and time that the trap alarm condition occurred.

Source — Displays the name of the system where the trap alarm condition occurred.

Message — Displays a message that describes the trap alarm condition.

See "Trap Alarm Conditions Reported in the Events Browser" on page 10-5 for a list and description of each of the trap alarm conditions that are reported in the Events Browser dialog box.

Viewing a Switch from the Events Browser

Use the following steps to view the switch that generated an event:

1. Select the event from the list.
2. From the Action menu, choose Highlight Source on Map. The network map appears and the switch that generated the event appears highlighted.
3. Use the standard menu commands to troubleshoot the problem.

For more information about the Event Browser, refer to the *HP OpenView Network Node Manager User's Guide* or choose Help.

Deleting an Event from the Events Browser

Use the following steps to delete an event:

1. Select the event from the list.
2. From the Action menu choose Delete ⇒ Selected Event.
3. To delete all the listed events, from the Action menu choose Delete ⇒ All Events.

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 to the **/usr/OV/log/trapd.log.old** files.

Adding Event Categories

Use the following steps to add one or more categories to the Event Categories window. For example, you may want to add a category for acknowledged events or canceled events. You can then move events into the categories as necessary.

1. From the Options menu choose Event Configuration: SNMP. The system then displays the Event Configuration dialog box.
2. Choose the Configure Categories... option button.
3. Specify the category name and choose the Add option button. The system then adds the new Event Category to the list.

Moving Events From One Category to Another

Use the following steps to move an event from one category to another.

1. From the Monitor menu choose the Events: SNMP option. The system then displays the All Events Browser dialog box.

2. Select the event(s) that you want to move.

3. From the Action menu choose the Assign Category... option. The system then displays the Assign Category: All Events dialog box.

4. Select the Category that identifies the location where you want to move the event.

5. Choose OK.

Trap Alarm Conditions Reported in the Events Browser

The following pages describe each of the trap alarm conditions that the system reports in the Events Browser. Some events are simply informational, while other events indicate a problem or potential problem within the network configuration.

The following list indicates each traps alarm condition message along with a description of the trap and, where possible, a resolution for the condition. Words that are in italics specify variable values. For example, *switch name* indicates that the message would specify the name of the switch.

A mismatched card has been detected at *switch name, slot number* (actual: *card type*, config: *port type*)

The card type on the specified slot is inconsistent with the configuration for this switch. The following table lists the possible *card type* values.

Table 10-1. Card Type Values

Message Text	Card Description
v35-6	6-port V.35 I/O
ft1-1-24	1-port, 24 channel fractional T1
fe1-1-30	1-port 30-channel fractional E1
uio-6	6-port Universal Input/Output (UIO)
cp1	Control Processor
uio-8	8-port, V.35 I/O
ft1-4-24	4-port, 24-channel fractional T1
fe1-4-30	4-port, 30-channel fractional E1
ft3-1	1-port, fractional T3 I/O
fe3-1	1-port fractional E3 I/O
hssi-1	HSSI I/O
dsx1-10	10-port DSX-1
rs232-18	18-port, X.21/V.24 I/O module (STDX 6000 only)
rs232-8	8-port, X.21/V.24 I/O card (STDX 6000 only)
ut1-4-24	4-port, 24-channel, Unchannelized T1
ue1-4-30	4-port, 30-channel, Unchannelized E1
atm-1	1-port, ATM DS3 UNI I/O
pri-4	4-port, ISDN PRI

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.

An authentication has failed on Login user console authentication login user due to console authentication login fail reason

This trap 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:

1. Lack of B-channel pool resources.
2. 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.

1. A user sent a configuration request without an IP address option.
2. The assigned logical port IP address doesn't match the one in the configuration option.
3. Their IP address conflicts with the one in the address pool that is already assigned.
4. 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 at Slot *physical slot number* Port *physical port number* in switch *switch name OID*

This trap indicates that a threshold crossing was detected on the performance parameter identified by the specified threshold table OID.

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 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.

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 CascadeView/UX.

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 CascadeView/UX.

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 Act 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+.

Circuit *circuit name* at switch *switch name* is *opstatus* with *reason*, (FailNode: *node*, FailPort: *port*)

The user-to-user PVC state has changed for the specified circuit. It has either been created or invalidated, or has toggled between the active and inactive states. The *port* and *node* values further specify the cause of the failure. Possible values for the *opstatus* variable are: invalid (0), inactive (1), or active (2).

Table 10-2 on page 10-11 lists each of the possible values for the *reason* variable.

Table 10-2. Reason Variable Values

Reason Variable	Condition
admindown	Admin status of the PVC is down
novcbuff	No virtual circuit buffer
nobw	No bandwidth
noroute	No circuit route
timeout	A timeout has occurred
nopdubuff	No PDU buffer
nodest	No destination
trknr	Trunk route not received
trkdown	Trunk down
balancereroute	Balance reroute
dead	Circuit is dead
defpathreroute	Define a new path
nidown	Network interface is down; PVC is not transmitting
otherpvcsegdown	Other PVC segment is down
otherpvcsegrnr	Other PVC segment route not received
usingaltpathwarning	Using an alternate path

Circuit *circuit name* at switch *switch name* has been rerouted

The specified 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 a Frame Relay SVC is setup or cleared. The value of cktStatus indicates whether the circuit is initiating a setup or a clear.

Circuit *circuit name* at switch *switch name* is *PVC op status, fail reason,node, pport*

The user-to-user ATM PVC state has been changed for the specified virtual circuit. It has either been created or invalidated, or has toggled between the active and inactive states. The *node* and *pport* variables indicate the node and pport that caused the PVC failure. The *op status* variable can be one of the following values:

invalid (0), inactive (1), active (2).

The *fail reason* variable can be one of the following values:

admindown (1)
novcbuff (2)
nobw (3)
noroute (4)
timeout (5)
nopdubuff (6)
nodest (7)
trkrnr (8)
trkdown (9)
balancereroute (10)
dead (11)
defpathreroute (12)
nidown (13)
otherpvcsegdown (14)
otherpvcsegrnr (15)
usingaltpathwarning(16)

Circuit *circuit name* at switch *switch name* has been re-routed

Indicates that an ATM PVC has been re-routed.

Circuit *circuit name.current op status of PVC* at switch *switch name* has changed state to *port on the fail node which caused the PVC failure* (FailReason:*PVC fail reason value*, FailNode:*node number*, FailPort:*port number*)

This trap indicates that the point-to-multipoint ATM PVC state has been changed.The possible values for the *current op status of PVC* are the following: invalid (0), inactive (1), active (2). The possible values for the PVC fail reason include the values in the following table.

Value	PVC Fail Reason
1	admindown
2	novcbuff
3	nobw
4	noroute
5	timeout
6	nopdubuff
7	nodest
8	trkrnr
9	trkdown
10	balancereroute
11	dead
12	defpathreroute
13	nidown
14	otherpvcsegdown
15	otherpvcsegrnr
16	usingaltpathwarning

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.

DS1 at Channel *chan ID*, PPort *pport number,* Slot *slot number,* Switch *switch name* has changed loopback state to *DS1 loopback status*

Indicates when the DS1 changes its current loopback state. The ***DS1 loopback status*** value can be any of the following values: 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.

Fan *fan name* at switch *switch name* is *status*

The specified fan has changed states. The *status* of the fan can be one of the following: *Up, Down,* or *Marginal*.

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.

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 has 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 SDESC

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 preventing them from being deliverable to a higher layer protocol. When this number exceeds the specified per minute threshold a link error trap is sent.

Lport lportname in switch *switch name* is down, following PVCs is also down: *circuit name list*

The specified logical port is down; as a result, the specified circuits are also down.

Lport *lportname* in switch *switch name* is up, following PVCs is also up: *circuit name list*

The specified logical port is now active; as a result, the specified circuits are now active.

Lport *port name* in switch *switch name* has congest rate *rate %* (exceed threshold *threshold %)*

The specified logical port has a congestion rate that exceeds the 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.

Lport *port name* in switch *switch name* has exceeded the threshold for SMDS DXI2 Invalid Mgmt Link ID violations

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* has exceeded the threshold for SMDS SIP3 Dest GA not found violations

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* has exceeded the threshold for Dest GA Screen Fail violations

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* has exceeded the threshold for SMDS SIP3 Dest IA Not Found violations

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* has exceeded the threshold for SMDS SIP3 Dest IA Screen Fail violations

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* has exceeded the threshold for SMDS SIP3 SA Not Found violations

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* has exceeded the threshold for SMDS SIP3 SA validation violations

The number of source address validation failures exceeds the specified SMDS PDU threshold for the logical port.

Lport *port name* in switch *switch name* has exceeded the threshold for SMDS SIP3 Source IA Screen Fail violations

The number of source individual address screen failures exceeds the specified SMDS PDU threshold for the logical port.

No format in cvtrapd.conf for cascade view spec

No other CascadeView trap is configured. To configure a trap, access the HP OpenView Network Node Manager and then select Option ⇒ Event Configuration:SNMP.

On switch *switch name* 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. The following table indicates the available card types.

Value	Card Type
1	spa
2	toc3-4
3	tstm1-4
4	tds3-8
5	te3-8
6	toc3-smfir-n-4
7	toc3-smfir-r-4
8	toc3-mm-r-4
9	toc3-smflr-n-4
10	toc3-smflr-r-4
11	tstm1-smfir-n-4
12	tstm1-smfir-r-4

Value	Card Type
13	tstm1-mm-r-4
14	tstm1-smflr-n-4
15	tstm1-smflr-r-4
16	tds3-r-8
17	te3-r-8
18	hssi-n
19	hssi-r
21	toc12-smf-n-1
22	tads1-t1-n-8
23	tads1-t1-r-8
24	tads1-e1-75-n-8
25	tads1-e1-75-r-8
26	tads1-e1-120-n-8
27	tads1-e1-120-r-8
28	tads1-j2-75-n-8
29	tads1-j2-75-r-8
30	tads1-j2-120-n-8
31	tads1-j2-120-r-8
32	spa-universal
39	toc3-stm1copper-n-4
40	toc3-stm1copper-r-4
41	nplus1-chassis

Power supply A at switch *switch name* is *status*

Power supply A has changed states. The *status* of power supply A can be one of the following: *Up*, *Down*, or *Marginal*.

Power supply B at switch switch name is status

Power supply B has changed states. The *status* of power supply B can be one of the following: *Up, Down*, or *Marginal*.

PPort *switch name slot number port number* is *state* with *alarm type*

The specified physical port has changed states. Possible *state* values for the physical port are: *Up*, *Down,* or *Testing*. Possible *alarm type* values are the following T1 standard alarms:

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 three millisecond period.
- Two or more errors within five or less 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 1's 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 4, "Loopbacks" for more information about loopbacks.

PPort at *switch name slot number, port number* has mismatched interface type (actual: *interface*, configured: *interface*)

The actual physical interface is different than the configured physical interface. Possible values for the *interface* variable are: eia449 (1), x21 (2), eia530 (3), eia530A (4), v35 (5), or none (8).

Port *Pport number* on slot *slot number, switch* switch name have just gone *loopback status*

The loopback status of a D3 or E3 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 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.

Line — Line loopback. A near-end loopback that operates upon receipt of specific framed pulse patterns. The line loopback pulse codes and functions are either Activate or Deactivate.

Port *Pport number* on slot *slot number, switch* switch name have just gone *loopback status*

The DS1 of the specified physical port number has changed its loopback status 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 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.

Line — Line loopback. A near-end loopback that operates upon receipt of specific framed pulse patterns. The line loopback pulse codes and functions are either Activate or Deactivate.

PRAM file *filename* download to switch *switch name* has complete SDESC

A PRAM download of the specified PRAM image file is complete.

PRAM file *filename* download to switch *switch name* has failed.

A PRAM download of the specified PRAM image file has failed.

Slot *slot number* in switch *switch name* has just come up

An intelligent card in the specified *slot number* has changed from a non-active to an active state.

Slot *slot number* in switch *switch name* has just gone down

An intelligent card has changed from active to non-active.

Slot *card slot number* at switch *switch name* transmit clock synchronization has changed state to *PLL synch stat*

This trap indicates the IOM transmit clock synchronization status has changed. The *PLL synch stat* variable indicates the transmit clock PLL synchronization status of the card.

Slot *card slot number* at switch *switch name* clock reference has changed state to *sys primary clk stat*

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 of the following: normal (1) or failure (2).

Slot *slot number* at switch *switch name* secondary clock reference has changed state to *sys secondary clk stat*

Indicates that the IOM system secondary clock reference status has changed to the specified system secondary clock status as detected on the card. The *sys secondary clk stat* value can be either of the following: normal (1) or failure (2).

Slot *physical slot number* at switch *switch name* Port *physical port number* DS1 ESF Data Link (FDL) status has changed state to *DS1 ESF Data Link (FDL) status*

This trap indicates that the status of the DS1 ESF Data Link (FDL)has changed.The DS1 ESF Data Link (FDL) status is the status as detected on the port and can be one of the following values: inService (1), outOfService (2).

SW file *filename* download to switch *switch name* has completed SDESC

A software download of the specified file is complete.

SW file *filename* download to switch *switch name* has failed

A software download of the specified file has failed.

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 *lportname*

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 IOP was removed
- An active PDN trunk had a status change and is now inactive
- An active Frame Relay virtual circuit had a status change and is now inactive
- An active T1 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 *lportname*

The sending protocol entity recognizes that one of the communication links represented in your network configuration has become active.

- 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 IOP which was removed is now active
- An inactive PDN trunk had a status change and is now active
- An inactive Frame Relay virtual circuit had a status change and is now active
- An inactive T1 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

The specified switch is reachable.

Switch *switch name* is unreachable

The specified switch is unreachable.

Switch *switch name* trace table full

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

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

A checksum error or battery problem occurred in the PRAM.

Switch *switch name* fatal internal error encountered and system needs to be rebooted

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

An I/O error occurred in DRAM or in SRAM.

Switch *switch name* non fatal error report: Slot=*slot number*, Src=*source*, Time=*time*, Major= *major errcode*, Minor=*minor errcode*, String=*ascii string*

A component in the switch discovered a non-fatal error condition in the specified slot. Possible values for the *source* variable are:

(1) – power-on diagnostics
(2) – background-diagnostics
(3) – fault
(4) – frame-heap

The *time* variable indicates the time that the last non-fatal error was reported. The *major errcode* variable indicates the major error code of the last non-fatal error. The *minor errcode* 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.

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 just changed to *prim clk synch ref*

Specifies that the Primary Synchronization Reference operational state has changed to the specified primary clock synchronization reference. Possible values for the *prim clk synch ref* 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 *prim clk synch ref*

Specifies that the Primary Synchronization Reference operational state has changed to the specified primary clock synchronization reference. Possible values for *prim clk synch ref* 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 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

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 stand-by card in slot *slot number* at switch *switch name* has become the active card

The card in the specified *slot number* has shot its active partner and is now the active partner of the pair.

The status of the ATM signaling function has changed to *status* on LPort *lport name* at switch *switch name*

Notification that the status of the ATM signaling function has changed on the port. *Status* indicates the operational status of the signaling function on the specified logical port.

The time-of-day clock on switch *switch name* is invalid or has not been configured.

This trap provides notification that the time-of-day clock on the switch is invalid or has not been configured.This trap is generated only at CP or SP boot-time.

Trunk *trunkname* in switch *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), nattempt (1), ninit (2), n2way (3), nexstart (4), nexchange (5), nloading (6), or nfull (7).

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* from *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).

11

Resolving Problems

This chapter describes general troubleshooting procedures for diagnosing NMS installation problems. This chapter addresses software problems related to the NMS installation as well as common operating problems. If you suspect hardware problems, refer to one of the applicable hardware manuals:

- *STDX 6000 Hardware Installation Guide*.
- *B-STDX 8000/9000 Hardware Installation Guide*.

Basic Troubleshooting

In diagnosing and troubleshooting software, proceed from the simple to the complex, following a systematic procedure. As a point of reference, keep in mind the directory structures listed in Table 11-1.

Table 11-1. 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	CascadeView/UX scripts
/opt/CascadeView/conf	trap daemon configurations
/opt/CascadeView/etc	CascadeView/UX configurations
/opt/CascadeView/sqr	network report binaries
/usr/OV/bin	OpenView binaries
/opt/cde	Common Desktop Environment (CDE) files
/opt/scripts	Installation scripts

SPARCstation Problems

If you are having problems on your SPARCstation, complete the following steps to isolate the cause of the problem:

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 following

☑ *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.

Problems With Solaris and Motif

I'm having trouble installing Solaris 2.5.

Verify that you have identified your hardware correctly and partitioned your disks properly.

1. To re-start the Solaris 2.5 installation, press Stop-A to interrupt the machine.
2. Verify that the Solaris 2.5 installation CD is installed in the CD-ROM drive.
3. Type **boot cdrom**
4. Refer to the *Network Management Station Installation Guide* for installation instructions.

After upgrading Solaris, I cannot pram sync. tftpserver 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 CascadeView/UX installation process, you added a line to the **inittab** file so that the system would invoke the Cascade 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 Cascade tftp daemon.

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, refer to 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 was changed since 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 target to which it pointed before the upgrade.

The Quit command does not appear on the Motif menu.

You did not copy the **system.mwmrc** file from the **/opt/SUNWmotif/lib** directory to the home directory as **.mwmrc**. For more information refer to the *Network Management Station Installation Guide*.

HP OpenView Problems

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.

SYBASE Problems

I can't start SYBASE!

To start SYBASE, you must be in the $SYBASE directory and logged in as the sybase user.

1. Type **cd $SYBASE**
2. Type **whoami** to verify that you are logged in as the sybase user.
3. Type **ls -l** to list the files in long format.
4. Verify that the correct read and execute permissions are set.
5. Type **cd install**
6. Type **ls -al RUN_CASCADE**
7. Verify that the file has the correct group and ownership and sybase and dba appear in the third and fourth columns.
8. Verify that the line begins with -r-xr--r--.

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. Type showserver.

How do I start the SYBASE server?

1. Log in as the sybase user.
2. Change to the following directory:

   /sybase/install
3. Type **startserver -f RUN_CASCADE**.

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 typing the following command:

```
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 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. Type the following commands:

```
1> shutdown
2> go
```

I get error 1997 in the same window I started Open Windows.

1. The SYBASE server cannot be accessed by CascadeView/UX.
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. Type **showserver**.

CascadeView/UX NMS Problems

How do I start CascadeView/UX?

1. Verify that you are logged in as the nms user by typing the following command:

   `whoami`

2. Verify that you are in the **/opt/nms** directory by typing the following command:

   `pwd`

3. Execute CascadeView by typing:

   `/usr/OV/bin/ovw &`

What is my password?

Cascade does not know your root or nms user password. Cascade 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. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information.

When I start CascadeView, I get the error “Cannot connect to database”.

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, type the following command:

   `/usr/OV/bin/ovstatus`

3. If all OV daemons are not running, restart the OV daemons by typing:

   `/usr/OV/bin/ovstart ovwdb`

4. To start all daemons, type the following command:

   `/usr/OV/bin/ovstart`

5. To confirm that all daemons are running, type:

   `/usr/OV/bin/ovstatus`

How do I copy Cascade 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, type:

   `/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.

6. Continue this procedure for each additional file that you want to copy. This process takes a few minutes to complete.

7. When the copy is complete, the icon appears.

8. Select the **eject disk** button located in the floppy File Manager box.

9. To download the switch software from the NMS to the switch, refer to the *Network Configuration Guide for B-STDX/STDX*.

How do I know if CascadeView/UX is running?

The CascadeView/UX icon appears at the bottom of the screen. Never close this box, unless one of the supporting programs (such as HP OpenView) stops processing.

General Questions and Problems

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 their respective 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. Type 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.

3. *Network Configuration Guide for B-STDX/STDX*.

What kind of hardware do I need?

Refer to the Hardware Requirements section of the *Network Management Station Installation Guide*.

What versions of software do I need?

Refer to the Software Requirements section of 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.

My mouse does not seem to be working.

The SPARCstation uses an optical mouse. Make sure you have the shiny mousepad.

Use the following steps to add the line to inittab:

1. Type the following command:

   ```
   vi /etc/inittab
   ```

2. While holding down the Shift key, type **$G** to go to the end of the file.

3. While holding down the Shift key, type **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 Cascade 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. Type **:wq!**

7. At the # prompt, type the following command:

   ```
   init Q
   ```

This command forces the system to read the inittab file. The system then starts the Cascade 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. Cascade does not support Sun Microsystem's tftp daemon on the STDX 3000/6000 switches.*

Common Operating Problems

General Questions and Problems

What is the Event Monitor and what does it do for me?

In the CascadeView/UX Network Management System (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 "Accessing the All Events Browser Dialog Box" on page 10-3 of this guide for more information.

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 CascadeView/UX 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?

Type **./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. Execute the following command to delete the current configuration and add a new configuration.

   /opt/sybase/sybtli

I keep getting the error / or /var is full.

1. The wtmp and wtmpx files may be too large. Use the following command 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, execute the following command:

   ps -ef|grep tftp

   Null results indicate that tftpserv is not running. Contact the Cascade Technical Response 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. Execute 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. Use 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, use the following command 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.

Switch Problems

My switch will not turn green.

1. Make sure you can ping the switch.
2. Make sure that the text file has been downloaded correctly.
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 type **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 that 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. You should also 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.

CascadeView/UX NMS Problems

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, it's possible for the switch to interchange the IP addresses but not the community names, resulting in unreachable nodes. Refer to the *Network Configuration Guide for B-STDX/STDX* to recheck those configurations.

I just want to start over, what do I do?

1. Delete each object from the HP OpenView map. (Use Delete to do this--do not use Cut).

2. Delete the map from HP OpenView.

3. Close the HP OpenView using the File ⇒ Exit.

4. Login as the root user as follows:

   su - root

   The system then prompts you for the root password. Enter the appropriate password.

5. Enter the following command to shut down HP OpenView services:

   /usr/OV/bin/ovstop

> *Step 6 completely removes the database. There is no database recovery process after you execute this command.*

6. Use the following command to completely remove the database.

   rm -rf/usr/OV/databases/openview/*/*

7. Use the following commands to remove the events and traps alarm logs that are associated with the database.

   rm /usr/OV/log/xnmevents.*username*

   rm /usr/OV/log/trapd.log

   rm /usr/OV/log/trapd.log.old

8. Use the following command to run the HP OpenView database daemon, register the fields in the database, and start all other OpenView daemons.

   /usr/OV/bin/ovstart ovwdb

   /usr/OV/bin/ovw -fields

   /usr/OV/bin/ovstart

9. Login as the sybase user as follows:

   su - sybase

10. Login as the root user as follows:

    su - root

11. Use the following command to stop the CascadeView trap log.

    /usr/OV/bin/ovstop cvtraplogd

12. Type the following command at the # prompt:

    /opt/CascadeView/bin/cv-install.sh

13. At the prompt for the name of your database server, press Return to accept the default name **CASCADE**.

14. At the prompt for the name of your SYBASE Administrator, type sa and press Return.

15. At the password prompt, type **superbase** and press Return. The script will configure OpenView to know about CascadeView/UX and will start the trap log daemon.

16. Type **yes** when prompted "Do you want to remove the database?"

17. Type N to answer that you are not running SYBASE Version 10.0.

18. Type Y to answer that you are running SYBASE Version 4.9.2.

    The system then recreates the cascview database. You now have a clean SYBASE and HP OpenView database.

I am locked out of a node that noone else is using.

This problem occurs if you improperly exit from HP OpenView or if HP OpenView windows is hung and for this reason the user kills the process. Use the following steps to correct this problem.

1. Change directories to **/opt/CascadeView/bin** and execute the **cv-release-locks.sh** shell script. This lists the nodes that are currently locked, and who has them locked.

   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, type **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 into the main screen.

2. Do not run more than three event logs at the same time.

3. Check the Cascade Event Browser dialog box and see how often events come in (See "Accessing the All Events Browser Dialog Box" on page 10-3.)

4. Check the CPU utilization with **/usr/openwin/bin/perfmeter**. Do not leave this running, however, since it takes over CPU resources.

5. Make sure the IP network icon is unmanaged (and has been from the start) and it is currently hidden. The IP network icon should be disabled.

I am experiencing OPTimum Trunk Problems

If you modify the DLCI or an OPTimum trunk, the trunk will fail to come up with a new DLCI. You must delete the previous OPTimum trunk and its associated logical ports, and re-add the logical ports with the desired DLCI and OPTimum trunk entries.

I cannot delete a switch configuration from the database

You cannot delete a switch from the database until all of its associated configurations (trunks, circuits, etc.) are deleted. Refer to "Deleting a Switch Configuration Database" on page 11-37 for instructions.

How do I change a logical port name?

You cannot use the CascadeView/UX NMS to make this change. Use the following steps to make this change:

1. Change directories to **/opt/CascadeView/bin**

2. Execute the **renamelp.sh** shell script.

   In addition, if your installation has access to the CascadeView/UX Toolbox product, you can use a utility called **cvtool_rename_lport** to rename logical ports.

Changing my lower K factor on trunk utilization reduces trunk bandwidth?

K factors for trunks are inverted for the CascadeView/UX Network Management System (NMS). Therefore, if you set the oversubscription factor to 400% you will have four times as much bandwidth. If the K factor is set to 25%, you will have one fourth as much bandwidth. This is the inverse of the DOS mechanism.

After importing a file from DOS, some objects do not display in 3-D.

The HP OpenView database contained objects that have the same name as the objects in the imported file. If the problem occurs with multiple objects, use Delete to delete the objects from the CascadeView/UX map and then import the file again.

If the problem occurs with only one object, select the switch, and use the Edit ⇒ Delete ⇒ From All Submaps menu option to delete the object. After you delete the object, add it to the map using the **same** name.

What do I do if I get an error that the log device is full?

The following two procedures describe how to do this. 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

Use the following procedure to purge the log daily when you do not want to backup the database. This procedure safely purges the transaction log.

1. Log into isql.
2. Issue the following commands.

```
1> dump transaction cascview with truncate_only

2> go
```

Procedure 2

> *The following steps leave the database in an inconsistent state. For this reason you must back up the database immediately after completing this procedure.*

1. Log into ISQL and issue the following command.

```
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 6-2 provides basic troubleshooting solutions for resolving problems when you test the connectivity of the CascadeView/UX NMS software applications and the Frame Relay network.

Table 11-2. Connectivity Troubleshooting Solutions

Problem	Possible Causes	Solutions
Changes that you entered to the netstat -r configuration have not taken affect.	Wrong order of addition to table not in script.	Use the **netstat -r** command to check routing. Make sure the entry comes 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.
Your modem does not dial when you use the SLIPDIAL option.	Your hardware may be connected improperly, or an incorrect serial port may be specified in the configuration files.	Verify that the correct cables are connected to the modem, phone jacks, and the Serial Mgmt Port. Make sure the serial port is configured properly.
When using SLIPDIAL, you cannot establish a connection. The modem dials and you get an answer, but no connection is established.	The setting on the remote modem may be incorrect.	Verify that the communicating systems are using the same baud rate and settings for data bits, parity type, stop bits and flow control. If your modem supports echo mode, you may further investigate connection problems by putting your modem into echo mode. The modem will then send back all commands it receives. On a Hayes compatible modem, you can turn on echo mode using the at e1 command and turn it off using the at e0 command.

Table 11-2. Connectivity Troubleshooting Solutions

Problem	Possible Causes	Solutions
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 CascadeView/UX 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.
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.

Table 11-2. Connectivity Troubleshooting Solutions

Problem	Possible Causes	Solutions
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 the following devices: 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 IP Address is different from the IP address assigned to your SPARC 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 CascadeView/UX 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.

Switching to a Redundant B-STDX 8000/9000 Standby Card

To manually pass operation from an active I/O module to a redundant standby card, complete the following steps:

1. On the network map, select the switch where the redundant card is configured.
2. From the Administer menu, choose Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears, displaying a graphical representation of the back plane of the selected switch.
3. Select the desired slot configuration and choose the Switch to Redundant Card ... command button located at the bottom of the dialog box.

Using the Upload PRAM Command

Occasionally a situation occurs where the switch configuration file for a specific I/O module and the configuration stored in the NMS database do not match. This can happen when you upgrade your switch software or use a network management product other than CascadeView/UX to manage the switch.

> ! *If you remove an I/O Module from one switch and install this module in a second switch, you get a PRAM conflict. This happens because the module contains an unknown configuration. Do not use PRAM upload to clear this condition. Instead, use the erase PRAM function described in the Network Configuration Guide for B-STDX/STDX to clear PRAM on this module and then reconfigure the module.*

To resolve PRAM conflicts, use the Upload PRAM command to view the switch configuration file stored in PRAM. This enables you to compare the configuration file stored in the switch (PRAM) to the configuration file stored in NMS database.

- If you need to replace the configuration file stored in the NMS database, use Upload PRAM to replace it with the switch configuration file stored in switch PRAM.
- If you need to replace the configuration file stored in switch PRAM, use the synchronize PRAM command to replace this file with the one stored in the NMS database. Refer to the Network Configuration Guide for B-STDX/STDX for details.

The following software is required to use the Upload PRAM command:

- CascadeView/UX 1.5.x or above
- Switch Release 4.0.3.yy or 4.1.x or above, where yy is greater than 50 for B-STDX 8000/9000 models.
- Switch Release 2.4 for STDX 3000/6000 models.

Upload PRAM Objects Supported

Upload PRAM currently supports the following objects:

- Physical ports
- Logical ports (except Trunk ports)
- SMDS Individual Addresses
- SMDS Group Addresses
- SMDS Alien Addresses
- SMDS Address Screens

Guidelines for Using Upload PRAM

Before you use the Upload PRAM command, review the following points:

- You can use upload PRAM to add objects from switch PRAM to the NMS database, as long as the objects being added to the database do not conflict with existing objects in the database. An example of this would be, the NMS database already contains a switch with that name.
- If you need to add SMDS Group Addresses and Group Address members, upload PRAM information from the CP before you upload PRAM from an I/O module.
  - The CP upload creates the Group Address in the CP.
  - The I/O module upload adds the members into the Group Address.
- If you need to add SMDS Address Screens and Address Screen members, upload PRAM information from the CP before you upload PRAM from an I/O module.
  - The CP upload creates the Address Screen in the CP.
  - The I/O module upload adds the members into the Address Screen.
- Due to the interdependency of objects with other objects in the database, *be careful* when you use upload PRAM to delete objects from the database. In general, do not create a situation where there are dangling objects (i.e., an object without a parent) in the switch before applying the upload PRAM. For example, deleting a logical port without first deleting all associated individual addresses or address screens will create dangling objects and will cause a problem during the upload PRAM process. Refer to Figure 6-1 to determine the relationships that exist between CascadeView/UX objects in the database.

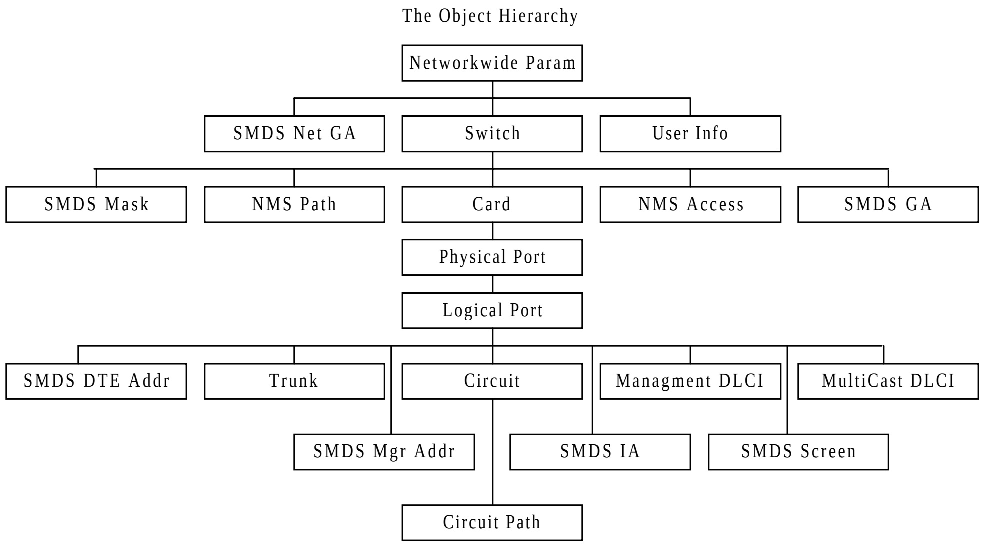


Figure 11-1. CascadeView/UX Object Hierarchy

To upload the switch configuration file stored in PRAM:

1. On the network map, select the switch object.

2. From the Administer menu, choose Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears, displaying a graphical representation of the back plane of the selected switch.

3. Select either the I/O module or the control processor module and choose the PRAM command. The CascadeView PRAM Sync dialog box appears.

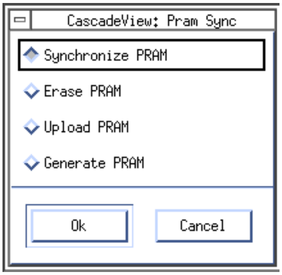


Figure 11-2. PRAM Sync Dialog Box

4. Select Upload PRAM and choose OK. The Card PRAM Upload and NMS Synchronization dialog box appears.

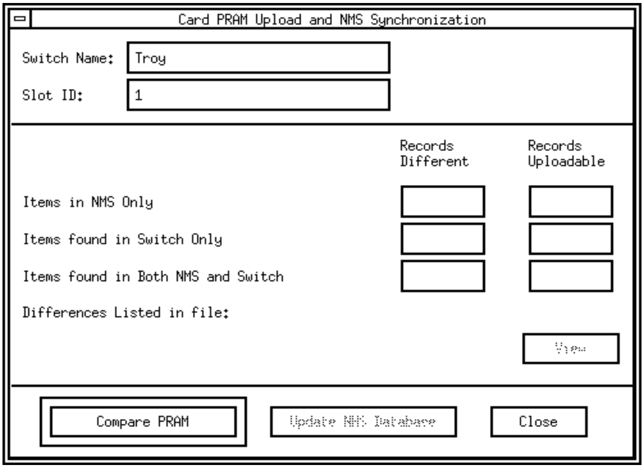


Figure 11-3. Card PRAM Upload and NMS Synchronization Dialog Box

5. Choose Compare PRAM.

6. The dialog box displays information about the number of inconsistencies between the PRAM configuration file and the NMS database. If the field displays a zero, there are no differences between the PRAM and NMS configurations.

   Review the following list for a description of the fields on this dialog box. For this example, keep in mind that *item* could be a single physical or logical port definition.

   Items in the NMS only — The item exists in the NMS database, but not in the switch PRAM. This could happen if you made configuration changes to an unmanaged switch.

   Items found in Switch only — The item exists in switch PRAM, but not in the NMS database. This could happen if you configured a switch using a third-party network management station.

   Items found in both NMS and Switch — This item exists in both places, but there are discrepancies in the configuration. This would happen if you modified the configuration directly from the console. For example, if you used console commands to change the admin status of a logical port, the logical port definition in switch PRAM indicates that the logical port is down; the NMS database records the logical port as up. These discrepancies can also occur if a PRAM synchronization or set fails.

7. The name and location of the file that stores the inconsistencies appears on the dialog box. Choose View to display the inconsistencies file.

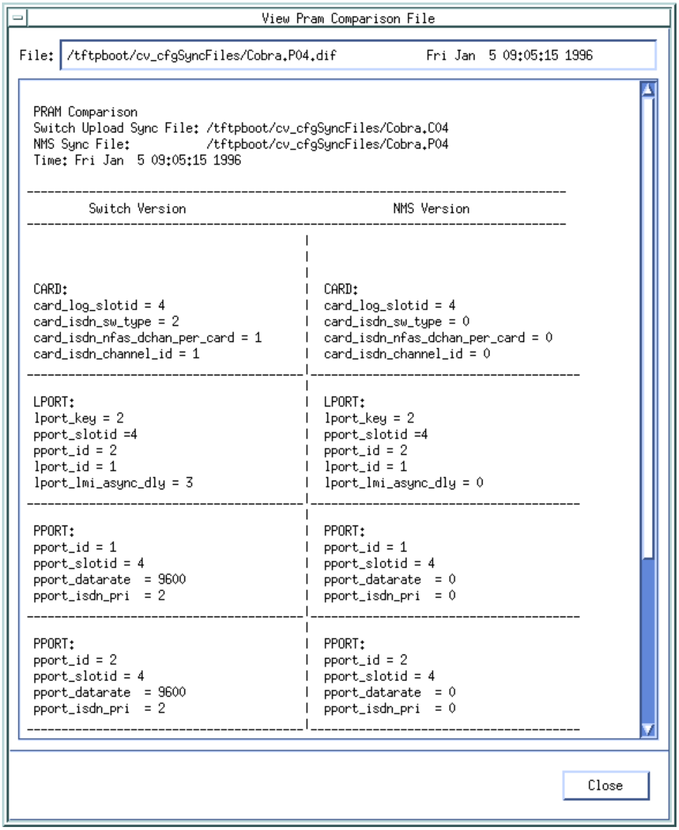


Figure 11-4. Sample PRAM Inconsistencies File

Choose Close to return to the Card PRAM Upload and NMS Synchronization dialog box.

8. To synchronize the information between switch PRAM and the NMS database, you have two options:

   - Choose the *Update NMS Database* command to use the configuration stored in switch PRAM.

   - If you need to use the configuration stored in the NMS database, choose Close. Use the Synchronize PRAM command to update PRAM (refer to the *Network Configuration Guide for B-STDX/STDX* for details).

9. Repeat Steps 3 through 8 for each I/O module to complete the configuration upload.

If an error occurs during the upload process, a message dialog appears. After closing this dialog box, you can choose Update NMS Database to continue the upload process for the remaining items.

If there are problems with the PRAM configuration file, refer to the description for chmod 666 /dev/cua/a <Return> in the Network Configuration Guide for B-STDX/STDX *for instructions to download the configuration file stored in the NMS database.*

Deleting a Switch Configuration Database

To delete a switch configuration from the database, you must first delete the entire configuration associated with the switch to be deleted, for example, logical ports, trunks, circuits, etc.

The following steps outline the proper order in which to delete a switch configuration from the database:

1. Delete all permanent virtual circuits defined for the switch to be deleted.
2. Delete all trunk connections to the switch to be deleted.
3. Delete all logical ports on the switch.
4. Delete all physical ports on the switch.
5. Delete all I/O module configurations on the switch.
6. Delete the switch icon from the map.

Technical Support Checklist

Before placing a call to the Cascade Technical Response Center (TRC), review the following checklist to make sure you have gathered all the information you need:

☑ If you are experiencing NMS SPARCstation problems, check the system and make note of the following information:

- Model type
- Amount of available memory
- Operating system and version number
- Network interface card (NIC) type
- NMS IP Address
- Subnet Mask used

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 examine later.

☑ If you cannot make a connection from the NMS to the switch, check and note the following:

- Connection method used, e.g., Ethernet, Indirect Ethernet, SLIP, Management DLCI, 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 NMSs (if any) , and Ethernet IP address (if any) configured on the switch.
- If using the Indirect Ethernet or Management DLCI connection method, note the IP addresses of the associated routers.

Please have access to your NMS SPARCstation when calling the Cascade Technical Response Center (TRC).

☑ If you are having trouble configuring a permanent virtual circuit (PVC), check and note the following:

- Physical and logical port configurations; LMI type, CIR, Be, Bc, clock speeds.

☑ If you are trying to diagnose physical port-level problems, check and note the following:

- Physical attributes configured on the ports
- Cables, pinouts, and DSU/CSU equipment and its configurations
- Admin status

☑ If you are trying to diagnose logical port-level problems, check and note the following:

- LMI port configuration
- Poll timers and verification timers configured for the port
- DSU/CSU equipment and configurations, etc.
- Admin status

Contacting Cascade

Cascade provides a full range of support services to ensure that the maximum network uptime is achieved with low equipment cost. The staff at the Cascade Technical Response Center are also available to assist with any problems encountered while using the NMS software. You can contact the Cascade Technical Response Center by phone, email, or fax.

Calling by Phone

Cascade offers Customer Support 24 hours a day, 7 days a week. To contact the Cascade Technical Response Center by phone, use one of the following numbers:

In the United States and Canada
1-800-DIAL-WAN (1-800-342-5296)

Outside the U.S., Canada, and the United Kingdom
1-978-952-7299

In the United Kingdom
0-800-96-2229

Sending Electronic Messages or Faxes

To contact the Technical Response Center by email, address your requests to

cs@casc.com

To contact the Technical Response Center by fax, 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 identifiable symptoms
- Any information that you gathered as a result of reviewing the "Technical Support Checklist" on page 11-38.

12

Reinstalling the Operating System

If you need to reinstall the Operating System software due to accidental loss or damage, please consult with a Cascade Customer Service representative immediately. Unless you are upgrading your switch software, Cascade does not generally recommend that you install the Operating System software, since it is loaded at the factory before shipment.

This chapter provides step-by-step instructions to download the Operating System software for the STDX 3000/6000 and the B-STDX 8000/9000. **Be sure to check the current Release Notes for updated information.**

About Cascade Firmware

The Cascade switch firmware uses a flash-based Operating System (OS) software loaded at the factory. You can erase and restore the flash in one of two ways:

- While the switch is communicating with an NMS and running an existing OS.
- While the switch is in an unknown or non-running state, and not communicating with an NMS.

The first method is the most desirable and easiest. Once the switch is operational and communicating with the NMS, you can download the software from the NMS over the network.

The sections that follow detail how to erase the existing flash and load a new version of the OS software.

Downloading Firmware to the STDX 3000/6000

There are two methods for downloading the firmware to the B-STDX 8000/9000. The first method is the normal method of operation and is strongly recommended. The second method should only be used as a backup.

Method 1 — Enables you to download the firmware from CascadeView/UX while the switch is up and communicating with the NMS, as described in the "Downloading from the NMS" section. This method is the normal and recommended method for downloading the firmware.

Method 2 — Enables you to download the firmware when the switch is not communicating with the NMS, as described in the section "Downloading from the Console." You should only use this method as a backup and only after consulting with a Cascade Technical Response Center representative.

Downloading from the NMS

Before you can download the switch firmware from the NMS to an STDX 3000 or 6000 switch, you need to install the NMS software and firmware as described in the *Network Management Station Installation Guide*. Make sure that the firmware file STDX.ROM is located in the directory:

/opt/CascadeView.var/SwitchSoftware

To download the firmware from the NMS, complete the following steps:

1. Start CascadeView/UX, and then open the network map. Select the switch to which you are installing the firmware. From the Misc menu, choose CascadeView _ Logon and enter your logon password.

2. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software. Select the file STDX.ROM from the listbox. Select **Yes** to answer the question “Reboot after Download?”

   After the TFTP file transfer completes, and the new software has been burned into FLASH storage area, the switch cold boots and adopts the new software. The switch now contains the new firmware.

Downloading from the Console

To download the firmware from the console, complete the following steps:

1. Install a connection from the SPARCstation to the Serial Network Management port on the back of the switch.

2. Execute a terminal emulation package.

3. Force a Line Break condition to the switch. One of the following prompts appears:

   \> Indicates that both OS software and a PRAM configuration is resident in the switch.

   \>> Indicates that OS software is resident in the switch but that no PRAM configuration is resident.

   => Indicates that the manual mode jumper is on both posts of the W1 jumper on the Packet Processor or that there is no OS in FLASH.

> *If the switch does not respond to a CTRL-BREAK command sequence, check to make sure that you installed a DTE - DTE crossover cable. (Refer to your hardware manual for cable diagrams.) Then, refer to the section "Bringing the Switch Up With the Manual Mode Jumper On" for further instructions.*

4. At either the > or >> prompt type the following:

   `login debug`

   `password: [your debug password]`

   If you do not know your debug password, contact the Technical Response Center.

5. At the ## prompt type the following:

   `nindy`

   The system is now entering the low level debugger. This process takes about one minute to complete. Once initiated, the => prompt appears.

6. At the => prompt, type the following command to erase PRAM:

   ep

   When the PRAM is erased, a >> prompt appears.

7. At the >> prompt, type the following command to delete the flash (or system operating code):

   df

   The df command responds by erasing flash and programming zeroes.

8. Once the df command stops at the Receiving File, start an Xmodem file transfer to send the operating (binary) code to the switch. The file is located in the following location:

/opt/CascadeView.var/SwitchSoftware

   The flash download takes about five minutes to complete.

9. When the file transfer completes, power the switch Off and then On to load the new OS software. The switch performs power up diagnostics and returns a >> prompt.

10. From the console terminal, force a Line Break condition. A banner appears, displaying the switch name and software release number. Verify the release number.

> *If the switch does not respond to a Line Break condition, bring up the switch with the Manual mode jumper installed. Refer to the instructions provided in the "Bringing the Switch Up With the Manual Mode Jumper On" section that follows.*

You must now download the initialization script file for the switch to become operational. The *Network Configuration Guide for B-STDX/STDX* describes this procedure.

Bringing Up the Switch With the Manual Mode Jumper

If the STDX 3000/6000 does not respond to a Line Break condition, complete the following steps to bring up the switch with the Manual mode jumper on.

> *Be sure to use the appropriate static guard measures and power off the switch.*

1. Power off the switch.
2. Loosen the two screws on the Packet Processor (PP) module and remove the card. Place the jumper for W1 across both posts. Jumper ***W1*** is located approximately midway on the right side of the board (front facing the user).
3. Return the PP module to the switch and power on the unit.
4. At the => prompt, type the following command to erase PRAM:

   `ep`

   When the PRAM is erased, the >> prompt appears.
5. At the => prompt, type the following to delete the flash (or system operating code):

   `df`

   The df command responds with erasing flash, programming zeroes.
6. Once the df command stops at the Receiving File, start an Xmodem file transfer to send the operating system code to the switch. The file is located in the following location:

/opt/CascadeView.var/SwitchSoftware

   The flash download takes about 5 minutes to complete.

7. Once loaded, power the switch off, return the jumper to one post, and then power the switch on.
8. You must now download the initialization script file for the switch to become operational. (The *Network Configuration Guide for B-STDX/STDX* describes this procedure.)

Clearing the STDX 3000/6000 Parameter RAM

The STDX 3000/6000 uses 64 KB of battery backed-up RAM for parameter configuration storage. The NMS SPARCstation generates an initialization script file containing the SNMP SET commands that control the switch's configuration. The SPARCstation that contains the initialization script file loads the initial parameter configuration into the switch.

After the switch is running with the configuration and is communicating with the NMS SPARCstation, you can make any additional configuration changes dynamically on-line. You only need to download the initialization script file if the switch does not contain a parameter configuration file or if you want to replace the existing configuration file. (The *Network Configuration Guide for B-STDX/STDX* describes how to produce the initialization script file.)

To remove an existing configuration from the STDX 3000/6000, complete the following steps:

1. Install a console terminal to the Serial Management Port on the Packet Processor.
2. Force a Line Break condition to the switch to get the > prompt.
3. At the > prompt, type the following:

   `login debug`

   `password: [your debug password]`

   If you do not know your debug password, contact the Technical Response Center.
4. At the ## prompt, type the following:

   `reset pram`

   `Are you sure (YES/NO)? YES` (YES must be typed in uppercase letters)
5. At the ## prompt, type the following:

   `reset system`

   `Are you sure (YES/NO)? YES`

   `(YES must be typed in uppercase letters.)`

The system then displays the following message:

```
resetting switch, stand by...
```

Once the switch comes up (1-2 minutes), a >> prompt appears. This prompt indicates that you successfully erased PRAM and the switch is ready for a new initialization script file download.

Downloading Firmware to the B-STDX 8000/9000

There are two methods for downloading the firmware to the B-STDX 8000/9000. The first method is the normal method of operation and is strongly recommended. The second method should only be used as a backup.

Method 1 — Enables you to download the firmware from CascadeView/UX while the switch is up and communicating with the NMS as described in the "Downloading from the NMS" section. This method is the normal and recommended method for downloading the firmware.

Method 2 — Enables you to download the firmware when the switch is not communicating with the NMS as described in the section "Downloading from the Console". You should only use this method as a backup and only after consulting with a Cascade Customer Support representative.

Cascade distributes the B-STDX 8000/9000 firmware in a set of files. Each file corresponds to a particular type of B-STDX 8000/9000 card or card family. Table 12-1 illustrates three firmware file description examples.

Table 12-1. Firmware File Description Examples

File	Description
CP.ROM	Supports the Control Processor card.
IOPTYPEA.ROM	Supports the UIO, T1/E1/DSX1 cards.
IOPTYPEB.ROM	Supports the HSSI, ATM, ATM DS3, and channelized DS3 IOP cards.

Downloading from the NMS

Before you can download the B-STDX firmware from the NMS to an STDX 8000/9000 switch, you need to:

- Install the NMS software and firmware as described in the Network Management Station Installation Guide.
- Make sure that the /opt/CascadeView.var/SwitchSoftware directory contains the firmware files listed in Table 12-1 on page 12-9.
- Verify that the TFTP daemon is running. If it is not, see the Network Management Station Installation Guide for instructions on how to configure the TFTP daemon to start automatically.

The procedure for downloading the firmware varies depending on whether you are downloading to a single CP or a redundant CP. The following sections describe each of these procedures.

Downloading to a Switch with a Single CP

To download the firmware from the NMS to a B-STDX 8000/9000 switch with a single CP module, complete the following steps:

1. Start CascadeView/UX, and then open the network map. Select the switch to which you are installing firmware. From the Misc menu, choose CascadeView ⇒ Logon and enter your logon password.
2. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software. Select the file **CP.ROM** from the listbox. Choose **No** to answer the question “Reboot after Download?”
3. After the TFTP file transfer completes, the switch is temporarily unreachable and its map icon changes to red. This condition should last only a few moments while the CP burns the new software image into its FLASH storage area.
4. When the switch becomes reachable again, select the switch on the network map to which you are installing firmware. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software.
5. Select the file **IOPTYPEA.ROM** from the listbox. Choose **No** to answer the question “Reboot after Download?”

6. After the TFTP file transfer completes, the switch is temporarily unreachable and its map icon changes to red. This condition should last only a few moments while the CP burns the new software image into its FLASH storage area.
7. Select the switch on the network map to which you are installing firmware. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software.
8. Select the file **IOPTYPEB.ROM** from the listbox. Choose **Yes** to answer the question “Reboot after Download?”
9. After the TFTP file transfer completes and the new image is burned into FLASH, the switch completely reboots and all the cards adopt the new software.

> *The switch takes longer than usual to reboot because each IOP may be burning in a new version of the boot flash before loading and adopting the new software. This process is a one-time only burn-in.*

10. Optionally upload the PRAM for each card. See “Using the Upload PRAM Command” on page 11-29 for more information.
11. PRAM Synch each card. When the switch becomes reachable from the NMS, each card is in a marginal state. The Background Diagnostics status screen displays a PRAM Obsolete error code. You must PRAM Synch each card to complete the installation process. Do not attempt to modify the switch configuration in any way until you synchronize all the cards. (Refer to the *Network Configuration Guide for B-STDX/STDX* for more information.)
12. Use the Clear Background option on the Foreground Diagnostics dialog box to clear each cards marginal state in the Background Diagnostics log. See “Foreground Diagnostics” on page 3-24 for more information.

Downloading to a Switch with a Redundant CP

These instructions assume that the CP in slot one is the active CP, and that the CP in slot two is the standby CP.

To download the firmware from the NMS to a B-STDX 8000/9000 switch with a redundant CP module, complete the following steps:

1. Start CascadeView/UX, and then open the network map. Select the switch to which you are installing firmware. From the Misc menu, choose CascadeView ⇒ Logon and enter your logon password.
2. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software.
3. Select the file **CP.ROM** from the list box. Choose **No** to answer the question “Reboot after Download?”
4. After the TFTP file transfer completes, the switch is temporarily unreachable and its map icon changes to red. This condition should last only a few moments while the CP in slot 1 burns the new software image into its FLASH storage area.
5. When the switch becomes reachable again, select the switch on the network map. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software.
6. Select the file **IOPTYPEA.ROM** from the list box. Choose **No** to answer the question “Reboot after Download?”
7. After the TFTP file transfer completes, the switch is temporarily unreachable and its map icon changes to red. This condition should last only a few moments while the CP in slot 1 burns the new software image into its FLASH storage area.
8. Select the switch to which you are installing firmware. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software.
9. Select the file **IOPTYPEB.ROM** from the list box. Choose **No** to answer the question “Reboot after Download?”
10. After the TFTP file transfer completes, the switch is temporarily unreachable and its map icon changes to red. This condition should last only a few moments while the CP in slot 1 burns the new software image into its FLASH storage area.

11. From the CascadeView Switch Back Panel screen, select the Switch to Redundant Unit option to switch to the standby CP.

12. Return to the CascadeView map and verify that the switch to which you are installing firmware is highlighted. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software.

13. Select the file **CP.ROM** from the list box. Choose **No** to answer the question “Reboot after Download?”

14. After the TFTP file transfer completes, the switch is temporarily unreachable and its map icon changes to red. This condition should last only a few moments while the CP in slot 1 burns the new software image into its FLASH storage area.

15. When the switch becomes reachable again, select the switch on the network map. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software.

16. Select the file **IOPTYPEA.ROM** from the list box. Choose **No** to answer the question “Reboot after Download?”

17. After the TFTP file transfer completes, the switch is temporarily unreachable and its map icon changes to red. This condition should last only a few moments while the CP in slot 1 burns the new software image into its FLASH storage area.

18. Again select the switch to which you are installing firmware. From the Administer menu, choose Cascade Switches ⇒ Download Switch Software.

19. Select the file **IOPTYPEB.ROM** from the list box. Choose **Yes** to answer the question “Reboot after Download?”

    After the TFTP file transfer completes and the new software burns into FLASH, the entire switch reboots and adopts the new software.

The switch takes longer than usual to reboot because each IOP may be burning in a new version of the boot flash before loading and adopting the new software. this process is a one-time only burn-in.

20. Optionally upload the PRAM for each card. See “Using the Upload PRAM Command” on page 11-29 for more information.

21. PRAM Synch each card. When the switch becomes reachable from the NMS, each card is in a marginal state. The Background Diagnostics status screen displays a PRAM Obsolete error code. You must PRAM Synch each card to complete the installation process. Do not attempt to modify the switch configuration in any way until you synchronize all the cards. (Refer to the *Network Configuration Guide for B-STDX/STDX* for more information.)

22. Use the Clear Background option on the Foreground Diagnostics dialog box to clear each cards marginal state in the Background Diagnostics log. See "Displaying Foreground Diagnostics" on page 3-26 for more information.

Downloading from the Console

To download the firmware from the console, complete the following steps:

1. Install a connection from the NMS SPARCstation to the B-STDX 8000/9000 Network Management Port. (Refer to the *B-STDX 8000/9000 Hardware Installation Guide* for details.)

2. Place both of the two-position dip switches (located on the front of the Control Processor card) to point left in the Off position.

> *If you have a redundant CP installed in the switch, remove it from the switch before continuing.*

3. Reset the CP card by sliding the ejector lock down and back up again.

4. Execute a terminal emulation package (such as TERM). Set the line parameters as follows: 19,200 baud, 8 bits, no parity.

5. On the terminal emulator, press Enter. The following prompt appears to indicate that you are in cell mode:

```
%
```

6. At the % prompt, type the following:

```
kermit
```

   The switch is now awaiting receipt of the firmware file.

7. Using the terminal emulation package, send the firmware files (CP.ROM, IOPTYPEA.ROM, and IOPTYPEB.ROM) to the switch via the kermit send protocol.
8. During the file transfer, the CP's Marginal LED should remain solid. When the file transfer completes, the Marginal LED shuts off.
9. Repeat Step 5 through Step 8 until all file transfers complete.
10. Place both of the CP's two-position dip switches to the On position, pointing to the right, away from the position numbers.
11. Reset the CP card by sliding the ejector lock down and back up again.
12. If you removed a redundant CP card from the switch, reinstall the card and then reactivate the card. To see if the redundant card is present:
    - Verify the Redundancy LED is blinking; or
    - Use the **show card state** command from the console to check if the slot is active
13. Use the following command to erase the PRAM and the flash memory from the redundant (standby) card. Note that there is **a space AFTER the last 2 and before the final number 1 in the command.**

    ```
    ## set card.2.1.72.1.2 1
    ```

    After the system erases the flash memory from the card, the active CP automatically downloads the current flash memory to the standby card.

Clearing the B-STDX 8000/9000 PRAM

The B-STDX 8000/9000 uses 64 KB of battery backed-up PRAM for configuration storage. The NMS generates an initialization script file that contains the SNMP SET commands for controlling the switch's configuration. The SPARCstation that contains this initialization script file loads the initial PRAM configuration into the switch.

Once you power on the switch with the new configuration, and it is actively communicating with the NMS, you can make additional configuration changes on-line. You only need to download the initialization script file if the switch does not contain a parameter configuration file, or if you want to replace the existing configuration file. (The *Network Configuration Guide for B-STDX/STDX* explains the procedure to generate and download an initialization script file.)

The following three methods are available for clearing the existing PRAM configuration from the B-STDX 8000/9000.

Method 1 — Uses the NMS software to clear PRAM. This first method is considered the normal operation and is strongly recommended.

Method 2 — Requires you to connect a console terminal and clear the PRAM on each card according to the slot number. You should only use this second method as a backup.

Method 3 — Is a backup method that you should only use as a last resort and only after consulting with a Cascade Customer Support representative.

Method 1

> *Use caution when relying solely on the NMS. If you reset PRAM on a card that contains the only trunk providing a path to the NMS, you will lose connectivity from the NMS to the switch.*

1. On the network map, select the switch for which you want to clear PRAM.
2. From the Administer Menu, choose Cascade Parameters ⇒ Set Parameters.
3. Select each IOP card (one at a time) and choose the Synch PRAM command button.
4. Choose Erase PRAM.
5. Repeat Step 3 and Step 4 until you have erased the PRAM for each card.

Method 2

1. Install a console terminal to the Network Management Port on the CPA. (Refer to the section "Connecting a Console" in the Cascade *B-STDX 8000/9000 Hardware Installation Guide* for details.)

2. Force a Line Break condition to the switch. Enter a minimum of three characters for login name and enter a valid community name as the password. ("cascade" is the default community name.)

3. At the > prompt, type the following:

   enable debug

   password: [your debug password] (or cascade)

   If you do not know your debug password, contact the Technical Response Center.

4. Choose one of the following actions depending on whether you are removing PRAM on individual cards.

   a. If you are removing PRAM on all cards in the switch, including the CP, at the ## prompt type the following:

      reset pram all

   b. If you are removing PRAM on individual cards in the switch, at the ## prompt type the following:

      reset pram [#] (where [#] is the card or slot number)

      Are you sure (YES/NO)? YES

5. At the ## prompt, type the following:

   reset system (this step reboots all cards)

   Are you sure (YES/NO)? YES

Once the switch comes up (1-2 minutes), a >> prompt appears. This prompt indicates that the PRAM is erased and the switch is waiting for a new initialization script file download.

Method 3

You should only use the following method as a last resort, and only as instructed by a Cascade Technical Response Center representative.

1. Power off the switch.
2. Install a connection from the NMS SPARCstation to the B-STDX 8000/9000 Network Management Port. (Refer to the *Cascade B-STDX 8000/9000 Hardware Installation Guide* for details.)
3. Place both of the two-position dip switches (located on the front of the Control Processor card) to the Off position (left).
4. Power on the switch.
5. Execute a terminal emulation package (such as TERM). Set the line parameters as follows: 19,200 baud, 8 bits, no parity.
6. On the terminal emulator, press Enter. The following prompt appears to indicate that you are in cell mode:

   ```
   %
   ```

7. At the % prompt, type the following:

   `erase_pram`

8. Power off the switch.
9. Place both of the CP's two-position dip switches to the On position, pointing to the right, away from the position numbers on the switch.
10. Power on the switch.

Once the switch comes up (1-2 minutes), a >> prompt appears. This prompt indicates that the PRAM is erased on the CP card only and that the switch is waiting for a new text file download.

A

Console Commands

This appendix provides a listing of the console commands that you can enter to perform various tasks on the switch, or to obtain information from the switch. The first section describes console commands for the B-STDX 8000/9000. The next section describes commands for the STDX 3000 and 6000.

> *The console remembers the last ten commands that you enter. ^B can be used to recall previous commands as needed.*

B-STDX Console Commands

This table provides a summary of all B-STDX Console Commands.

Table A-1. B-STDX Console Commands

Command	Description
Press BREAK to log in to console	The first command you see
STDX (nodename) login: yourname password:	The login procedure
Cascade B-STDX Configuration Console Name: nodename Location: Model: 651-09000-00 Serial# 0040FB010166 SW Rev: 03.01.01.02 >	The Console Header
enable	go in master mode
get <oid string>	SNMP get
help	Displays help message
next <oid string>	SNMP next
ping <ip address>	ICMP ping (page A-7)
quit, exit, end, bye, logout	Exit from console
reset pvc	Sets the Admin status down and then up to quickly reset the PVC. Can only be used in debug mode (page A-8).

Command	Description
>>set debug password	Old password: New password: Verify new password: Debug password has been changed
show ?	Display parameters (page A-61)
show card <slot>	Displays the card configuration (page A-9)
show external	Displays System External (ASE) OSPF Autonomous host table (page A-15)
show hardware	The Module Identification Memory (MIM) device allows you to use this command to remotely access your card to determine card type, hardware revision, serial number, manufacturing part number, and product code. (page A-14)
show icmp	ICMP statistics (page A-15)
show imxclk	Displays the IMX clocking statistics (page A-16)
show ip	IP statistics (page A-17)
show lport attributes <interface>	Displays logical port attributes (page A-28)
show lport statistics <interface>	Displays logical port statistics (page A-31)
show ospf adv [link type] [internal ip]	Displays a specified link-state advertisement
show ospf database	Displays a link-state database, one per line (page A-18).
show ospf interface	Shows the state of all OSPF trunks (page A-19).
show ospf names	Shows the routing table for resilient names (page A-21).

Command	Description
show ospf route	Shows the IP routing table (page A-23).
show ospf statistics	Displays various OSPF statistics (page A-24)
show ospf vcpath [destination internal ip address]	Shows the path a virtual circuit will take page A-26)
show pvc statistics <interface.dlci>	Displays pvc statistics and attributes (pages A-16 to A-19)
attributes <interface.dlci>	
show pport statistics <slot.port>	Displays physical port statistics (page A-33)
show pport attributes <slot.port>	Displays physical port attributes (page A-32)
show rip route	Displays information about the routing information protocol (RIP) attributes (page A-38)
show rip statistics	Displays information about the routing information protocol (RIP) statistics (page A-39)
show smds addr	Shows the SMDS address table and addresses (page A-41)
show smds area	Shows all the NPA/NXX Area Numbers that are known to this switch. This command also displays information about the Virtual Circuit table entries (page A-40).
show smds ga_area	Shows the SMDS GA areas (page A-43)
show smds path	Shows the SMDSvirtual paths set up through OSPF (page A-45)
show smds scrn	Shows the SMDS screens and smds_lnk (page A-46)

Command	Description
show smds statistics	Shows the SMDS IA and GA statistics (page A-58)
show smds trace	Shows the SMDS tracing (page A-49)
show software (all)	Displays all cards and the software information for them (page A-61)
show software card [slot_number]	Displays software information for a specific card (page A-62)
show software flash	Displays software versions in CP(s) flash memory (page A-63)
show smds path	Shows all the circuits that have been created or are in the process of being set up by this switch. Each pair of switches has one Virtual Circuit setup for the SMDS Switching System functionality (page A-45).
show system	Shows general system information and status (page A-64)
show tcp	TCP statistics (page A-65)
show udp	UDP statistics (page A-66)
show users	Displays current users logged on the switch through console or telnet (page A-67).
> Idle log out	Appears when you have not used the console for a few minutes.

Example B-STDX Console Commands

The following pages list each of the console commands along with an example. The commands are organized alphabetically. Each command is listed on a separate page.

ping

Seeks a response from another network device.

```
>ping 192.9.200.22


Reply in < 100 ms
```

reset pvc [interface.dlci]

If you enable debug (#), you can use this command to set the PVC's Admin Status value to down and then up. This quickly resets the PVC.

```
# reset pvc [interface.dlci]
```

set debug password

Changes the debug password.

```
>> set debug password


Old password:
New password:
Verify new password
Debug password has been changed
```

show card [*slot number*]

This command displays information about the control processor or card. This information includes serial number, hardware, EPROM, software revisions, and status. This command also retrieves statistics for memory and CPU utilization.

```
> show card
```

Examples

Example 1

```
> show card
```

Slot	Type	Redund State	State	SW Rev	HW Rev	EPROM	Serial #
1	CP-BASIC	Active	Active	04.01.00.00	10.00.00	04.00.00.00	0040FB011185
2	CP-BASIC	Standby	Active	04.01.00.00	10.00.00	04.00.00.00	0040FB011265
5	UIO-8	Active	Active	04.01.00.01	05.00.00	03.03.00.00	0040FB0102D1
6	UIO-8	Standby	Active	04.01.00.01	04.00.00	03.03.00.00	0040FB010618
15	HSSI-2	Active	Active	04.01.00.01	02.00.00	04.00.00.00	0040FB010608

Example 2

The following command displays information about the CP card in slot 1.

```
>show card 1
```

Serial #	0040FB020F5E	Configured Card Type:	CP-BASIC
Hardware Revision:	10.00.00	Actual Card Type:	CP-BASIC
EPROM Revision:	04.00.00.00	Physical Slot:	1
Software Revision:	04.01.00.00	Logical Slot:	1

Redund State:	Active		
Card State:	Active	Memory Utilization:	728560
Administrative Status:	Up	CPU Utilization:	1%
Operational Status:	Up		
Diagnostic Status:	Up		

Example 3

The following command displays information about the UIO card in slot 5.

```
>show card 5
```

Serial #	0040FB020E CC	Configured Card Type:	UIO-8
Hardware Revision:	05.00.00	Actual Card Type:	UIO-8
EPROM Revision:	03.03.00.00	Physical Slot:	5
Software Revision:	04.01.00.00	Logical Slot:	5
Redund State:	Active		
Card State:	Active	Memory Utilization:	3596688
Administrative Status:	Up	CPU Utilization:	1%
Operational Status:	Up		
Diagnostic Status:	Up		
Packets Received:	0	Active PVCs:	2190
Octets Received:	0	Inactive PVCs:	2
Packets Sent:	0	Pending PVCs:	2188
Octets Sent:	0		

show external

This command displays OSPF Autonomous System Externals, such as the static routes in OSPF.

```
> show external
```

Destination	Mask	Gateway	Metric	Status	Index	DLCI
192.9.200.101	255.255.255.255	0.0.0.0	1	1	4097	0
192.9.200.173	255.255.255.255	0.0.0.0	1	1	4097	0
192.9.200.175	255.255.255.255	0.0.0.0	1	1	4097	0

show hardware

The Module Identification Memory (MIM) device allows you to use this command to remotely access your card to determine card type, hardware revision, serial number, manufacturing part number, and product code. For more information on MIM, contact the Cascade Technical Response Center.

```
> show hardware
```

show icmp

This command displays ICMP statistics.

```
> show icmp
```

```
                             Receive      Transmit
Messages:                    142          201
Errors:                      1            0
Dest Unreachables:           142          201
Time Exceeded:               0            0
Parameter Problems:          0            0
Source Quenches:             0            0
Redirects:                   0            0
Echos:                       0            0
Echo Replies:                0            0
Timestamps:                  0            0
Timestamp Replies:           0            0
Addr Masks:                  0            0
Addr Mask Replies:           0            0
```

show imxclk

This command displays IMX clocking statistics.

```
> show imxclk

Current IMX Clocking

Clock Master Slot:       0

Clock Source Slot:       0

Clock Source ID:         0

No. of Clock Masters:    0

No. of Clock Sources:    0

       Last 8 States of Clocking

State Description             Initialization

State clock master slot:      0

State clock source index:     22

State Message ID:             0

State Message Source:         0

   .

   .

   .

State Description             Initialization

State clock master slot:      0

State clock source index:     22

State Message ID:             0

State Message Source:         0
```

show ip

This command displays IP statistics.

```
> show ip
```

```
Inbound Direction
Datagrams Rcvd from Below:     0
Header Errors:                 0
Address Errors:                145
Datagrams Forwarded:           6586
Reassembly Reqds:              0
Datagrams Reassembled OK:      0
Reassembly Failures:           0
Reassembly Timeouts:           0
Unknown Protocol Errors:       0
Datagrams Discarded:           0
Datagrams Passed to Above:     2257
Outbound Direction
Datagrams from Above:          2782
Datagrams Discarded:           0
No Route Discards:             0
Datagrams Fragmented OK:       0
Fragmentation Failures:        0
Fragments Created:             0
```

show ospf database

This command displays a link-state database, one per line.

```
> show ospf database
```

Type ID	Adv-Switch	Seq#	Age
1(6) 201.201.201.1	201.201.201.1	0x8000015e	1046
1(6) 201.201.201.2	201.201.201.2	0x80000071	1046
1(6) 201.201.201.8	201.201.201.8	0x80000151	1046
5 152.148.81.66	201.201.201.1	0x80000122	963
5 152.148.81.5	201.201.201.8	0x80000124	747
5 152.148.81.5	201.201.201.2	0x80000045	1050
5 152.148.81.5	201.201.201.8	0x80000124	747
5 152.148.81.72	201.201.201.1	0x80000122	963
15(3) 0.0.0.2	201.201.201.2	0x80000045	1050
15(3) 0.0.0.2	201.201.201.1	0x8000011d	963
15(3) 0.0.0.3	201.201.201.2	0x80000045	1035
15(3) 0.0.0.3	201.201.201.1	0x80000068	899
15(3) 0.0.0.4	201.201.201.2	0x80000010	1035
15(3) 0.0.0.4	201.201.201.1	0x800000cf	228
15(3) 0.0.0.5	201.201.201.2	0x80000003	1272

LSAs: 19

Xsum: 0x8d9be

show ospf interface

This command shows the state of all OSPF trunks.

```
> show ospf interface
```

LPort	Neighbor	Nbr_ State	Vers	#Rxmt	#LS Req	DB sum	Instance
Int	0.0.0.7	Full	6	0	0	0	
Int	0.0.0.8	Full	6	0	0	0	
Int	0.0.0.11	Full	6	0	0	0	
17	201.201.201.1	Full	6	0	0	0	0x22
38	201.201.201.1	Full	6	0	0	0	0x19

show ospf namedpath [*type*] [*name*] [*len*] [*card*]

This command shows the path that a circuit would take when an SVC call is made to the *name*. *Names* can be resilient UNI/NNI names, E.164 addresses, and NSAP addresses.

```
> show ospf namedpath 3 0x39998989898 40 8
```

This example would specify that the system print the path that an SVC which originated on card 8 would take to the NSAP address (type = 3) 0x39998989898/40.

Parameters

The following list describes each of the parameters for the show ospf namedpath console command.

Type — Specify a 1, 2, or 3 to indicate the type of name. Type 1= Resilient UNI/NNI names. Type 2 = E.164 addresses. Type 3 = NSAP addresses (type=3).

Name — This parameter specifies the name. The name is specified as a hexadecimal string. In the example above the name is 0x39998989898. If you do not know the name, refer to “show ospf names” on page A-21 for information on how to obtain the name.

Len — The length of the name is specified in bits. For example, in the sample above, this parameter is 40. If you do not know the length, refer to “show ospf names” on page A-21 for information on how to obtain the length.

Card — The card where the SVC originated.

show ospf names

This command prints a line for every *name* known to the switch. *Names* can be resilient UNI/NNI names, E.164 addresses, and NSAP addresses.

```
> show ospf names
```

Type	Cost	Name/Len Primary (Secondaries)
2	0	0x0/0 2/15
3	0	0x0/0 2/15
3	0	0x39018200000000000000000000000000000000/152 1/9
3	0	0x39028200000000000000000000000000000000/152 2/14
3	0	0x392222/24 2/13
3	0	0x39333333333333333333333333333333333333/152 2/15
3	1	0x39989898/32 1/39

Attributes

The following list describes each of the attributes for the show ospf names output.

Type — Lists a 1, 2, or 3 to indicate the type of name. Type 1= Resilient UNI/NNI names. Type 2 = E.164 addresses. Type 3 = NSAP addresses (type=3).

Cost — The cost of the path to the switch currently hosting the name (i.e., the name's primary location).

Name/Len Primary — This parameter indicates the name itself along with the primary location for the name. These two parameters are separated by a slash. The name is shown as a hexadecimal string. The length is shown in bits. For example, in the first line of the output shown above, the name is 0x0 and the length is 0 bits.

Secondary — Any secondary locations for the name.

show ospf qospath [*IP address of destination node*] [*card*]

This command displays various qospath statistics.

```
> show ospf qospath
```

Forward BW (Kbytes):

Reverse BW (Kbytes):

Forward QoS (1-4):

Reverse QoS (1-4):

Metric (0-3):

Current Path ID:

S/W version (2-6):

Characteristics:

E-E Delay (milliseconds):

Private Net ID:

Void trunk (switch/IFIndex):

Dest: 0.0.0.0

Result: Destination unreachable

show ospf route

This command shows the OSPF routing table.

```
> show ospf route
```

Dest	Mask	Next_hop	State	Cost
152.148.81.2	255.255.255.255	201.201.201.1	External	3
152.148.81.5	255.255.255.255	None	Static	N/A
152.148.81.17	255.255.255.255	201.201.201.1	External	3
152.148.81.66	255.255.255.255	201.201.201.1	External	3
152.148.81.72	255.255.255.255	201.201.201.8	External	2
201.201.201.2	255.255.255.255	170.170.170.170	Internal	0
201.201.201.8	255.255.255.255	201.201.201.8	Internal	1

show ospf statistics

This command displays various OSPF statistics.

```
> show ospf statistics
```

# switches:	3	# reachable switches:	3
# Dijkstra runs:	6	# Trunks:	9(10)
Max LSA size:	252	# Stub links:	3(3)
# router-LSAs:	3	#AS-external-LSAs:	8
# name-LSAs:	8	# LSA-Xsum:	0x8d9be
# VC lookups:	0	# VC reroute attempts:	0
# successful defaults:	0	# specific VC calc.:	0
# QoS failures:	0	# VC unreachables:	0
# VC reroutes:	0		
# VC crankbacks	0	# Multipoint cranks:	0
# OSPF trunk inst ch:	0	# VCMGR trunk inst ch:	0
# Bad paths reg:	0	# VCs using old rev:	0
Routing S/W revision:	6	Network S/W revision:	6
Max task latency (ms):	25	Max lookup time (ms):	0

show ospf trunk

This command displays various OSPF trunk statistics.

```
> show ospf trunk
```

sw/ prt	sw/ prt	f_bw3	r_bw3	delay	cost	f_inst	r_inst	comments
1/14	2/38	52638	52638	14	2	0x10e	0x19	
1/11	2/17	138937	138937	14	10	0x117	0x22	
2/37	8/41	20506	20506	16310	1	0x54	0x138	
2/35	8/23	29481	29481	16358	1	0x5	0x137	

show ospf vcpath

This command displays various OSPF trunk statistics.

```
> show ospf vcpath
```

Dest: 0.0.0.0

Result: Destination unreachable

show pport [*slot number*]

This command provides information about all physical ports. This includes the pport number, the type of card, the number of logical ports, the clock speed, and admin status. If you specify a slot number (see example), this command provides information about the card in the selected slot only.

```
>> show pport 4
```

pport	type	# of lports	datarate	status
1	UIO	1	8192000	Up
2	UIO	0	1536000	Down
3	UIO	0	64000	Down
4	UIO	0	64000	Down
5	UIO	0	64000	Down
6	UIO	0	64000	Down
7	UIO	0	64000	Down
8	UIO	1	2048000	Up

show lport attributes [*interface number*]

This command displays information about the logical port you specify. Use the interface number (*ifnum*) to specify the logical port.

The following command displays the output you would receive for a trunk logical port.

```
> show lport attributes 1
```

Slot:	12		
Port:	1		
Interface:	1		
Data Rate:	2048000		
Trunk Status:	Full	Trunk Overhead:	5
Remote Node:	150.150.50.1	Trunk Utilization:	100
Remote Interface:	2	Available Bandwidth:	19426 0
Maximum Transmission Unit:	512		
Administrative Status:	Up		
Operational Status:	Up		

The following command displays the output you would receive for a logical port.

```
> show lport attributes 6
```

Slot:	12
Port:	5
Interface:	6
Data Rate:	2048000
Maximum Transmission Unit:	8192

Administrative Status	Up
Operational Status:	Up

The following command displays the output you would receive for a channelized port.

```
> show lport attributes 12
```

```
Slot:                          15

Port:                          2

Interface:                     12

Data Rate:                     1536000

Member DS0s:                   8,9,10,11,12,13,14,15,16,17,18,19,20,21,
                               22,23,24,25,26,27,28,29,30,31

Bit Stuffing:                  No

Maximum Transmission Unit:     8192

Administrative Status:         Up

Operational Status:            Up
```

show lport statistics [*ifnum*]

This command displays logical port statistics, including the number of frames transmitted and received. It also provides information about errors, if applicable.

```
> show lport statistics 1
```

	Receive	Transmit
Frames:	890	825
Octets:	92064	59852
Discards:	0	0
Errors:	0	0

show pport attributes [*pport id*]

This command displays information about the physical port you specify. The physical port id is made up of the slot number and physical port number.

```
> show pport attributes 3.1
```

```
Slot:                    3
Port:                    1
Configured Port Type:    UIO    Actual Port Type:         UIO
Configured Interface:    V.35   Actual Interface Type:    V.35
Administrative Status:   Up     Data Rate:                64000
Operational Status:      Down   Clock Source:             DCE
Link Down Reason:        NONE
```

show pport statistics [*pport id*]

This command displays physical port statistics including the number of frames transmitted and received. It also provides information about errors, if applicable.

```
> show pport statistics 8.8
```

	Receive	Transmit
Octets:	302687	992145
Frames:	3680	3689
Discards:	0	0
Errors:	0	0

show pvc statistics [*interface.dlci*]

This command displays statistics for the specified circuit. Use the interface index (ifnum) and dlci to specify the circuit.

```
> show pvc statistics 6.241
```

```
                   Receive       Transmit

Octets:            20018376      0

Frames:            119155        119158

DE Frames:         0             0

ODE Frames:        0             118742

DE Octets:         0             0

ODE Octets:        0             0

FECN:              118739        118817

BECN:              118814        20018880

Discards:          0             -

Lost Frames:       -             0

DE Frames Lost:    -             0

ODE Frames Lost:   -             0

Lost Octets:       -             0

DE Octets Lost:    -             0

ODE Octets Lost:   -             0
```

Receive and Transmit Counters

These statistics are the receive and transmit counters for the following items:

Octets — The number of bytes.

Frames — The number of frames.

DE Frames — The number of Discard Eligible frames.

ODE Frames — The number of Over Discard Eligible frames.

DE Octets — The number of Discard Eligible bytes.

ODE Octets — The number of Over Discard Eligible bytes.

FECN — The number of Forward Explicit Congestion Notification frames.

BECN — The number of Backward Explicit Congestion Notification frames.

Discards — The number of frames discarded (receive only).

Lost Frames — The number of frames lost (transmit only).

DE Frames Lost — The number of lost Discard Eligible frames.

ODE Frames Lost — The number of Over Discard Eligible frames lost.

Lost Octets — The number of lost bytes.

DE Octets Lost — The number of lost Discard Eligible bytes.

ODE Octets Lost — The number of lost Over Discard Eligible bytes.

show pvc attributes [*interface.dlci*]

This command displays information about the specified circuit. Use the interface index (ifnum) and dlci to specify the circuit.

```
> show pvc attributes 6.241

Src Interface:          6
Src DLCI:               241
Priority:               1
Commited Info Rate:     5000
Commited Burst Size:    5000
Excess Burst Size:      0
Dst node ID:            2
Dst Interface:          8
Dst DLCI:               241
Type of Service:        1
Discard enable:         0 (Off)
Admin Status:           2 (Active)
Creation time:          0
Last change:            0
PVC state:              6 (Active)
DCE state:              2
DTE state:              2
DTE status:             2
Receive ready:          0
Interface state:        0
Data flow:              1
Operation status:       2 (Active)
```

Attributes

Src Interface — The source interface index (same as II or ifnum).

Src DLCI — The source DLCI index (same as DD).

Priority — The PVC's configured priority.

Commited Info Rate — The Committed Information Rate (CIR) for this PVC.

Commited Burst Size — The Committed Burst (Bc) Size for this PVC.

Excess Burst Size — The Excess Burst (Be) Size for this PVC.

Dst Node ID — The PVC destination node identifier.

Dst Interface — The PVC's destination interface index (ifnum).

Dst DLCI — The PVC's destination DLCI.

Type of Service — The PVC service type.

Discard Enabled — Discard enabled is 1(On) or 2(Off).

Admin Status — Admin status is 2(On) or 1(Off).

Creation Time — The amount of time since the switch booted up prior to the PVC creation (zero if the PVC was initialized out of PRAM).

Last Change — The amount of time since the switch booted up prior to the last change to the PVC (zero if the PVC is unchanges since the last boot).

PVC State — The internal PVC state.

DCE State — The end-to-end state.

DTE State — The endpoint state.

DTE Status — The endpoint status.

Receive Ready — The PVC is capable of receiving frames (In Flow).

Interface State — The state of the interface of the PVC.

Data flow — The PVC is capable of forwarding frames.

Operational Status — The external PVC state.

show rip route

This command displays information about the routing information protocol route.

```
> show rip route
```

```
Dest        Mask    Next_hop    Cost Age
```

show rip statistics

This command displays information about the routing information protocol statistics.

```
> show rip statistics

RIP is enabled on 1 interfaces

Send Host Routes is enabled.

# Pkts Received:            4413   # Pkts Transmitted:    850
# RxRequests:               25     # TxRequests:          1
# RxResponses:              4388   # TxFullUpdates        849
# RxTraceONs:               0      # TxPartUpdates:       0

# RxTraceOFFs:              0
# RxOthers:                 0
# RxBadVers:                0
# RxBadResps:               3
# RxBadNets:                9497

# FlashSched:               0
```

show smds area

This command displays SMDS path information for the current switch using SMDS NPA-NXX Numbers.

```
>show smds area
```

```
SMDS NPA-NXX Numbers discovered through OSPF

Node IP Address: 152.148.56.2


NPA-NXX     Destination_Node    VP_Index    VP_Slot

00020401    152.148.56.2        0000        0

00021001    152.148.56.2        0000        0

00021002    152.148.56.2        0000        0

00011401    152.148.56.1        0002        4

00011402    152.148.56.1        0002        4

00040401    152.148.56.4        0004        11

00040402    152.148.56.4        0004        11

00030800    152.148.56.3        0002        11
```

This command provides an alternate view of SMDS path information. NPA-NXX Numbers show the area numbers that are defined on remote nodes. For example, 00011401 is defined on switch 152.148.56.1.

- The *VP_Index* column shows the Virtual Circuit setup for each of these switches. There is a virtual circuit entry in both the CP and the IOP.
- The *VP_Slot* shows the outgoing IOP slot (i.e. the trunk card) that is used for this virtual circuit.

> *If the VP_Index and VP_Slot fields equal zero (0), then the NPA-NXX numbers are defined locally on this switch.*

show smds addr

This command displays the SMDS slot option address along with any specified parameters from the following list.

```
>show smds area slot address parameter
```

Where:

slot — is value from 3 through 16 that indicates the slot number.

address — is the specified address structure.

parameter — is one of the parameters from the following list.

Parameters

The following list describes each of the parameters for the show smds addr console command.

ia — displays the individual address.

ga — displays the group address.

aa — displays the alien address.

dia — displays the distributed individual address.

opt — displays the optimum address.

fdr — displays the feeder address.

Examples

```
show smds addr 8
```

Displays all addresses in the hash table on slot 8.

```
show smds addr 4 ia
```

Displays all individual addresses defined in slot 4.

```
show smds addr 3 ga
```

Displays all group addresses defined in slot 3.

```
show smds addr 11 dia
```

show smds ga_area

This command displays the SMDS group address area.

```
>show smds ga_area slot "nodeid"
```

Where:

slot — is the specified slot number.

address — is the specified address structure.

> *To determine interface information for a destination node, use the show smds path command. See* *page A-45* *for details.*

Examples

Example 1

The following example displays all group address areas for the specified slot.

```
>show smds ga_area 3
```

```
## -----  SMDS Ga Area Table (at 0x90341940)  -----
    -----  All Ga Areas    -----
        00000000-00800999
```

Example 2

The following example displays the group address area for the specified node IDs. Node IDs must be entered in quotation marks.

```
>sh smds ga_area 3 "00000000" "00800999"
```

----- SMDS Ga Area Table (at 0x90341940) -----

----- smdsi_ga_area object -----(at 0x9063AB60)

next_p = 0x00000000

GaArea = 0x0000000000800999

GaNodeCount = 1

pNextNode = 0x9063A6D0

----- DestNodeIds for this Area -----

258

show smds path

This command displays the SMDS path information with respect to the current switch (152.148.56.2).

```
>show smds path
```

SMDS Virtual Paths setup through OSPF

Node IP Address: 170.170.170.1

Destination_Node	VCid	VP_Index (CP, IOP)	VP_Slot	Lport	Hop Count	Interface Path
170.170.170.2	000B	0026, 000B	4	0166	0001	358

- The *Destination Node* column shows all switches which are accessable from the current switch.
- The *VC_ID* column shows the Virtual Circuit Identifier in the IOP card from which the virtual circuit is initiated.
- The *VP_Index* column shows the Virtual Circuit setup for each of these switches. There is a virtual circuit entry in both the CP and the IOP.
- The *VP_Slot* shows the outgoing IOP slot (i.e. the trunk card) that is used for this virtual circuit.
- The *Lport* shows the logical port ID of the trunk port from which the virtual circuit is set up.
- The *Hop Count* indicates the number of hops from this node to each of the destinations.
- The *Interface Path* shows the intermediate logical port IDs the virtual circuit setup.

show smds scrn

This command displays the SMDS screen map and information about the SMDS link structure.

```
>show smds scrn slot [if] [ia or ga]
```

Where:

if — Specifies an interface number for a specified slot.

slot — The specified slot number.

ia — A specified individual address.

ga — A specified group address.

Examples

Example 1

The following example displays all SMDS DXI interface numbers for slot 3.

```
show smds scrn 3
```

System2## ----- SMDS lnk & addr screen Response -----

----- Logical port table at 0x902BE7C0 -----

```
-----   smds dxi_sni if_nums   -----
```

3 4 5

Example 2

The following example displays the SMDS link structure for interface number 5 in slot 3.

```
show smds scrn 3 5
```

System2## ----SMDS lnk & addr screen Response----

Link switch structure at 0x902BE7D4

--smds_lnk object (at 0x9045D670--

ssi_lnk_p = 0x00000000 next_smds_lnk_p = 0x00000000

ssi_node =	0	ssi_log_slot =	0	ssi_slot =	0
ssi_if_num =	0	ssi_vp_index =	0	ssi_vp_slot =	0
scrn_id =	1	pr_flags =	0	flags =	0

Example 3

The following example displays the SMDS individual address screen map structure for interface number 5 in slot 3. Note that each address has an associated address ID assigned by the CascadeView NMS.

```
show smds scrn 3 5 ia
```

System2## ----SMDS lnk & addr screen Response----

Link switch structure at 0x902BE7D4

---- IA & AIA ids in screen map (at 0x9045D68A) -----

```
2
```

show smds trace

This command provides SMDS frame trace information. The command enables you to verify whether or not specified frames are entering the switch. If the frames are entering the switch, the system saves the header.

After reception or transmission of an SMDS frame, the system checks the trace flag. If you have set the flag to *off*, no trace logic is used and the frame continues with the processing. If it is set to *on*, the tracing routine is called.

By default, the trace logic saves all frame headers.If any of the options (da, sa, or if) are turned on, logic for that function is invoked and if the frame header meets the criteria set in the trace variables, the header is saved.

There are three different usages for this console command.

Usage 1 — Resetting the Trace Filters

The first usage enables you to turn tracing on or off or to reset the trace filters. The format for this use of the command follows:

```
>show smds trace slot [on|off|reset]
```

Where:

slot — is the specified slot number.

on — Indicates that tracing is on. All frame headers are saved and the system displays a response to indicate that tracing is on.

off — Indicates that tracing is off. Trace filters are cleared when tracing is set to off.

reset — Clears the contents of the trace area to zeroes.

Usage 2 — Selectively Narrowing Traffic Tracing

Use the following command after you turn tracing on. This usage of the SMDS trace command enables you to compare the destination or source address of a frame that the trace logic has saved and compares the frame to a specified parameter.The format for this use of the command follows:

```
>show smds trace slot [da|sa|if] (param)
```

Where:

slot — The specified slot number.

da — Sets the SMDS trace 16-digit destination address value for a specified slot.

sa — Sets the SMDS trace 16-digit source address value for a specified slot.

if — Specifies an interface number for a specified slot. This parameter cannot be used if you are performing cell bus tracing.

param — The value of the destination address, source address, or interface number. If tracing is turned *on*, the trace utility compares the parameter value to the frame's *da*, *sa*, or *if* (depending on what the command specifies). If the value of *da*, *sa*, or *if* matches the specified parameter, the frame header is saved. A destination address or source address must be entered in quotation marks. Interface numbers are entered without using quotation marks. For example, to specify a trace on a destination address, you would enter the following command:

```
sh smds trace 3 da "C15089522600FFFF"
```

To specify a trace on an interface number , you would enter the following command:

```
sh smds trace 3 if 12
```

> *If you have two or more levels of tracing turned on, you must turn the tracing off (using the trace off command) so that you can perform the trace at a broader level.*

Usage 3 — Showing Saved Output

```
>show smds trace slot dump [1|2]
```

slot — The specified slot number.

dump 1 — Displays what the trace logic has saved for incoming frames on a specified slot.

dump 2 — Displays what the trace logic has saved for outgoing frames on a specified slot.

Usage 4 — Cell Bus Tracing

This usage enables you to turn cell bus tracing on. The format for this use of the command follows:

```
>show smds trace slot [da|sa] cell
```

Where:

slot —The specified slot number.

cell — Specifies that cell bus tracing should be turned on.

da — Sets the SMDS trace 16-digit destination address value for a specified slot.

sa — Sets the SMDS trace 16-digit source address value for a specified slot.

> *If the interface filter is on when the cell bus tracing is also on, the outgoing dump will be invalid. The interface must be cleared. Turn of f the trace first (using the show smds trace off command), then turn it on. After these tasks are complete, you can enable cell bus tracing.*

Examples

Example 1

The following example specifies that all frames wil be traced on slot 3 and that the system should display the trace results.

```
>show smds trace 3 on
```

System2## ----- SMDS Trace Response -----

Tracing on

```
>show smds trace 3 dump 1
```

System2## ---- SMDS Trace Response -----

----- Traced clin smds frames -----

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000 000000000000

05030000000002DCE18009990001FFFFC15089522602FFFF000300000300010000 000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000 000000000000

0503000000000340E18009990001FFFFC15089522602FFFF000300000300010000 000000000000

05030000000003A4E18009990001FFFFC15089522602FFFF000300000300010000 000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000 000000000000

0503000000000408E18009990001FFFFC15089522602FFFF000300000300010000 000000000000

.

.

.

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000000000000000

0503000000000214E18009990001FFFFC15089522602FFFF000300000300010000000000000000

0503000000000278E18009990001FFFFC15089522602FFFF000300000300010000000000000000

Example 2

The following examples display the results of the tracing for a specified destination address on slot 3.

```
>sh smds trace 3 da "C15089522600FFFF"
```

Nashua2## ----- SMDS Trace Response -----

```
Tracing on da  C15089522600FFFF|
```

```
>sh smds trace 3 dump 1
```

Nashua2## ----- SMDS Trace Response -----

```
-----  Traced clin smds frames  -----
```

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000000000000000

.

.

.

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000
000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000
000000000000

0503000000000408C15089522600FFFFC16034379600FFFF000300000300010000
000000000000

Example 3

The following examples display the results of the tracing for a specified destination address on slot 3.

```
>show smds trace 3 cell
```

Nashua2## ----- SMDS Trace Response -----

Cell bus tracing on

Note that if you were to use the dump option with the show command, you must use only the *dump 2* option. The reason for this is that the cell bus captures outgoing traffic. (The *dump 1* option is for ingoing traffic, the *dump 2* option is for outgoing traffic).

show smds statistics

This command provides SMDS frame trace statistics on incoming and outgoing DXI SNI and SSI FDR ports. This command does not support the update of statistics on trunk ports.

As each frame is processed on the DXI/SNI or SSI/FDR port, the system increments the appropriate individual address and group address counts (frames and bytes). These counts are increment prior to SIP3 frame statistic updates. On low speed cards, the byte counts increment for each BTU whereas on the high speed, the whole frame is available during process and the byte counts are updated immediately. The reason for this is that byte counts may not be totally accurate if the command is issued when only a fraction of the BTU's for this frame have been processed.

>show smds statistics *slot [parameters]*

Where:

slot — is the specified slot number.

parameters — are the parameters in the following list.

Parameters

The following list describes each of the parameters that you can use to set SMDS trace variables.

all — Displays the SMDS statistics for all SMDS logical ports available on this IOP.

if_num — Displays the SMDS frame statistics for the specified interface number.

Examples

Example 1

The following example displays statistics for slot 3, interface number 5.

>show smds statis 3 5

Nashua2## ----- SMDS statistics Response -----

----- logical_port (at 0x8000A650) -----

	ia_frames	ia_bytes	ga_frames	ga_bytes	%ia	%ga
Incoming	0	0	2523	1624980	0.00	100.00
Outgoing	0	0	0	0	0.00	0.00

Example 2

The following example displays statistics for all logical ports on slot 3.

>show smds statis 3 all

```
Nashua2##   -----  SMDS statistics Response  -----

        ia_frames    ia_bytes   ga_frames    ga_bytes    %ia       %ga

if:          3

Incoming|  1454 |    1517976 |          0 |          0 | 100.00|   0.00

Outgoing|  1454 |    1517976 |          0 |          0 | 100.00|   0.00

if:          4

Incoming|     0 |          0 |          0 |          0 |   0.00|   0.00

Outgoing|     0 |          0 |          0 |          0 |   0.00|   0.00

if:          5

Incoming|     0 |          0 |       2683 |    1727488 |   0.00| 100.00

Outgoing|     0 |          0 |          0 |          0 |   0.00|   0.00

if:          6

Incoming|     0 |          0 |          0 |          0 |   0.00|   0.00

Outgoing|     0 |          0 |          0 |          0 |   0.00|   0.00
```

show software (all)

This command lists all cards and software information running on each card.

```
> show software (all)
```

Slot	Type	Redund	SW Revision	Software ID	Date
1	CP-BASIC	Active	04.01.00.00	03-B000001C3	20-Nov-1995.17:16:18
2	CP-BASIC	Standby	04.01.00.00	03-B000001C	20-Nov-1995.17:16:18
5	UIO-8	Active	04.01.00.00	03-Q000001AD	16-Nov-1995.15:41:38
6	UIO-8	Standby	04.01.00.00	03-Q000001AD	16-Nov-1995.15:41:38
15	HSSI-2	Active	04.01.00.00	03-B000000FA	20-Nov-1995.11:17:06

show software card [*slot_number*]

This command shows software information (more details in debug mode) running on a particular card. This example displays information for the card in slot 1.

> show software card 1

```
CP Application Image -- For Internal Distribution Only
Copyright (c) 1991-1995 Cascade Communications Corporation

Software Revision: 04.01.00.00
Software ID:       03-B000001C3
Image generated:   20-Nov-1995.17:16:18
```

show software flash

This command shows all software in the CP's flash memory.

```
> show software flash
```

```
Active CP Software:

Part #        Revision      Size      Description

7000900100    3.02.07.00    149961    CP Boot FLASH

7000910100    4.01.00.00    425028    CP Application [03-B000001C3]

                            574989    Total

7000910200    4.01.00.00    394590    IOPA Application [03-Q000001AD]

7000900200    3.01.11.08    122984    IOPA Boot Flash

                            517574    Total

7000914600    4.01.00.00    329270    IOPB Application [03-B00000FA]

7000904600    4.01.00.00    159591    IOPB Boot FLASH

                            488861    Total

Standby CP Software:

Part #        Revision      Size      Description

7000900100    3.02.07.00    149961    CP Boot FLASH

7000910100    4.01.00.00    425028    CP Application [03-B000001C3]

                            574989    Total

7000910200    4.01.00.00    394590    IOPA Application [03-Q000001AD]

7000900200    3.02.00.00    122913    IOPA Boot FLASH

                            517574    Total

7000914600    4.01.00.00    329270    IOPB Application [03-B00000FA]

7000904600    4.01.00.00    159591    IOPB Boot FLASH

                            488861    Total
```

show system

This command displays general system information and status.

```
> show system
```

Switch Name:	92
System Desc:	Cascade Communications Corporation B-STDX 9000
Model:	651-09000-00
Location:	
Contact:	
System State:	Active
Uptime:	1 hours 17 minutes 12 seconds

Serial Number:	0040FB01016 6	Internet IP Addr:	150.150.50.2
Hardware Rev:	01.00.00	Ethernet IP Addr:	192.9.200.174
EPROM Rev:	03.01.00.00	Network Wide Addr:	150.150.50.0
Software Rev:	03.01.01.02	Network Mask:	255.255.255.0

Slot	Type	State	SW Rev	HW Rev	EPROM	Serial #
1	CP	Active	03.01.01.02	01.00.00	03.01.00.00	0040FB0101 66
3	V35-8	Active	03.01.01.02	02.00.00	03.01.00.00	0040FB0102 DD
4	V35-8	Active	03.01.01.02	02.00.00	03.01.00.00	0040FB0102 DE
8	V35-8	Active	03.01.01.02	01.00.00	03.01.00.00	0040FB0101 01

12	V35-8	Active	03.01.01.02	02.00.00	03.01.00.00	0040FB010310
14	FT-4-24	Active	03.01.01.02	02.00.00	03.01.00.00	0040FB0102C3
15	FT-4-24	Active	03.01.01.02	02.00.00	03.01.00.00	0040FB0102C2
16	V35-8	Active	03.01.01.02	02.00.00	03.01.00.00	0040FB0102D8

show tcp

This command displays basic counters on TCP (Transmission Control Protocol) such as the number of TCP connections requested and the number of TCP connections denied.

```
> show tcp

                   Receive       Transmit

Packets            0             0

Retransmissions    -             0


                           TCP Connections Counts

Connections Requested:     0

Connections Accepted:      0

Connections Failed:        0

Connections Reset:         0

Current Connections:       0
```

show udp

This command displays counters on UDP (User Datagram Protocol), such as the number of UDP packets transmitted and received and the number of errors that occured.

```
> show udp

             Receive      Transmit

Datagrams:   747          1181

Errors:      0            -

No Ports:    0            -
```

show users

This command displays users currently logged on to the switch through console or telnet.

```
> show users
```

user	location	time
your name	console	14 minutes 21 seconds

DEBUG LEVEL

```
> enable debug
Password:
DEBUG ACCESS LEVEL GRANTED.
##              << DEBUG PROMPT
```

Table A-2. Debug Commands

Command	Description
set ?	Set parameters
reset ? reset pram <slot> reset system reset pport <slot.port> reset lport <interface> reset pvc <interface.dlci>	Reset PRAM, system, pport, lport, or pvc
install	Invoke installation procedure (You should only use this command to bring the switch to a readable state from the NMS.)
disable [master]	Return to normal read-only mode
telnet <host> [term]	Telnet to another switch
heapwalk	Check heap
dump	Dump memory contents
mb	Modify a byte in memory
modify	Modify a word (4 bytes) in memory
cell	Enter low level debug

SMDS Billing Console Commands

This sections describes the console commands that you can use for SMDS Billing. For more information, refer to the *SMDS Billing System Administrator's Guide*.

show billing

This command shows the current state of SMDS billing, including information on the current Aggregation Period and usage data file transfer status.

> show billing

```
1 SMDS Billing Status: (Billing is enabled)
2    State: Idle
3    Adjunct Processor            : 152.148.30.19
4    Aggregation Period Ends      : 1 hr 2 min 20 sec (14:00:00 -
                                  16:00:00)
5    Daily Audit Processing       : Enabled (Nov 2 00:00:00-Nov 3
                                  00:00:00)
6    Next Usage Data Collection   : 23 sec
7    Usage data staging           : 0x9039adb0
8    Size of usage data staging   : 245760 (Last read = 245760 bytes)
9    Last unsched upload from     :0
     IOP
10   Unsched IOP uploads          : 0 (Failed : 0)
     requested
11   VCC read errors              : 0
12
13   Records sent to AP:                         0 Total for day : 0
14   Usage record creation        :              0 Total for day : 0
     failure
15   UDF reached capacity         :              0 Total for day : 0
```

```
16   Counter overflow warnings   :              0 Total for day : 0
17   File transfer successes     :              23
18   File transfer failures      :              0
19   Primary UDF is in use.
```

Lines 1 through 11 present the state of the system.

- Line 1 indicates whether SMDS billing is enabled or disabled on the switch.
- Line 2 gives the state of the SMDS billing system. In the example, the Billing System on the CP is enabled, but idle,(i.e., it is not in the process of collecting usage data from the IOPs or transferring data to the Adjunct Processor.) Billing data is, however, being measured at each DXI/SNI for which billing is enabled.
- Line 3 indicates the IP address of the Adjunct Processor.
- Line 4 indicates the time remaining in the current aggregation period, including the starting and end-time of the period.
- Line 5 indicates if daily audit reconciliation processing is enabled, including the reconciliation period.
- Line 6 indicates the number of seconds until the next poll of the IOPs for billing data (used for debugging).
- Line 7 is used for debugging only.
- Line 8 is used for debugging only.
- Line 9 gives the slot number of the last IOP which requested an unscheduled upload of usage data to the CP; a non-zero number indicates that an IOP's billing data store reached capacity before the next scheduled upload to the CP.
- Line 10 indicates the total number of unscheduled IOP upload requested received.
- Line 11 is used for debugging; a non-zero count indicates that the CP is having trouble uploading billing data from one or more IOPs.

Lines 13 to 16 present statistics on the operation of the system; these statistics can also be viewed through CascadeView/UX. The first count is the number of occurrences of the event during the current aggregation period; the second count is the total for the current day (since 00:00:00).

- Line 13 indicates the number of usage records that have been sent to the AP.
- Line 14 indicates the number of times the CP failed to create a usage record.
- Line 15 indicates the number of times the usage data store on the CP reached capacity.
- Line 16 indicates the number of times a usage data counter overflow condition was detected (and the associated record was closed).

Lines 17 and 18 indicate the state of usage file transfers to the Adjunct Processor. Additional information is displayed during a file transfer (see next example). Additional information is also available from the SHOW BILLING FTP command.

- Line 17 indicates the total number of successful usage file transfers to the Adjunct Processor.
- Line 18 indicates the total number of failed usage file transfer attempts to the Adjunct Processor.
- Line 19 indicates which usage data store is currently in use, either the Primary or Secondary.

Example 2

This example captures the SMDS Billing System when it is uploading usage data from an IOP and also performing a Usage Data store transfer to the Adjunct Processor.

```
> show billing
```

1 SMDS Billing Status: (Billing is enabled)

2	State:	Polling IOPs for Usage Data	
3		End of Aggr Period; Primary UDF transfer in progress	
4	Adjunct Processor	:	152.148.30.19
5	Aggregation Period Ends	:	1 hr 59 min 54 sec(20:00:00 - 22:00:00)
6	Daily Audit Processing	:	Enabled (Nov 20 00:00:00-Nov 21 00:00:00)
7	Next Usage Data Collection	:	29 sec
8	Usage data staging	:	0x9039ae70
9	Size of usage data staging	:	245760 (Last read = 12288 bytes)
10	IOP currently being processed	:	5
11	Last unsched upload from IOP	:	0
12	Unsched IOP uploads requested	:	0 (Failed : 0)
13	VCC read errors	:	0
14	Records sent to AP	:	25 Total for day : 125
15	Usage record creation failure	:	0 Total for day : 0
16	UDF reached capacity	:	0 Total for day : 0

17	Counter overflow warnings	:	0 Total for day : 0
18	File transfer successes	:	221
19	File transfer failures	:	0
20	File being transferred	:	bs_A_SMDS.152.148.177.2.20Nov95200000
21	Current FTP error retries	:	1
22	Current FTP retry time	:	1 sec
23	Secondary UDF is in use.		

- Lines 2 gives the state of the system, indicating that
  - Usage data is being collected from the IOPs (Polling IOPs for Usage Data).
  - The current aggregation period has ended and the Primary Usage Data store is being transferred to the Adjunct Processor.
- Lines 9-10 indicates that usage data from the IOP in slot 5 is currently being uploaded and aggregated into the current Usage Data store. Line 9 indicates that 12288 out of 245760 bytes have been uploaded from IOP 5 (and that 233472 bytes have yet to be transferred).
- Lines 17-20 indicate the state of the Usage Data store transfer. The name of the data store being transferred is given in line 20; this is the name of the file that will be created at the AP.
- Lines 21 and 22 provide information on the number of attempts to transfer the given file.
- Line 23 indicates that the Secondary Usage Data store is in use; this is because the Primary data store is being transferred to the Adjunct Processor.

show billing udf

This command shows the current state of the two SMDS Billing Usage Data Stores (sometimes referred to as Usage Data Files, or UDF). This command is primarily used for debugging purposes, but it does provide usage information pertaining to the number of usage records in the data stores.

> show billing udf

```
1 Primary UDF is in use.
2
3    Primary UDF: (bof) 0x50800400 (eof) 0x508ce000 (842752 bytes 823 KB)
4    Record Table:
5          Base addr 0x50810434 End 0x508ce000  Length 777164 bytes (758 KB)
6          Resident: 0 records  Free Ptr: 0x50810434 (777164 free bytes)
7          Longest hash chain: 0 entries (in bucket 0)
8    Lookup Table (base address 0x50800434):
9          Capacity: 8192 entries  Resident: 0 entries
10         Longest hash chain: 0 entries (in bucket 0)
11
12   Secondary UDF: (bof) 0x508ce000 (eof) 0x50900000 (204800 bytes 200 KB)
13   Record Table:
14         Base addr 0x508d6034 End 0x50900000  Length 171980 bytes (167 KB)
15         Resident: 0 records  Free Ptr: 0x508d6034 (171980 free bytes)
16         Longest hash chain: 0 entries (in bucket 0)
17   Lookup Table (base address 0x508ce034):
18         Capacity: 4096 entries  Resident: 0 entries
19         Longest hash chain: 0 entries (in bucket 0)
```

- Line 1 indicates if the Primary or Secondary usage data store is in use.

- The next two groups show the state of the Primary and Secondary usage data files (lines 3-10 and 12-19). An SMDS Usage Data store contains two objects: a Record Table which contains the SMDS usage records, and an E.164 address Lookup Table, which contains E.164 addresses. The output gives the number of records and addresses contained in each object, the address of each object and the amount of space available to store additional billing data.
- Lines 6 and 15 indicate the state of the record table, including the number of records currently in the table and the amount of available space remaining.
- Lines 7 and 16 provide performance measurements that are used for debugging the system.
- Lines 9 and 18 indicate the state of the E.164 address lookup table, including the size of the table (e.g., 8192 addresses in the Primary) and the number of addresses currently in the table.
- Lines 10 and 19 provide performance measurements that are used for debugging the system.

show billing ftp

This command shows the state of the file transfer task that performs Usage Data store transfers from the billing system on the switch to the Adjunct Processor. This command provides useful information that can be used to troubleshoot the system when the switch is having problems transferring Usage Data stores to the Adjunct Processor.

The output shows the state of the file transfer task, either Idle or Busy, where Busy indicates that a file transfer is being attempted or is in progress.

The counts are defined as follows:

Transfers requested	The number of file transfers requested since the last reboot of the system.
Successful transfers	The number of successful file transfers.
Failed transfers	The number of file transfers that have failed, due to a network failure, rejection by the Adjunct Processor or the absence of a route to the Adjunct Processor.
Requests denied (busy)	The number of file transfer requests that were denied due to the file transfer task being in the Busy state.
Protocol errors	The number of file transfer protocol errors.

The TCP connection error counts categorize any TCP/IP related errors that have occurred during a file transfer.

The non-zero Net Unreachable count shown below indicates that a path to the Adjunct Processor does not exist. If this count is non-zero (and usage data file transfer failures are occurring), verify that an NMS Path to the Adjunct Processor exists; also verify that the Adjunct Processor has a route to the switch.

The Connection Refused count will increment when billing is disabled on the Adjunct Processor (or billing software has not been installed). In this case, the AP software does not accept a file transfer from the switch.

```
> show billing ftp
```

FTP state: Idle

Transfers requested	: 68
Successful transfers	: 0
Failed transfers	: 68
Requests denied (busy)	: 0
Protocol errors	: 0

TCP connection error counts:

Sys Err	0	Net Unreachable	: 68
Conn Timeout	0	Conn refused	: 0
Port In Use	0	Unknown error	: 0
Dropped conns	0	(possibly dropped)	

STDX 6000 Console Commands

The commands listed in this section apply to the STDX 3000/6000 Frame Relay release.

- To display a list of available commands, type '?'

```
> ?
CONFIGURATION CONSOLE COMMANDS:

get <oid>
next <oid>
```

For get & next, the following OID shorthand prefixes can be used:

std, system, interface, ip, icmp, udp, snmp,
ds1, frx, net, ase, node, pport, lport, ckt

ping <[ip address]>

bye, end, exit or quit

- To go into master or debug mode:

```
login [master|debug]

> login debug
Password:
DEBUG ACCESS LEVEL DENIED.
> login master
Password:
MASTER ACCESS LEVEL GRANTED.
```

- snmp get

```
get <oid>
```

example 1: `get 1.3.6.1.2.1.1.1.0`
example 2: **`get node.10.0`**

- snmp set

  set <oid> <<integer> | <asn.1> | <"string"> | <[ip address]>>

  example: `set node.1.0 [152.148.100.1]`

- snmp next

  next <oid>

  example: `next node`

- change community name

- **set community<0-7> <"read-only community name">**
  set community<0-7> <"master community name"> <[master ip address]>

> *You can only specify one master community.*

- To test reachability of an IP node:

  ping <[ip address]>

- To exit from the console:

  bye, end, exit or quit

- To clear the configuration:

  reset pram

- To restart the system:

  reset system

- To read directly from and write directly to memory:

```
mb <address> | <address#bytes>(modify one byte)
modify <address> | <address#words>(modify a 4-byte word)
dump [[address] | [address#length]](dump memory contents)
```

B

DS3 and DS1 Statistics

This appendix lists and describes the DS3 and DS1 current, interval, and total statistics and variables.

DS3 Statistics and Variables

This section lists and describes the DS3 current, interval, and total statistics and variables.

DS3 Current Statistics

DS3 Current Statistics provide up-to-date statistical information for the current 15-minute interval. Table B-1 lists and describes the DS3 current statistics and variables.

Table B-1. DS3 Current Statistics and Variables

Variable	Displays
Index	The index value that identifies this entry's DS3 interface.
P-bit Errored Seconds	The number of P-bit Errored-Seconds encountered by a DS3 interface in the current 15-minute interval.
P-bit Severely Errored Seconds	The number of P-bit Severely Errored Seconds encountered by a DS3 interface in the current 15-minute interval.
Severely Errored Framing Seconds	The number of Severely Errored Framing Seconds encountered by a DS3 interface in the current 15 minute interval.
Unavailable Seconds	The number of Unavailable Seconds encountered by a DS3 interface in the current 15-minute interval.
Line Coding Violations	The number of Line Coding Violations encountered by a DS3 interface in the current 15-minute interval.
P-bit Coding Violations	The number of P-bit Coding Violations (PCV) encountered by a DS3 interface in the current 15-minute interval.
Line Errored Seconds	The number of Line Errored Seconds encountered by a DS3 interface in the current 15-minute interval.

Table B-1. DS3 Current Statistics and Variables (Continued)

Variable	Displays
C-bit Coding Violations	The number of C-bit Coding Violations encountered by a DS3 interface in the current 15-minute interval.
C-bit Errored Seconds	The number of C-bit Errored-Seconds encountered by a DS3 interface in the current 15-minute interval.
C-bit Severely Errored Seconds	The number of C-bit Severely Errored Seconds encountered by a DS3 interface in the current 15-minute interval.

DS3 Interval Statistics

DS3 Interval Statistics provide statistical information on the last 24 hours of operation. The last 24 hours are broken down into 96 completed 15-minute intervals. Table B-2 lists and describes the DS3 interval statistics and variables.

Table B-2. DS3 Interval Statistics and Variables

Variable	Displays
Interval Number	A number between 1 and 96 (1 is the most recently completed interval).
Index	The index value that identifies this entry’s DS3 interface.
P-bit Errored Seconds	The number of P-bit Errored-Seconds encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.
P-bit Severely Errored Seconds	The number of P-bit Severely Errored Seconds encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.

Table B-2. DS3 Interval Statistics and Variables (Continued)

Variable	Displays
P-bit Severely Errored Framing	The number of P-bit Severely Errored Framing Seconds encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.
Unavailable Seconds	The number of Unavailable Seconds encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.
Line Coding Violations	The number of Line Coding Violations encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.
P-bit Coding Violations	The number of P-bit Coding Violations (PCV) encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.
Line Errored Seconds	The number of Line Errored Seconds encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.
C-bit Coding Violations	The number of C-bit Coding Violations encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.
C-bit Errored Seconds	The number of C-bit Errored-Seconds encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.
C-bit Severely Errored Seconds	The number of C-bit Severely Errored Seconds encountered by a DS3 interface in one of the previous 96 (individual 15 minute) intervals.

DS3 Total Statistics

DS3 Total Statistics provide statistical information for the sum of all intervals and the current interval. Table B-3 lists and describes the DS3 total statistics and variables.

Table B-3. DS3 Total Statistics and Variables

Variable	Displays
Index	The index value that identifies this entry's DS3 interface.
P-bit Errored Seconds	The number of P-bit Errored-Seconds encountered by a DS3 interface in the previous 24 hour interval.
P-bit Severely Errored Seconds	The number of P-bit Severely Errored Framing Seconds encountered by a DS3 interface in the previous 24-hour interval.
P-bit Severely Errored Framing	The number of Severely Errored Seconds encountered by a DS3 interface in the previous 24-hour interval.
Unavailable Seconds	The number of Unavailable Seconds encountered by a DS3 interface in the previous 24-hour interval.
Line Coding Violations	The number of Line Coding Violations encountered by a DS3 interface in the previous 24-hour interval.
P-bit Coding Violations	The number of P-bit Coding Violations (PCV) encountered by a DS3 interface in the previous 24-hour interval.
Line Errored Seconds	The number of Line Errored Seconds encountered by a DS3 interface in the previous 24-hour interval.

Table B-3. DS3 Total Statistics and Variables (Continued)

Variable	Displays
C-bit Coding Violations	The number of C-bit Coding Violations encountered by a DS3 interface in the previous 24-hour interval.
C-bit Errored Seconds	The number of C-bit Errored-Seconds encountered by a DS3 interface in the previous 24-hour interval.
C-bit Severely Errored Seconds	The number of C-bit Severely Errored Seconds encountered by a DS3 interface in the previous 24-hour interval.

DS1 Statistics and Variables

This section lists and describes the DS1 current, interval, and total statistics and variables.

DS1 Current Statistics

DS1 Current Statistics provide up-to -date statistical information for the current 15-minute interval. Table B-4 lists and describes the DS1 current statistics and variables.

Table B-4. DS1 Current Statistics and Variables

Variable	Displays
Current Index	The index value that identifies this entry's DS1 interface.
Current Errored Seconds	The number of Errored-Seconds encountered by a DS1 interface in the current 15-minute interval.

Table B-4. DS1 Current Statistics and Variables (Continued)

Variable	Displays
Current Severely Errored Seconds	The number of P-bit Severely Errored Seconds encountered by a DS1 interface in the current 15-minute interval.
Current Severely Errored Framing Seconds	The number of Severely Errored Framing Seconds encountered by a DS1 interface in the current 15-minute interval.
Current Unavailable Seconds	The number of Unavailable Seconds encountered by a DS1 interface in the current 15-minute interval.
Current Controlled Slip Seconds	Not Supported.
Current Path Coding Violations	The number of Path Coding Violations encountered by a DS1 interface in the current 15-minute interval.
Current Line Errored Seconds	The number of Line Errored Seconds encountered by a DS1 interface in the current 15-minute interval.
Current Bursty Errored Seconds	The number of Bursty Errored Seconds encountered by a DS1 interface in the current 15-minute interval.
Current Degraded Minutes	The number of Degraded Minutes encountered by a DS1 interface in the current 15-minute interval.
Current Line Code Violations	The number of Line Code Violations encountered by a DS1 interface in the current 15-minute interval.

DS1 Interval Statistics

DS1 Interval Statistics provide statistical information on the last 24 hours of operation. Table B-5 lists and describes the DS1 interval statistics and variables.

Table B-5. DS1 Interval Statistics and Variables

Variable	Displays
Interval Index	The index value that identifies this entry's DS1 interface.
Interval Errored Seconds	The number of Errored-Seconds encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.
Interval Severely Errored Seconds	The number of Severely Errored Seconds encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.
Interval Severely Errored Framing Seconds	The number of Severely Errored Framing Seconds encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.
Interval Unavailable Seconds	The number of Unavailable Seconds encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.
Interval Path Coding Violations	The number of Path Coding Violations encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.
Interval Line Errored Seconds	The number of Line Errored Seconds encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.
Interval Bursty Errored Seconds	The number of Bursty Errored Seconds encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.

Table B-5. DS1 Interval Statistics and Variables (Continued)

Variable	Displays
Interval Degraded Minutes	The number of Degraded Minutes encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.
Interval Line Code Violations	The number of Line Code Violations encountered by a DS1 interface in one of the previous 96 (individual 15 minute) intervals.
Interval Number	A number between 1 and 96, where 1 is the most recently completed 15 minute interval.

DS1 Total Statistics

DS1 Total Statistics provide statistical information for the sum of all intervals and the current interval. Table B-6 lists and describes the DS1 total statistics and variables.

Table B-6. DS1 Total Statistics and Variables

Variable	Displays
Total Index	The index value that identifies this entry's DS1 interface.
Total Errored Seconds	The number of Errored Seconds encountered by a DS1 interface for the sum of all intervals.
Total Severely Errored Seconds	The number of Severely Errored Seconds encountered by a DS1 interface for the sum of all intervals.
Total Severely Errored Framing Seconds	The number of Severely Errored Framing Seconds encountered by a DS1 for the sum of all intervals.
Total Unavailable Seconds	The number of Unavailable Seconds encountered by a DS1 interface for the sum of all intervals.

Table B-6. DS1 Total Statistics and Variables (Continued)

Variable	Displays
Total Path Coding Violations	The number of Path Coding Violations encountered by a DS1 interface for the sum of all intervals.
Total Line Errored Seconds	The number of Line Errored Seconds encountered by a DS1 interface for the sum of all intervals.
Total Bursty Errored Seconds	The number of Bursty Errored Seconds encountered by a DS1 interface for the sum of all intervals.
Total Degraded Minutes	The number of Degraded Minutes encountered by a DS1 interface for the sum of all intervals.
Total Line Code Violations	The number of Line Code Violations encountered by a DS1 interface for the sum of all intervals.

C

Using Copy Database

Overview

The Copy Database utility enables you to copy data into or out of any CascadeView/UX 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 utility automatically creates a DDL script when copying data out from an existing CascadeView/UX database. The data files and the DDL scripts are bundled into a single tar file. (Bulk Copy generates the data files. The files 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

So if you were copying 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.

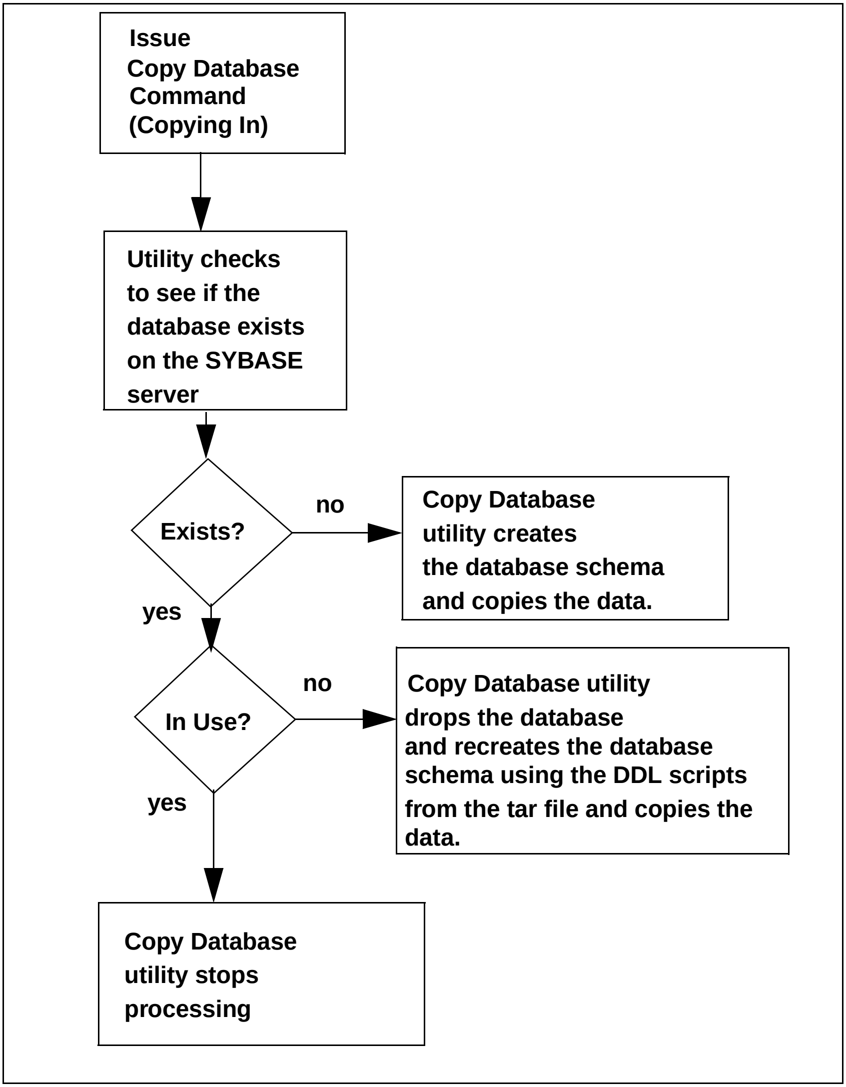


Figure C-1. Process Flow for Using Copy Database to Copy In

Figure C-2 illustrates the process flow for the Copy Database utility when you use the utility to copy in data.

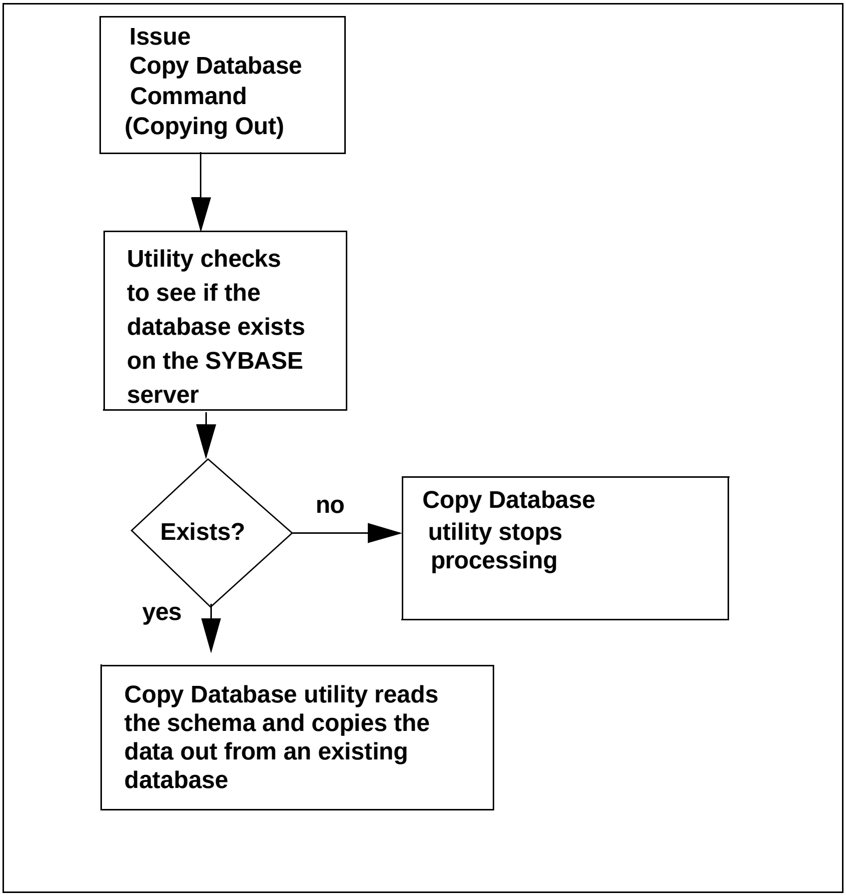


Figure C-2. Process Flow for Using Copy Database to Copy Out

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]***

Where:

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 will copy. 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.

Parameter	Specifies
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 will copy 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 six 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 result when you are using the Copy Database utility.

General Errors

Error

The SYBASE server defined in cvdb.cfg is not accessible.

Resolution

This problem can be caused by a number of factors. The most common cause is a lack of space. Contact the Technical Resource Center for further information about how to resolve this error.

Error

Cannot log in to the database server $DSQUERY. Please check your input parameters, exiting now.

Resolution

The specified database does not exist in the SYBASE server. Check the database name and server name and reenter using a valid name.

Error

Cannot locate the database $DB_NAME from server $DSQUERY, exiting now.

Resolution

You have not specified a valid input database name for the db_name parameter. Check the value and reenter the command.

Error

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.

Resolution

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

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.

Resolution

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

Error discovered while using bulkcopy to copy out data for table *$table.*

Resolution

Contact the Technical Support Center.

Copy In Errors

Error

Cannot drop the database $TEMP_DB_NAME, because it is in use.

Resolution

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.

Resolution

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

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.

Resolution

Change the data size for the database and run the utility again.

Error

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.

Resolution

Change the log space value and run the utility again.

Error

Error discovered when trying to create the schema for $TEMP_DB_NAME.

Error

Fatal error discovered when trying to create the schema for $TEMP. For more information about the error, please read $TMPFILE.

Resolution

Review the $TMPFILE for more information about this error.

Index

E